HP ProtectTools

Mise en route

© Copyright 2012 Hewlett-Packard Development Company, L.P.

Bluetooth est une marque commerciale détenue par son propriétaire et utilisée sous licence par Hewlett-Packard Company. Intel est une marque commerciale d'Intel Corporation aux Etats-Unis et dans d'autres pays et est utilisée sous licence. Microsoft et Windows sont des marques déposées de Microsoft Corporation aux Etats-Unis.

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

Première édition : août 2012

Référence du document : 702113-051

Sommaire

1 Présentation de la sécurité

Le logiciel HP ProtectTools Security Manager fournit des fonctions de sécurité conçues pour empêcher tout accès non autorisé à l'ordinateur, aux réseaux et aux données critiques.

Application	Fonctions
Console d'administration de HP ProtectTools Security Manager (pour les administrateurs)	• Accès nécessitant des droits d'administrateur Microsoft Windows®. • Offre un accès aux modules configurés par un administrateur et non disponibles pour les utilisateurs. • Permet la configuration initiale de la sécurité et configure des options et des exigences pour l'ensemble des utilisateurs.
Console utilisateur de HP ProtectTools Security Manager (pour les utilisateurs)	• Permet aux utilisateurs de configurer les options fournies par un administrateur. • Permet aux administrateurs d'offrir aux utilisateurs un contrôle limité sur certains modules HP ProtectTools.

Les modules logiciels disponibles pour votre ordinateur peuvent varier en fonction du modèle de celui-ci.

Les modules logiciels HP ProtectTools peuvent être préinstallés, préchargés ou disponibles pour téléchargement à partir du site Web HP. Pour plus d'informations, accédez à l'adresse http://www.hp.com.

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

Fonctions de HP ProtectTools

Le tableau suivant détaille les principales fonctions des modules HP ProtectTools.

Module	Fonctions principales
Console d'administration de HP ProtectTools Security Manager	Les administrateurs peuvent exécuter les fonctions suivantes : • Utiliser l'Assistant de configuration de Security Manager pour configurer les méthodes de connexion sécurisées et les niveaux de sécurité. • Configurer les options masquées, non accessibles aux utilisateurs. • Activer Drive Encryption et configurer l'accès utilisateur. • Configurer l'accès utilisateur et les règles de Device Access Manager. • Utiliser les outils d'administration pour ajouter et supprimer des utilisateurs HP ProtectTools et afficher le statut des utilisateurs.

Module	Fonctions principales
Console utilisateur de HP ProtectTools Security Manager	Les utilisateurs généraux peuvent exécuter les fonctions suivantes : • Afficher les paramètres État du cryptage et Device Access Manager • Activer Computrace for HP ProtectTools. • Configurer les préférences et les options de sauvegarde et de restauration.
Credential Manager	Les utilisateurs généraux peuvent exécuter les fonctions suivantes : • Modifier les noms d'utilisateur et les mots de passe. • Configurer et modifier les informations d'authentification de l'utilisateur, telles qu'un mot de passe Windows, une empreinte digitale, des images faciales, une Smart Card, une carte de proximité ou une carte sans contact.
Password Manager	Les utilisateurs généraux peuvent exécuter les fonctions suivantes : • Organiser et configurer les noms d'utilisateur et les mots de passe. • Créer des mots de passe plus forts afin de renforcer la sécurité du compte. Password Manager insère et envoie automatiquement les informations. • Rationnaliser le processus de connexion avec la fonction d'authentification unique, qui mémorise et applique automatiquement les informations d'authentification de l'utilisateur.
Drive Encryption for HP ProtectTools (certains modèles uniquement)	• Fournit un cryptage du volume complet du disque dur. • Permet de forcer une authentification au préamorçage afin de décrypter les données et d'y accéder. • Offre la possibilité d'activer des unités autocryptées (certains modèles uniquement).
Device Access Manager for HP ProtectTools (certains modèles uniquement)	• Permet aux responsables informatiques de contrôler l'accès aux périphériques en fonction des profils des utilisateurs. • Empêche les utilisateurs non autorisés de supprimer des données en les transférant sur un support de stockage externe et d'introduire des virus dans le système à partir d'un support externe. • Permet aux administrateurs de désactiver l'accès d'un utilisateur ou d'un groupe d'utilisateurs spécifique aux périphériques de communication.
Récupération en cas de vol (Computrace for HP ProtectTools, acheté séparément)	• Activation nécessitant des abonnements séparés aux services de suivi et de traçage. • Permet le suivi des ressources en toute sécurité. • Surveille les activités de l'utilisateur, ainsi que les modifications apportées au matériel et aux logiciels. • Reste actif même si vous reformatez ou remplacez le disque dur.

Description des produits de sécurité HP ProtectTools et exemples d'utilisation courante

La plupart des produits de sécurité HP ProtectTools intègrent une fonction d'authentification utilisateur (généralement un mot de passe) et de sauvegarde administrative afin d'obtenir un accès en cas de perte, d'indisponibilité ou d'oubli des mots de passe ou chaque fois que la sécurité de l'entreprise requiert un accès.

REMARQUE : Certains produits de sécurité HP ProtectTools sont conçus pour limiter l'accès aux données. Les données doivent être cryptées lorsqu'elles sont tellement importantes que l'utilisateur préfère les perdre que les compromettre. Il est recommandé de sauvegarder l'intégralité des données dans un emplacement sécurisé.

Password Manager

Password Manager stocke les noms d'utilisateur et les mots de passe, et permet d'effectuer les opérations suivantes :

- Enregistrer les noms et les mots de passe de connexion pour l'accès à Internet ou à la messagerie électronique.
- Connecter automatiquement l'utilisateur à un site Web ou à la messagerie électronique.
- Gérer et organiser des authentifications.
- Sélectionner une ressource Web ou réseau et accéder directement au lien.
- Afficher les noms et les mots de passe si nécessaire.

Exemple 1 : Un acheteur travaillant pour le compte d'un grand fabricant effectue la plupart des transactions d'entreprise sur Internet. Par ailleurs, elle consulte fréquemment de nombreux sites Web populaires qui requièrent des informations de connexion. Elle est consciente des risques liés à la sécurité et n'utilise pas le même mot de passe sur chaque compte. L'acheteur a décidé d'utiliser le Gestionnaire de mots de passe pour attribuer des noms d'utilisateur et des mots de passe différents aux liens Web. Lorsqu'elle accède à un site Web pour ouvrir une session, le Gestionnaire de mots de passe présente automatiquement les informations d'authentification. Si elle souhaite consulter les noms d'utilisateur et les mots de passe, elle peut configurer le Gestionnaire de mots de passe pour les afficher.

Vous pouvez également utiliser Password Manager pour gérer et organiser les authentifications. Cet outil permet à un utilisateur de sélectionner une ressource Web ou réseau et d'accéder directement au lien. L'utilisateur peut également afficher les noms d'utilisateur et les mots de passe en cas de besoin.

Exemple 2 : Un expert-comptable enthousiaste a été promu et va désormais gérer tout le service de comptabilité. L'équipe doit se connecter à un grand nombre de comptes Web client, dont chacun utilise des informations de connexion différentes. Comme ces informations de connexion doivent être partagées avec d'autres employés, la confidentialité représente un problème. L'expert-comptable décide d'organiser tous les liens Web, les noms d'utilisateur de l'entreprise et les mots de passe dans le Gestionnaire de mots de passe. Une fois cette opération effectuée, il met le Gestionnaire de mots de passe à la disposition des employés pour qu'ils puissent utiliser les comptes Web sans jamais connaître les informations d'identification de connexion utilisées.

Drive Encryption for HP ProtectTools (certains modèles uniquement)

Drive Encryption permet de limiter l'accès aux données de tout le disque dur de l'ordinateur ou d'un disque secondaire. Drive Encryption permet également de gérer les unités autocryptées.

Exemple 1 : Un médecin souhaite s'assurer qu'il est le seul à pouvoir accéder aux données stockées sur le disque dur de son ordinateur. Il active Drive Encryption, qui requiert une authentification au préamorçage afin de pouvoir ouvrir une session Windows. Une fois configuré, il est impossible d'accéder au disque dur sans un mot de passe, avant le démarrage du système d'exploitation. Le médecin peut renforcer davantage la sécurité du disque dur en choisissant de crypter les données à l'aide de l'option Unité autocryptée.

Drive Encryption for HP ProtectTools ne permet pas d'accéder aux données cryptées même lorsque vous retirez le disque dur. En effet, ils sont tous les deux intégrés à la carte mère d'origine.

Exemple 2 : Un administrateur d'hôpital souhaite s'assurer que seuls les médecins et le personnel autorisé peuvent accéder aux données de leur ordinateur local, sans partager leurs mots de passe personnels. Le service informatique ajoute l'administrateur, les médecins et tout le personnel autorisé en tant qu'utilisateurs de Drive Encryption. Désormais, seul les membres du personnel autorisé peuvent démarrer l'ordinateur ou le domaine à l'aide de leur nom d'utilisateur et de leur mot de passe personnel.

Device Access Manager for HP ProtectTools (certains modèles uniquement)

Device Access Manager for HP ProtectTools permet à un administrateur de limiter et de gérer l'accès au matériel. Vous pouvez utiliser Device Access Manager for HP ProtectTools pour bloquer tout accès non autorisé aux unités flash USB, sur lesquelles les données peuvent être copiées. Il permet également de limiter l'accès aux lecteurs de CD/DVD, le contrôle des périphériques USB, les connexions réseau, etc. A titre d'exemple, un fournisseur externe doit accéder aux ordinateurs de l'entreprise, mais ne doit pas pouvoir copier les données sur un lecteur USB.

Exemple 1 : Un directeur d'une société spécialisée dans la fourniture d'équipement médical utilise souvent des dossiers médicaux personnels avec les données de son entreprise. Les employés doivent accéder à ces données. Cependant, ils doivent veiller à ne pas supprimer les données de l'ordinateur en les transférant sur un lecteur USB ou sur tout autre support de stockage externe. Le réseau est sécurisé, mais les ordinateurs sont équipés de graveurs de CD et de ports USB qui peuvent permettre aux employés de copier ou de voler des données. Le directeur utilise Device Access Manager pour désactiver les ports USB et les graveurs de CD. De cette façon, il est impossible de les utiliser. Même si les ports USB sont bloqués, la souris et les claviers restent fonctionnels.

Exemple 2 : Une compagnie d'assurances ne souhaite pas que ses employés installent ou chargent des logiciels ou des données personnelles depuis chez eux. Certains employés doivent accéder au port USB de tous les ordinateurs. Le responsable informatique utilise Device Access Manager pour activer l'accès pour certains employés, tout en bloquant l'accès externe pour d'autres.

Computrace for HP ProtectTools (anciennement LoJack Pro) (acheté séparément)

Computrace for HP ProtectTools (acheté séparément) est un service capable de suivre l'emplacement d'un ordinateur volé chaque fois que l'utilisateur accède à Internet. Computrace for HP ProtectTools permet également de gérer et de localiser des ordinateurs à distance. Par ailleurs, il permet de surveiller l'utilisation des ordinateurs et les applications informatiques.

Exemple 1 : Un directeur d'école a indiqué au service informatique d'effectuer le suivi de tous les ordinateurs de l'école. Une fois l'inventaire des ordinateurs effectué, l'administrateur informatique a enregistré l'ensemble des ordinateurs par le biais de Computrace afin qu'ils puissent être suivis en cas de vol. L'école a récemment constaté que plusieurs ordinateurs étaient manquants. L'administrateur informatique a donc alerté les autorités et les agents Computrace. Les autorités ont localisé les ordinateurs et les ont remis à l'école.

Exemple 2 : Une société immobilière doit gérer et mettre à jour des ordinateurs partout dans le monde. Elle utilise Computrace pour surveiller et mettre à jour les ordinateurs, sans dépêcher un informaticien pour chacun d'eux.

Atteinte des principaux objectifs de sécurité

Les modules HP ProtectTools peuvent fonctionner ensemble afin de fournir des solutions à divers problèmes de sécurité, y compris pour atteindre les principaux objectifs de sécurité suivants :

- Protection contre le vol ciblé
- Limitation de l'accès aux données sensibles
- Blocage de l'accès non autorisé depuis les emplacements internes ou externes
- Création de règles de mot de passe fort

Protection contre le vol ciblé

Un exemple de vol ciblé pourrait être le vol d'un ordinateur contenant des données confidentielles et des informations client au point de contrôle de la sécurité d'un aéroport. Les fonctions suivantes permettent de protéger contre le vol ciblé :

- Une fois activée, la fonction d'authentification au préamorçage d'empêcher l'accès au système d'exploitation.
  - Security Manager for HP ProtectTools—Voir HP ProtectTools Security Manager à la page 26.
  - Drive Encryption for HP ProtectTools—Voir Drive Encryption for HP ProtectTools (certains modèles uniquement) à la page 43.
- Encryption permet de garantir que les données ne sont pas accessibles même si le disque dur est retiré et installé dans un système non sécurisé.
- Computrace peut suivre l'emplacement de l'ordinateur volé.
  - Computrace for HP ProtectTools—Voir Récupération en cas de vol (certains modèles) à la page 63.

Limitation de l'accès aux données sensibles

Supposons qu'une personne chargée de l'audit des contrats travaille sur site et a été autorisée à accéder à l'ordinateur afin de consulter les données financières sensibles. Vous ne souhaitez pas qu'elle puisse imprimer les fichiers ou les enregistrer sur un périphérique inscriptible, tel qu'un CD. La fonction suivante permet de limiter l'accès aux données :

- Device Access Manager for HP ProtectTools permet aux responsables informatiques de limiter l'accès aux périphériques de communication de façon à ce que les informations sensibles ne puissent pas être copiées depuis le disque dur. Reportez-vous à la section Configuration de classe de périphérique à la page 54.

Blocage de l'accès non autorisé depuis les emplacements internes ou externes

L'accès non autorisé à un ordinateur professionnel non sécurisé représente un risque réel pour les ressources réseau de l'entreprise, notamment les informations provenant des services financiers, d'un cadre ou de l'équipe de Recherche et développement, et les informations privées telles que les

dossiers de patient ou les dossiers financiers personnels. Les fonctions suivantes permettent d'empêcher tout accès non autorisé :

- Une fois activée, la fonction d'authentification au préamorçage permet d'empêcher l'accès au système d'exploitation.
  - Security Manager for HP ProtectTools—Voir HP ProtectTools Security Manager à la page 26.
  - Drive Encryption for HP ProtectTools—Voir Drive Encryption for HP ProtectTools (certains modèles uniquement) à la page 43.
- Security Manager permet de garantir qu'un utilisateur non autorisé ne peut pas obtenir les mots de passe, ni l'accès aux applications protégées par un mot de passe. Reportez-vous à la section HP ProtectTools Security Manager à la page 26.
- Device Access Manager for HP ProtectTools permet aux responsables informatiques de limiter l'accès aux périphériques inscriptibles de façon à ce que les informations sensibles ne puissent pas être imprimées ou copiées depuis le disque dur. Reportez-vous à la section Device Access Manager pour HP ProtectTools (certains modèles) à la page 52.

Création de règles de mot de passe fort

Si une politique d'entreprise exige que vous utilisiez un mot de passe fort pour une dizaine d'applications et de bases de données Web, Security Manager propose un référentiel sécurisé pour simplifier les mots de passe et l'authentification unique. Reportez-vous à la section HP ProtectTools Security Manager à la page 26.

Éléments de sécurité supplémentaires

Attribution de rôles de sécurité

Dans le cadre de la gestion de la sécurité informatique (en particulier pour les grandes entreprises), une pratique importante consiste à répartir les responsabilités et les droits entre différents types d'administrateur et d'utilisateur.

REMARQUE : Dans une petite entreprise ou dans le cadre d'un usage personnel, ces rôles peuvent tous êtres détenus par la même personne.

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

- Agent de sécurité—Définit le niveau de sécurité de l'entreprise ou du réseau et détermine les fonctions de sécurité à déployer, telles que Drive Encryption.

  REMARQUE : De nombreuses fonctions de HP ProtectTools peuvent être personnalisées par l'agent de sécurité en collaboration avec HP. Pour plus d'informations, accédez à l'adresse http://www.hp.com.
- Administrateur informatique—Applique et gère les fonctions de sécurité définies par l'agent de sécurité. Peut également activer et désactiver certaines fonctions. Ainsi, si l'agent de sécurité a décidé de déployer des cartes Smart Card, l'administrateur informatique peut activer à la fois le mot de passe et le mode Smart Card.
- Utilisateur—Utilise les fonctions de sécurité. Ainsi, si l'agent de sécurité et l'administrateur informatique ont activé les cartes Smart Card du système, l'utilisateur peut définir le code PIN de la carte Smart Card et utiliser cette dernière pour l'authentification.

⚠ **ATTENTION :** Les administrateurs sont encouragés à suivre les « meilleures pratiques » pour limiter les privilèges des utilisateurs finaux et limiter l'accès des utilisateurs.

Les privilèges d'administration ne doivent pas être accordés aux utilisateurs non autorisés.

Gestion des mots de passe HP ProtectTools

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

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

Mot de passe HP ProtectTools	Défini dans le module suivant	Fonction
Mot de passe d'ouverture de session Windows	Panneau de configuration Windows ou HP ProtectTools Security Manager	Peut être utilisé pour la connexion manuelle et pour l'authentification afin d'accéder à diverses fonctions de Security Manager.
Mot de passe de sauvegarde et restauration Security Manager	Security Manager, par chaque utilisateur	Protège l'accès au fichier de sauvegarde et restauration de Security Manager.
Code PIN de la carte Smart Card	Credential Manager	Peut être utilisé pour une authentification multifacteur. Peut être utilisé pour une authentification Windows. Authentifie les utilisateurs de Drive Encryption si la carte Smart Card est sélectionnée.

Création d'un mot de passe sécurisé

Lorsque vous créez des mots de passe, vous devez suivre les spécifications qui sont définies par le programme. En général, tenez toutefois compte des directives suivantes afin de créer des mots de passe forts et de réduire le risque que votre mot de passe soit compromis :

- Utilisez des mots de passe de plus de 6 caractères, et même de préférence de plus de 8 caractères.
- Mélangez les majuscules et les minuscules dans votre mot de passe.
- Si possible, mélangez les caractères alphanumériques et incluez des caractères spéciaux et des signes de ponctuation.
- Remplacez les lettres par des caractères spéciaux ou des nombres dans un mot clé. Par exemple, vous pouvez utiliser le chiffre 1 pour la lettre I ou L.
- Combinez des mots de 2 langues ou plus.
- Insérez des chiffres ou des caractères spéciaux au milieu d'un mot ou d'une expression, par exemple « Mary2-2Cat45 ».
- N'utilisez pas un mot de passe qui figurerait dans un dictionnaire.

- N’utilisez pas votre nom comme mot de passe, ni aucune autre information personnelle, telle que votre date de naissance, des noms d'animaux de compagnie ou le nom de jeune fille de votre mère, même si vous le saisissez à l’envers.
- Modifiez les mots de passe régulièrement. Vous pouvez ne modifier que quelques caractères.
- Si vous notez votre mot de passe, ne le stockez pas à un endroit visible proche de l’ordinateur.
- N’enregistrez pas le mot de passe dans un fichier, tel qu’un message électronique, sur l’ordinateur.
- Ne partagez pas les comptes et ne communiquez votre mot de passe à personne.

Sauvegarde des informations d’authentification et des paramètres

Vous pouvez sauvegarder les informations d’authentification comme suit :

- Utilisez Drive Encryption for HP ProtectTools pour sélectionner et sauvegarder les informations d’authentification HP ProtectTools.
- Utilisez l’outil Sauvegarde et restauration de HP ProtectTools Security Manager comme emplacement central à partir duquel vous pouvez sauvegarder et restaurer les informations d’authentification de sécurité de certains des modules HP ProtectTools installés.

2 Mise en route

Pour configurer les paramètres de HP ProtectTools, utilisez l'Assistant de configuration de HP Client Security ou l'Assistant de configuration de HP ProtectTools Security Manager.

Une fois l'Assistant de configuration de HP Client Security terminé, l'état des applications est affiché sur le tableau de bord de HP Client Security.

Assistant de configuration de HP Client Security

REMARQUE : L'administration de HP ProtectTools nécessite des droits d'administration.

L'assistant de configuration de HP Client Security vous guide tout au long du processus de configuration des fonctions les plus couramment utilisées de Security Manager. Si vous n'avez jamais utilisé l'Assistant de configuration de HP Client Security auparavant, vous pouvez lancer l'Assistant de configuration de HP Client Security en utilisant l'une des méthodes suivantes :

▲ Depuis l'écran Démarrer, cliquez ou tapez sur l'application **HP Client Security**.

– ou –

Depuis le Bureau Windows, cliquez ou tapez sur le gadget **HP ProtectTools**.

Les pages sont affichées dans l'ordre suivant :

1. **Mot de passe Windows**—Entrez votre mot de passe Windows.

   Ceci protège votre compte Windows grâce à une authentification forte.

2. **SpareKey**—Pour activer l'option SpareKey, choisissez trois questions de sécurité.

3. **Inscrire des empreintes digitales**—Si un lecteur d'empreintes digitales et le pilote associé sont installés, vous pouvez inscrire des empreintes digitales. Vous devez sélectionner et inscrire au moins 2 empreintes digitales.

4. **Drive Encryption**—Si Drive Encryption pour HP ProtectTools est installé, vous pouvez activer le cryptage sur l'unité principale :

   - Cryptage logiciel pour un disque dur traditionnel
   - Cryptage matériel si une unité auto-cryptée est détectée.

   Vous devez enregistrer une clé de cryptage sur un ou plusieurs des supports suivants pour que le cryptage soit activé :

   REMARQUE : Si vous annulez l'assistant à ce stade, vous ne pourrez pas activer l'authentification Windows et Drive Encryption.

   - **Support amovible**, comme une clé USB, avec le format FAT 32.
     - Cette option est sélectionnée par défaut si un périphérique amovible est détecté avant que la page Drive Encryption soit affichée.
     - Si 2 périphériques amovibles ou plus sont détectés, sélectionnez l'une des unités affichées.
   - **SkyDrive**—Cette option est disponible si une connexion Internet est détectée.

Un identifiant Windows Live ID® est requis. Entrez votre identifiant et votre mot de passe ou créez-en un.

5. La page Terminer fournit une notification de réussite et vous êtes invité à redémarrer pour activer Drive Encryption.

Assistant de configuration de HP ProtectTools Security Manager

REMARQUE : L'administration de HP ProtectTools nécessite des droits d'administration.

L'Assistant de configuration de HP ProtectTools Security Manager vous guide au cours des étapes de configuration de Security Manager. Outre les paramètres disponibles dans l'assistant, les administrateurs peuvent configurer de nombreuses fonctions de sécurité supplémentaires via la console d'administration. Ces paramètres s'appliquent à l'ordinateur et à tous les utilisateurs qui le partagent.

Pour lancer l'Assistant de configuration de HP ProtectTools Security Manager :

▲ Cliquez sur **Assistant de configuration** dans le volet gauche de la Console d'administration, puis suivez les instructions à l'écran jusqu'à ce que la configuration soit terminée.

Les administrateurs peuvent accéder à la Console d'administration depuis la console utilisateur de HP ProtectTools Security Manager. Pour plus d'informations, reportez-vous à la section Console d'administration de HP ProtectTools Security Manager à la page 15.

Security Manager et ses applications sont accessibles à tous les utilisateurs partageant cet ordinateur.

Tableau de bord de HP Client Security

Pour ouvrir HP Client Security si vous avez déjà utilisé l'Assistant de configuration de HP Client Security auparavant :

▲ Depuis l'écran Démarrer, tapez `hp` puis sélectionnez **HP Client Security**.

Le tableau de bord affiche une présentation rapide des fonctionnalités et de l'état associé pour chaque application.

▲ Cliquez ou tapez sur une ligne d'application pour afficher plus d'informations sur l'application sélectionnée :

- Le bouton **Configurer maintenant** indique que l'application en question n'est pas encore configurée. Cliquez ou tapez sur le bouton pour ouvrir la page de l'application afin de configurer l'application.
- Le bouton **Paramètres** indique que l'application en question possède un statut OK. Cliquez ou tapez sur le bouton pour accéder aux paramètres de l'application.
- La **Console utilisateur** est lancée pour effectuer une configuration utilisateur.
- La **Console d'administration** est lancée pour effectuer une configuration utilisateur nécessitant des droits d'administrateur.
- Le **tableau de bord État** reste ouvert après le lancement de la Console utilisateur ou de la Console d'administration et une fois que vous avez configuré les paramètres et fermé la Console, l'état est actualisé.

3 Guide de configuration facile pour les petites entreprises

Ce chapitre est conçu pour démontrer les étapes de base à suivre afin d'activer les options les plus courantes et les plus utiles de HP ProtectTools for Small Business. Les nombreux outils et options disponibles dans ce logiciel vous permettent d'affiner vos préférences et de définir le contrôle d'accès. Ce Guide de configuration rapide vise à vous permettre d'exécuter chaque module le plus rapidement et avec le moins de travail de configuration possible. 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 actuellement affichée.

Mise en route

1. Sur le Bureau Windows, ouvrez HP ProtectTools Security Manager en double-cliquant sur l'icône **HP ProtectTools** dans la zone de notification située à l'extrémité droite de la barre des tâches.
2. Entrez votre mot de passe Windows ou créez-en un.
3. Exécutez l'assistant de configuration.

REMARQUE : Par défaut, HP ProtectTools Security Manager est défini sur la règle d'authentification forte.

Ce paramètre est conçu pour empêcher tout accès non autorisé lorsque les utilisateurs sont connectés à Windows et il doit être utilisé lorsqu'un niveau de sécurité élevé est nécessaire ou si des utilisateurs s'éloignent fréquemment de leur système au cours de la journée. Si vous souhaitez modifier ce paramètre, cliquez sur l'onglet Règles de session et faites les sélections voulues.

Pour que HP ProtectTools Security Manager n'exige qu'une seule authentification lors de l'ouverture de session Windows, suivez la procédure suivante.

1. Sur le Bureau Windows, ouvrez HP ProtectTools Security Manager en double-cliquant sur l'icône **HP ProtectTools** dans la zone de notification située à l'extrémité droite de la barre des tâches.
2. Dans le panneau de gauche, cliquez sur **Administration**, puis sur **Console d'administration**.
3. Dans le panneau de gauche, sous **Système**, sélectionnez **Authentification** dans le groupe **Sécurité**.
4. Cliquez sur l'onglet **Règles de session**, puis sélectionnez les exigences de combinaison d'ouverture de session. Pour annuler les options sélectionnées, cliquez sur **Restaurer les valeurs par défaut**.
5. Cliquez sur le bouton **Appliquer** lorsque vous avez fini.

Password Manager

Mots de passe ! Nous avons tous de nombreux mots de passe, notamment pour les sites Web régulièrement consultés ou lorsque nous utilisons des applications qui exigent une authentification. L'utilisateur normal utilise le même mot de passe pour toutes les applications et les sites Web ou il est vraiment créatif mais oublie rapidement le mot de passe correspondant à telle ou telle application.

Le Gestionnaire de mots de passe peut se rappeler automatiquement de vos mots de passe ou vous donner la possibilité de choisir les sites à mémoriser et ceux à omettre. Lorsque vous vous connectez sur un ordinateur, le Gestionnaire de mots de passe vous fournit les mots de passe ou les informations d'authentification permettant d'accéder aux applications ou aux sites Web.

Lorsque vous accédez à une application ou un site Web exigeant des données d'authentification, Password Manager reconnaît automatiquement le site et vous demande si vous voulez que le logiciel mémorise vos informations. Si vous voulez exclure certains sites, vous pouvez refuser la demande.

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

1. Par exemple, accédez à un site Web ou à une application, puis cliquez sur l'icône Gestionnaire de mots de passe dans le coin supérieur gauche de la page Web pour ajouter l'authentification Web.
2. Nommez le lien (facultatif) et entrez un nom d'utilisateur et un mot de passe dans Password Manager.

REMARQUE : Les zones que Password Manager va utiliser maintenant, ainsi que lors des visites ultérieures, sont mises en surbrillance.

3. Lorsque vous avez fini, cliquez sur le bouton **OK**.
4. Password Manager peut également enregistrer votre nom d'utilisateur et vos mots de passe pour les partages réseau ou les unités réseau mappées.

Affichage et gestion des authentifications enregistrées dans Password Manager

Password Manager vous permet d'afficher, gérer, sauvegarder et lancer vos authentifications depuis un emplacement central. Password Manager prend également en charge le lancement de sites enregistrés à partir de Windows.

Pour ouvrir Password Manager, utilisez l'une des deux méthodes suivantes :

- Utilisez la combinaison de touches ctrl+touche logo Windows+h pour ouvrir Password Manager, puis cliquez sur **Ouvrir** pour lancer et authentifier le raccourci enregistré.

  – ou –

- Sélectionnez l'onglet **Gérer** du Gestionnaire de mots de passe pour ouvrir HP ProtectTools Security Manager afin de modifier les informations d'authentification.

L'option **Modifier** du Gestionnaire de mots de passe 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 de sauvegarder et/ou de copier toutes les informations d'authentification et les paramètres sur un autre ordinateur.

Device Access Manager for HP ProtectTools

Device Access Manager permet de limiter l'utilisation de divers périphériques de stockage internes et externes afin que vos données restent sécurisées sur le disque dur et ne risquent pas de sortir 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 mémoire USB. Une procédure de configuration facile est fournie ci-après.

1. Sur le Bureau Windows, ouvrez la console utilisateur de HP ProtectTools Security Manager en double-cliquant sur l'icône **HP ProtectTools** dans la zone de notification située à l'extrémité droite de la barre des tâches.
2. Dans le volet gauche de HP ProtectTools Security Manager, cliquez sur **Administration**, puis sur **Console d'administration**.
3. Cliquez sur **Device Access Manager**, puis sur **Configuration de classe de périphérique**.
4. L'étape suivante consiste à sélectionner les utilisateurs qui pourront continuer à y avoir accès alors que tous les autres seront bloqués.
5. Sélectionnez les périphériques matériels auxquels limiter l'accès, puis cliquez sur le bouton **Appliquer** pour terminer la procédure.
6. Sélectionnez **Ajouter**, cliquez sur **Avancés** puis sur **Rechercher maintenant**.
7. Sélectionnez l'utilisateur de votre choix, puis cliquez sur **OK > OK > Appliquer**.

   Votre choix apparaît dans la zone **Utilisateurs ou groupes**.
8. Sélectionnez la **Classe de périphérique** utilisée par l'utilisateur, sélectionnez **Autoriser** ou **Refuser**, puis cliquez sur **Appliquer**.

Drive Encryption for HP ProtectTools

Drive Encryption for HP ProtectTools vous permet de protéger vos données en cryptant le disque dur entier. Les données du disque dur resteront ainsi protégées même si votre PC est volé et/ou si le disque dur est retiré de l'ordinateur d'origine et placé dans un autre ordinateur.

Sur le plan de la sécurité, l'autre avantage est que Drive Encryption exige une authentification correcte, avec le nom d'utilisateur et le mot de passe avant que le système d'exploitation démarre. Ce processus est appelé authentification au préamorçage.

Pour vous faciliter les choses, plusieurs modules logiciels synchronisent automatiquement les mots de passe, y compris les comptes utilisateurs Windows, les domaines, Drive Encryption for HP ProtectTools, Password Manager et HP ProtectTools Security Manager.

Utilisez la procédure simple suivante pour activer Drive Encryption for HP ProtectTools :

1. Sur le Bureau Windows, ouvrez HP ProtectTools Security Manager en double-cliquant sur l'icône **HP ProtectTools** dans la zone de notification située à l'extrémité droite de la barre des tâches.
2. Dans le panneau de gauche, cliquez sur **Administration**, puis sur **Console d'administration**.
3. Dans le volet gauche, cliquez sur **Assistant de configuration**.
4. Sélectionnez **Suivant** dans l'écran d'accueil.
5. Entrez votre mot de passe Windows pour lancer l'assistant d'activation, puis cliquez sur **Suivant**.

6. Ignorez SpareKey si cette option n’est pas souhaitée.
7. Cochez la case **Drive Encryption**, puis cliquez sur **Suivant**.
8. Cochez l’unité à crypter, puis cliquez sur **Suivant**.
9. La fenêtre de configuration de Drive Encryption nécessite l'utilisation d'une clé USB ou d'un autre périphérique externe pour stocker la clé de récupération de chiffrement. Stockez cette clé de récupération en vous assurant de sa sécurité car elle sert à récupérer les données ou à accéder au lecteur si le mot de passe de pré-amorçage est oublié ou échoue.
10. Cliquez sur **Suivant**, terminez la procédure, puis cliquez sur **Terminer**. Retirez l’unité flash USB, puis redémarrez l’ordinateur lorsque vous êtes prêt.
11. Lorsque le système démarre, Drive Encryption vous demande votre mot de passe Windows. Entrez le mot de passe, puis cliquez sur **OK**.

REMARQUE : Il est possible que l'ordinateur soit ralenti lorsque le lecteur est en cours de cryptage. Une fois le cryptage terminé, les performances redeviennent normales. En cas d'accès aux données présentes sur le lecteur, les données sont cryptées ou décryptées conformément aux exigences de l'administrateur.

L'authentification de Drive Encryption « ignore » la connexion Windows et affiche directement le Bureau Windows de sorte que vous n'avez pas à entrer votre mot de passe une seconde fois.

4 Console d'administration de HP ProtectTools Security Manager

Le logiciel HP ProtectTools Security Manager fournit des fonctions de sécurité conçues pour empêcher tout accès non autorisé à l'ordinateur, aux réseaux et aux données critiques. L'administration de HP ProtectTools Security Manager est fournie via la fonction Console d'administration.

D'autres applications sont disponibles dans la Console utilisateur de Security Manager pour vous permettre de récupérer les données de l'ordinateur en cas de perte ou de vol (sur certains modèles uniquement).

La Console d'administration permet à l'administrateur local d'effectuer les tâches suivantes :

- Activation ou désactivation des fonctions de sécurité
- Spécification des informations de connexion requises pour l'authentification
- Gestion des utilisateurs de l'ordinateur
- Réglage des paramètres spécifiques aux périphériques
- Configuration des applications de Security Manager installées

Mise en route

Pour configurer les paramètres de HP ProtectTools, utilisez l'Assistant de configuration de HP Client Security ou l'Assistant de configuration de HP ProtectTools Security Manager.

Une fois l'Assistant de configuration de HP Client Security terminé, l'état des applications est affiché sur le tableau de bord de HP Client Security.

Assistant de configuration de HP Client Security

REMARQUE : L'administration de HP ProtectTools nécessite des droits d'administration.

L'assistant de configuration de HP Client Security vous guide tout au long du processus de configuration des fonctions les plus couramment utilisées de Security Manager. Si vous n'avez jamais utilisé l'Assistant de configuration de HP Client Security auparavant, vous pouvez lancer l'Assistant de configuration de HP Client Security en utilisant l'une des méthodes suivantes :

▲ Depuis l'écran Démarrer, cliquez ou tapez sur l'application **HP Client Security**.

– ou –

Depuis le Bureau Windows, cliquez ou tapez sur le gadget **HP ProtectTools**.

Les pages sont affichées dans l'ordre suivant :

1. **Mot de passe Windows**—Entrez votre mot de passe Windows.

   Ceci protège votre compte Windows grâce à une authentification forte.

2. **SpareKey**—Pour activer l'option SpareKey, choisissez trois questions de sécurité.

3. **Inscrire des empreintes digitales**—Si un lecteur d'empreintes digitales et le pilote associé sont installés, vous pouvez inscrire des empreintes digitales. Vous devez sélectionner et inscrire au moins 2 empreintes digitales.

4. **Drive Encryption**—Si Drive Encryption pour HP ProtectTools est installé, vous pouvez activer le cryptage sur l'unité principale :

   - Cryptage logiciel pour un disque dur traditionnel
   - Cryptage matériel si une unité auto-cryptée est détectée.

   Vous devez enregistrer une clé de cryptage sur un ou plusieurs des supports suivants pour que le cryptage soit activé :

   REMARQUE : Si vous annulez l'assistant à ce stade, vous ne pourrez pas activer l'authentification Windows et Drive Encryption.

   - **Support amovible**, comme une clé USB, avec le format FAT 32.
     - Cette option est sélectionnée par défaut si un périphérique amovible est détecté avant que la page Drive Encryption soit affichée.
     - Si 2 périphériques amovibles ou plus sont détectés, sélectionnez l'une des unités affichées.
   - **SkyDrive**—Cette option est disponible si une connexion Internet est détectée.

     Un identifiant Windows Live ID® est requis. Entrez votre identifiant et votre mot de passe ou créez-en un.

5. La page Terminer fournit une notification de réussite et vous êtes invité à redémarrer pour activer Drive Encryption.

Assistant de configuration de HP ProtectTools Security Manager

REMARQUE : L'administration de HP ProtectTools nécessite des droits d'administration.

L'Assistant de configuration de HP ProtectTools Security Manager vous guide au cours des étapes de configuration de Security Manager. Outre les paramètres disponibles dans l'assistant, les administrateurs peuvent configurer de nombreuses fonctions de sécurité supplémentaires via la console d'administration. Ces paramètres s'appliquent à l'ordinateur et à tous les utilisateurs qui le partagent.

Pour lancer l'Assistant de configuration de HP ProtectTools Security Manager :

▲ Cliquez sur **Assistant de configuration** dans le volet gauche de la Console d'administration, puis suivez les instructions à l'écran jusqu'à ce que la configuration soit terminée.

Les administrateurs peuvent accéder à la Console d'administration depuis la console utilisateur de HP ProtectTools Security Manager. Pour plus d'informations, reportez-vous à la section Console d'administration de HP ProtectTools Security Manager à la page 15.

Security Manager et ses applications sont accessibles à tous les utilisateurs partageant cet ordinateur.

Tableau de bord de HP Client Security

Pour ouvrir HP Client Security si vous avez déjà utilisé l'Assistant de configuration de HP Client Security auparavant :

▲ Depuis l'écran Démarrer, tapez `hp` puis sélectionnez **HP Client Security**.

Le tableau de bord affiche une présentation rapide des fonctionnalités et de l'état associé pour chaque application.

▲ Cliquez ou tapez sur une ligne d'application pour afficher plus d'informations sur l'application sélectionnée :

- Le bouton **Configurer maintenant** indique que l'application en question n'est pas encore configurée. Cliquez ou tapez sur le bouton pour ouvrir la page de l'application afin de configurer l'application.
- Le bouton **Paramètres** indique que l'application en question possède un statut OK. Cliquez ou tapez sur le bouton pour accéder aux paramètres de l'application.
- La **Console utilisateur** est lancée pour effectuer une configuration utilisateur.
- La **Console d'administration** est lancée pour effectuer une configuration utilisateur nécessitant des droits d'administrateur.
- Le **tableau de bord État** reste ouvert après le lancement de la Console utilisateur ou de la Console d'administration et une fois que vous avez configuré les paramètres et fermé la Console, l'état est actualisé.

Ouverture de la console d'administration de HP ProtectTools

Utilisez la Console d'administration HP ProtectTools pour les tâches d'administration, comme définir des stratégies système ou configurer le logiciel. Accédez à la Console d'administration en ouvrant HP ProtectTools Security Manager :

1. Sur le bureau Windows, double-cliquez sur l'icône **HP ProtectTools** dans la zone de notification, située à l'extrémité droite de la barre des tâches.

   – ou –

   Dans le **Panneau de configuration**, sélectionnez **Système et sécurité**, puis sélectionnez **HP ProtectTools Security Manager**.

2. Dans le panneau de gauche de la Console utilisateur de Security Manager, cliquez sur **Administration**, puis sur **Console d'administration**.

Utilisation de la console d'administration

La console d'administration de HP ProtectTools est l'emplacement qui centralise l'administration des fonctions et applications de HP ProtectTools Security Manager.

1. Sur le bureau Windows, double-cliquez sur l'icône **HP ProtectTools** dans la zone de notification, située à l'extrémité droite de la barre des tâches.

   – ou –

   Dans le **Panneau de configuration**, sélectionnez **Système et sécurité**, puis sélectionnez **HP ProtectTools Security Manager**.

2. Dans le panneau de gauche de la Console utilisateur de Security Manager, cliquez sur **Administration**, puis sur **Console d'administration**.

Les options suivantes sont affichées dans le panneau gauche de la console d'administration, sous Accueil :

- **Système**—Vous permet de configurer les fonctions de sécurité suivantes et l'authentification pour les utilisateurs et les périphériques.
  - **Sécurité**
  - **Utilisateurs**
  - **Informations d'authentification**
- **Applications**—Vous permet de configurer les paramètres de HP ProtectTools Security Manager et des applications de Security Manager.
- **Données**—Vous permet de configurer les paramètres de Drive Encryption (sur certains modèles uniquement).
- **Ordinateur**—vous permet de configurer les paramètres de Device Access Manager.
- **Assistant de configuration**—Vous guide au cours des étapes de configuration de HP ProtectTools Security Manager.
- **À propos de**—Affiche des informations sur HP ProtectTools Security Manager, telles que le numéro de version et la mention des droits d'auteur.
- **Zone principale**—Affiche les écrans spécifiques aux applications.

  ?—Affiche l'aide de la Console d'administration. Cette icône se trouve dans la partie supérieure droite du cadre de la fenêtre, à côté des icônes d'agrandissement et de réduction.

Configuration de votre système

Le groupe **Système** est accessible via le panneau du menu situé à gauche de la console d'administration de HP ProtectTools. Vous pouvez utiliser les applications de ce groupe pour gérer les règles et les paramètres de l'ordinateur, ses utilisateurs et ses périphériques.

Les applications suivantes sont incluses dans le groupe **Système** :

- **Sécurité**—Gérez les fonctions, l'authentification et les paramètres régissant la manière dont les utilisateurs interagissent avec cet ordinateur.
- **Utilisateurs**—Configurez, gérez et enregistrez des utilisateurs pour cet ordinateur.
- **Informations d'authentification**—Gérez les paramètres des périphériques de sécurité intégrés ou connectés à l'ordinateur et configurez les paramètres.

Configuration de l'authentification pour votre ordinateur

Dans l'application Authentification, vous pouvez définir les règles d'accès à l'ordinateur. Vous pouvez spécifier les informations d'authentification nécessaires à l'authentification de chaque classe d'utilisateurs lors de la connexion à Windows ou à des sites Web et des programmes au cours d'une session utilisateur.

Pour configurer l'authentification sur votre ordinateur :

1. Dans le panneau gauche de la console d'administration, cliquez sur **Sécurité**, puis sur **Authentification**.
2. Pour configurer l'authentification de la connexion, cliquez sur l'onglet **Règles de connexion**, effectuez les modifications, puis cliquez sur **Appliquer**.
3. Pour configurer l'authentification de la session, cliquez sur l'onglet **Règles de session**, effectuez les modifications, puis cliquez sur **Appliquer**.

Règles de connexion

Pour définir les règles relatives aux informations requises pour l'authentification d'un utilisateur lors de la connexion à Windows :

1. Dans le panneau de gauche de la console d'administration, cliquez sur **Sécurité**, puis sur **Authentification**.
2. Dans l'onglet **Règle de connexion**, sélectionnez une catégorie d'utilisateur, telle que utilisateurs Administrateurs ou Standard.
3. Cliquez sur une information d'authentification pour afficher la boîte de dialogue de modification.
4. Pour demander une combinaison de deux informations d'authentification, cliquez sur la flèche vers le bas pour sélectionner chaque information d'authentification requise, puis cliquez sur **OK**.
5. Pour supprimer une information d'authentification, cliquez sur **X** ou cliquez avec le bouton droit de la souris sur l'information d'authentification à supprimer, puis cliquez sur **Supprimer**.
6. Cliquez sur **Oui** dans la boîte de dialogue de configuration.
7. Pour confirmer si les utilisateurs peuvent se connecter, cliquez sur **Vérifiez si les utilisateurs HP ProtectTools peuvent se connecter**.
8. Pour rétablir les paramètres par défaut, cliquez sur **Restaurer les valeurs par défaut**.
9. Cliquez sur **Appliquer**.

Règles de session

Pour définir les règles relatives aux informations d'authentification requises pour procéder à l'authentification au cours d'une session Windows :

1. Dans le panneau de gauche de la console d'administration, cliquez sur **Sécurité**, puis sur **Authentification**.
2. Dans l'onglet **Règle de session**, sélectionnez une catégorie d'utilisateur, telle que utilisateurs Administrateurs ou Standard.
3. Cliquez sur une information d'authentification pour afficher la boîte de dialogue de modification.
4. Pour demander une combinaison de deux informations d'authentification, cliquez sur la flèche vers le bas pour sélectionner chaque information d'authentification requise, puis cliquez sur **OK**.
5. Pour supprimer une information d'authentification, cliquez sur **X** ou cliquez avec le bouton droit de la souris sur l'information d'authentification à supprimer, puis cliquez sur **Supprimer**.
6. Cliquez sur **Oui** dans la boîte de dialogue de configuration.
7. Pour confirmer si les utilisateurs peuvent se connecter, cliquez sur **Vérifiez si les utilisateurs HP ProtectTools peuvent se connecter**.

8. Pour rétablir les paramètres par défaut, cliquez sur **Restaurer les valeurs par défaut**.
9. Cliquez sur **Appliquer**.

Paramètres

Pour permettre aux utilisateurs de cet ordinateur d'ignorer la connexion Windows si l'authentification a déjà été effectuée au niveau du BIOS ou de Drive Encryption :

1. Dans le panneau gauche de la console d'administration, cliquez sur **Sécurité**, puis sur **Paramètres**.
2. **Autoriser la connexion directe**—Cochez cette case pour activer la connexion directe ou décochez-la pour la désactiver.
3. Cliquez sur **Appliquer**.

Gestion des utilisateurs

Dans l'application Utilisateurs, vous pouvez contrôler et gérer les utilisateurs de HP ProtectTools sur cet ordinateur.

Tous les utilisateurs de HP ProtectTools sont répertoriés et comparés aux règles définies via Security Manager. Il est également vérifié s'ils ont enregistré les bonnes informations d'authentification, ce qui leur permet de respecter ces règles.

Pour gérer les utilisateurs, sélectionnez au choix les options suivantes :

- Pour ajouter des utilisateurs supplémentaires, cliquez sur **Ajouter**.
- Pour supprimer un utilisateur, cliquez sur celui-ci, puis sur **Supprimer**.
- Pour configurer des informations d'authentification supplémentaires pour l'utilisateur, cliquez sur celui-ci, puis sur **Inscrire**.
- Pour afficher les règles d'un utilisateur spécifique, sélectionnez-le, puis affichez les règles dans la partie inférieure de la fenêtre.

Informations d'authentification

Dans l'application Informations d'authentification, vous pouvez configurer les paramètres disponibles pour tous les périphériques de sécurité intégrés ou connectés reconnus par HP ProtectTools Security Manager.

SpareKey

Vous pouvez autoriser ou refuser l'authentification SpareKey pour la connexion Windows et gérer les questions de sécurité qui seront posées aux utilisateurs lors de leur inscription à SpareKey.

1. Sélectionnez les questions de sécurité qui seront posées aux utilisateurs lors de leur inscription à SpareKey.

   Vous pouvez définir jusqu'à trois questions personnalisées ou vous pouvez permettre aux utilisateurs de saisir leur propre phrase de passe.
2. Pour autoriser la récupération de SpareKey pour la connexion Windows, cochez la case.
3. Cliquez sur **Appliquer**.

Empreintes digitales

Si un lecteur d'empreintes digitales est installé ou connecté à l'ordinateur, la page Empreintes digitales affiche les onglets suivants :

- **Inscription**—Choisissez le nombre minimum et maximum d'empreintes digitales qu'un utilisateur est autorisé à inscrire.

  Vous pouvez également effacer toutes les données du lecteur d'empreintes digitales.

  ATTENTION : Si vous effacez toutes les données du lecteur d'empreintes, les empreintes digitales de tous les utilisateurs sont effacées, y compris celles des administrateurs. Si les règles de connexion requièrent uniquement des empreintes digitales, cette suppression risque d'empêcher tous les utilisateurs de se connecter à l'ordinateur.

- **Sensibilité**—Déplacez le curseur pour ajuster la sensibilité utilisée par le lecteur d'empreintes digitales lorsque vous faites glisser vos empreintes digitales.

  Si votre empreinte digitale n'est pas reconnue à chaque passage, vous pouvez sélectionner un paramètre de sensibilité inférieur. Un paramètre plus haut augmente la sensibilité aux variations dans les passage d'empreinte digitale et par conséquent diminue la possibilité d'une fausse acceptation. Le paramètre **Moyen-Haut** fournit une bonne engeance de sécurité et de commodité.

- **Avancé**—Sélectionnez une des options suivantes pour configurer le lecteur d'empreintes digitales afin qu'il économise de l'énergie et améliore le retour visuel :

  - **Optimisé**—Le lecteur d'empreintes digitales est activé lorsque cela s'avère nécessaire. Vous pourrez constater un court délai lorsque le lecteur est utilisé pour la première fois.
  - **Economie d'énergie**—Le lecteur d'empreintes digitales est plus lent à répondre, mais le paramètre nécessite moins d'énergie.
  - **Mode normal**—Le lecteur d'empreintes digitales est toujours prêt à être utilisé, mais ce paramètre utilise un maximum d'énergie.

Visage

Si une webcam est installée ou connectée à l'ordinateur, et si le programme Face Recognition est installé, les administrateurs peuvent définir le niveau de sécurité de Face Recognition pour rechercher un équilibre entre la facilité d'utilisation et la sécurité de l'ordinateur.

1. Cliquez sur **Informations d'authentification**, puis sur **Visage**.
2. Pour plus de convivialité, cliquez sur le curseur pour le déplacer vers la gauche, ou pour plus de précision, cliquez sur le curseur pour le déplacer vers la droite.

   - **Convivialité**—Pour faciliter l'accès aux utilisateurs inscrits dans des situations marginales, cliquez sur la barre du curseur pour le déplacer vers la position **Convivialité**.
   - **Equilibre**—Pour assurer un bon compromis entre sécurité et convivialité, ou si vous disposez d'informations sensibles ou que votre ordinateur est situé dans une zone où des accès non autorisés peuvent avoir lieu, cliquez sur la barre du curseur pour le déplacer vers la position **Equilibre**.
   - **Précision**—Pour rendre plus difficile l'accès aux utilisateurs si les scènes enregistrées ou les conditions d'éclairage en cours se situent à un niveau inférieur à la normale et qu'il est peu probable qu'une acceptation erronée se produise, cliquez sur la barre du curseur pour le déplacer vers la position **Précision**.

3. Pour rétablir les paramètres sur leurs valeurs par défaut, cliquez sur **Restaurer les valeurs par défaut**.
4. Cliquez sur **Appliquer**.

Smart Card

Les administrateurs doivent initialiser la carte Smart Card avant de pouvoir l'utiliser pour l'authentification. La plupart des cartes Smart Card CSP et PKCS11 sont prises en charge sous Windows.

Initialisation de la Smart Card

HP ProtectTools Security Manager peut prendre en charge plusieurs Smart Card. Le nombre et le type des caractères utilisés pour le code PIN peuvent varier. Le fabricant de la Smart Card doit fournir des outils pour installer un certificat de sécurité et gérer le code PIN que HP ProtectTools utilisera dans son algorithme de sécurité.

REMARQUE : Le logiciel médiateur de la carte Smart Card doit être installé.

1. Procurez-vous et installez le logiciel médiateur de la carte Smart Card utilisée (par exemple ActivClient 6.x pour une carte Smart Card ActivIdentity).
2. Insérez la carte Smart Card dans le lecteur.
3. Initialisez (formatez) la carte Smart Card.
   a. Lancez l'outil d'initialisation de la carte Smart Card, ou il peut s'afficher lorsque vous insérez la carte Smart Card dans le lecteur.
   b. Suivez les instructions à l'écran pour configurer un code PIN.
   c. Notez le code de déblocage pour pouvoir vous y référer ultérieurement.
4. Créez une paire de clés et un certificat.
   a. Ouvrez la **Console d'administration de HP ProtectTools**.
   b. Cliquez sur **Informations d'authentification**, puis sur **Smart Card** et enfin sur l'onglet **Administration**.
   c. Assurez-vous que l'option **Initialiser la carte Smart Card** est sélectionnée.
   d. Saisissez votre code PIN, cliquez sur **Appliquer**, puis suivez les instructions à l'écran.

   Après avoir correctement initialisé la carte Smart Card, vous devez l'enregistrer.

Enregistrement de la Smart Card

Après avoir initialiser la Smart Card, les administrateurs peuvent l'enregistrer comme méthode d'authentification dans la console d'administration de HP ProtectTools :

1. Cliquez sur **Assistant de configuration**.
2. Dans l'écran **Bienvenue**, cliquez sur **Suivant**.
3. Entrez votre mot de passe Windows, puis cliquez sur **Suivant**.
4. Sur la page **SpareKey**, cliquez sur **Ignorer la configuration de SpareKey** (sauf si vous souhaitez mettre à jour les informations SpareKey), puis cliquez sur **Suivant**.
5. Sur la page **Activer les fonctions de Sécurité**, cliquez sur **Suivant**.

6. Sur la page **Choisissez vos informations d'authentification**, assurez-vous que l'option **Smart Card** est sélectionnée, puis cliquez sur **Suivant**.
7. Sur la page **Smart card**, saisissez votre code PIN, puis cliquez sur **Suivant**.
8. Cliquez sur **Terminer**.

Les utilisateurs peuvent également enregistrer une carte Smart Card dans la Console utilisateur de Security Manager. Pour plus d'informations, reportez-vous à l'aide du logiciel de HP ProtectTools Security Manager en cliquant sur l'icône **?** bleue située dans la partie supérieure droite de la page Smart Card.

Configuration de la Smart Card

Si un lecteur Smart Card est installé ou connecté à l'ordinateur, la page Smart Card affiche les onglets suivants :

- **Paramètres**—Cochez la case **Verrouiller l'ordinateur après le retrait de la carte Smart Card** pour configurer l'ordinateur afin qu'il se verrouille automatiquement lorsqu'une carte Smart Card est retirée, puis cliquez sur **Appliquer**.

REMARQUE : L'ordinateur ne se verrouille que si la Smart Card a été utilisée comme information d'authentification lors de la connexion à Windows. Le retrait d'une Smart Card n'ayant pas été utilisée pour se connecter à Windows ne verrouille pas l'ordinateur.

- **Administration**—Sélectionnez parmi les options suivantes :
  - **Initialiser la carte Smart Card**—Prépare une carte Smart Card pour une utilisation avec HP ProtectTools. Si une Smart Card a été précédemment initialisée en dehors de HP ProtectTools (avec une paire de clés asymétriques et un certificat associé), elle n'a pas besoin d'être initialisée à nouveau, sauf si une initialisation avec un certificat spécifique est nécessaire.
  - **Modifier le code PIN de la carte Smart Card**—Vous permet de modifier le code PIN utilisé avec la carte Smart Card.
  - **Effacer uniquement les données HP ProtectTools**—Efface uniquement le certificat HP ProtectTools créé lors de l'initialisation de la carte. Aucune autre donnée ne sera effacée de la carte.
  - **Effacer toutes les données de la carte Smart Card**—Efface toutes les données de la carte Smart Card spécifiée. Vous ne pourrez plus utiliser la carte avec HP ProtectTools ou toute autre application.

REMARQUE : Les fonctions qui ne sont pas prises en charge par votre carte Smart Card ou l'intergiciel associé ne sont pas disponibles.

▲ Cliquez sur **Appliquer**.

Carte sans contact

Une carte sans contact est une petite carte en plastique avec une puce informatique intégrée. Si un lecteur de cartes sans contact est connecté à l'ordinateur et le pilote fourni par le fabricant installé, et si vous avez sélectionné une carte sans contact comme informations d'authentification, vous pouvez

utiliser votre carte sans contact pour l'authentification. Les types de carte sans contact suivants sont pris en charge par HP ProtectTools :

- cartes mémoires sans contact iCLASS HID ;
- cartes mémoires sans contact MiFare Classic 1k et 4k, et mini cartes mémoires sans contact.

▲ Pour configurer votre carte sans contact, placez-la tout près du lecteur et suivez les instructions à l'écran, puis cliquez sur **Appliquer**.

Carte de proximité

Une carte de proximité est une petite carte en plastique avec une puce informatique intégrée. Si un lecteur de cartes de proximité est connecté à l'ordinateur et le pilote fourni par le fabricant est installé, et si vous avez sélectionné une carte de proximité comme information d'authentification, vous pouvez utiliser une carte de proximité en conjonction avec d'autres informations d'authentification pour plus de sécurité.

▲ Pour configurer votre carte de proximité, placez-la tout près du lecteur, puis cliquez sur **Appliquer**.

Bluetooth

Si l'ordinateur est équipé de la fonctionnalité Bluetooth® et que vous avez sélectionné Bluetooth comme information d'authentification, et si un téléphone Bluetooth est associé à l'ordinateur, vous pouvez utiliser votre téléphone Bluetooth en conjonction avec d'autres informations d'authentification pour plus de sécurité. Spécifiez les paramètres Bluetooth :

▲ Pour autoriser l'authentification silencieuse, cochez la case correspondante, puis cliquez sur **Appliquer**.

PIN

Si vous avez sélectionné PIN comme information d'authentification, vous pouvez utiliser un code PIN en conjonction avec d'autres informations d'authentification pour plus de sécurité. Spécifiez les paramètres du code PIN :

1. Sélectionnez la longueur minimale du code PIN en cliquant sur la flèche vers le haut ou vers le bas.

   La longueur du code est limitée à 8 chiffres maximum.

2. Cliquez sur **Appliquer**.

Applications

La page Paramètres, sous Applications dans le panneau gauche de la console d'administration, comprend deux onglets qui vous permettent de personnaliser le comportement des applications HP ProtectTools Security Manager installées.

▲ Dans le panneau de gauche de la console d'administration, sous **Applications**, cliquez sur **Paramètres**.

Onglet Général

Les paramètres suivants sont disponibles dans l'onglet **Général** :

- **Ne pas lancer automatiquement l'Assistant de configuration pour les administrateurs**—Sélectionnez cette option pour empêcher l'assistant de s'ouvrir automatiquement à la connexion.
- **Ne pas lancer automatiquement l'assistant de mise en route pour les utilisateurs**—Sélectionnez cette option pour empêcher la configuration utilisateur de s'ouvrir automatiquement à la connexion.

1. Sélectionnez la case à cocher en regard d'un paramètre spécifique pour l'activer ou désélectionnez-la pour le désactiver.
2. Cliquez sur **Appliquer**.

Onglet Applications

Les administrateurs peuvent activer ou désactiver les applications suivantes :

- **État**—Cochez cette case pour activer toutes les applications ou décochez-la pour toutes les désactiver.
- **Gestionnaire de mots de passe**—Active le Gestionnaire de mots de passe pour tous les utilisateurs de l'ordinateur.

1. Sélectionnez la case à cocher en regard d'un paramètre spécifique pour l'activer ou désélectionnez-la pour le désactiver.
2. Cliquez sur **Appliquer**.

Pour restaurer les paramètres d'usine de toutes les applications, cliquez sur **Restaurer les valeurs par défaut**.

Données

La partie Données du panneau gauche de la Console d'administration vous permet de configurer les paramètres des applications suivantes :

- **Drive Encryption**—Configurez les paramètres et affichez l'état de l'unité. Pour plus d'informations, reportez-vous à l'aide du logiciel Drive Encryption en cliquant sur l'icône **?** bleue située dans la partie supérieure droite de la page Drive Encryption.

Ordinateur

La partie Ordinateur du panneau gauche de la console d'administration vous permet de configurer les paramètres de l'application Device Access Manager :

- Configuration simple
- Configuration de classe de périphérique
- Configuration de l'authentification Just-In-Time (JIT)
- Paramètres avancés

Pour plus d'informations, consultez l'aide du logiciel Device Access Manager en cliquant sur l'icône bleue **?** située dans la partie supérieure droite de la page Device Access Manager.

5 HP ProtectTools Security Manager

HP ProtectTools Security Manager vous permet d'améliorer considérablement la sécurité de votre ordinateur.

Vous pouvez utiliser des applications Security Manager préchargées, ainsi que des applications supplémentaires disponibles pour un téléchargement immédiat sur le Web :

- Gérer votre connexion et vos mots de passe.
- Changer aisément le mot de passe du système d'exploitation Windows®.
- Définir des préférences de programme.
- Utiliser les empreintes digitales pour une sécurité et un confort accrus.
- Enregistrer une ou plusieurs scènes pour une authentification.
- Configurer une Smart Card pour l'authentification.
- Sauvegarder et restaurer les données du programme.
- Ajouter des applications.

Ouverture de Security Manager

Vous pouvez ouvrir Security Manager selon l'une des méthodes suivantes :

▲ Sur le bureau Windows, double-cliquez sur l'icône **HP ProtectTools** dans la zone de notification, située à l'extrémité droite de la barre des tâches.

– ou –

Dans le **Panneau de configuration**, sélectionnez **Système et sécurité**, puis sélectionnez **HP ProtectTools Security Manager**.

Utiliser la Console utilisateur de Security Manager

La Console utilisateur de Security Manager est l'emplacement central qui permet d'accéder aisément aux fonctionnalités, aux applications et aux paramètres de Security Manager. La Console utilisateur affiche les éléments suivants :

- **Carte d'identité**—Affiche le nom d'utilisateur Windows et l'icône identifiant le compte utilisateur connecté.
- **Applications de sécurité**—Affiche un menu expansible des liens de configuration des catégories de sécurité suivantes :
  - **Accueil**—Permet de gérer les mots de passe, de configurer les informations d'authentification ou de vérifier l'état des applications de sécurité.
  - **Récupération en cas de vol**—Computrace pour HP ProtectTools (acheté séparément)
- **Mes connexions**—Permet de gérer les informations d'authentification avec le Gestionnaire de mots de passe et Credential Manager.
- **Mes données**—Permet de gérer la sécurité des données avec Drive Encryption.

REMARQUE : Cet élément ne s'affiche pas si l'application n'est pas installée.

- **Poste de travail**—Permet de gérer la sécurité de votre ordinateur avec Device Access Manager.

REMARQUE : Cet élément ne s'affiche pas si l'application n'est pas installée.

- **Administration**—Permet aux administrateurs d'accéder à la **Console d'administration** pour gérer la sécurité et les utilisateurs.
- **Avancé**—Affiche les commandes permettant d'accéder à des fonctions supplémentaires, notamment :
  - **Préférences**—Vous permet de personnaliser les paramètres de Security Manager.
  - **Sauvegarder et restaurer**—Vous permet de sauvegarder ou de restaurer des données.
  - **À propos de**—Affiche des informations sur HP ProtectTools Security Manager, telles que le numéro de version et la mention des droits d'auteur.
- **Zone principale**—Affiche les écrans spécifiques aux applications.
- **?**—Affiche l'aide de la Console utilisateur de Security Manager. Cette icône se trouve dans la partie supérieure droite du cadre de la fenêtre, à côté des icônes d'agrandissement et de réduction.

Votre carte d'identification personnelle

Votre carte d'identification vous identifie de façon unique comme étant le propriétaire de ce compte Windows et elle affiche votre nom et une photo de votre choix. Elle est affichée bien en évidence dans la partie supérieure gauche des pages de Security Manager.

Vous pouvez changer la façon dont votre nom s'affiche. Par défaut, votre nom d'utilisateur Windows complet et la photo sélectionnée lors de la configuration de Windows sont affichés.

Pour changer le nom affiché :

1. Ouvrez la Console utilisateur de Security Manager. Pour plus d'informations, reportez-vous à la section Ouverture de Security Manager à la page 26.
2. Cliquez sur la carte d'identité dans le coin supérieur gauche de la Console utilisateur.
3. Cliquez sur la zone affichant votre nom d'utilisateur Windows pour ce compte, entrez le nouveau nom, puis cliquez sur **Enregistrer**.

My Logons (Mes connexions)

Les applications incluses dans ce groupe vous aident à gérer divers aspects de votre identité numérique.

- **Gestionnaire de mots de passe**—Crée et gère les Liens rapides, ce qui vous permet de lancer des sites Web et des programmes, et de vous y connecter en vous authentifiant avec votre mot de passe Windows, votre empreinte digitale, votre visage, une Smart Card, une carte de proximité, une carte sans contact, un téléphone Bluetooth ou un code PIN.
- **Credential Manager**—Permet de modifier aisément votre mot de passe Windows, d'inscrire vos empreintes digitales ou votre visage, ou de configurer une Smart Card, une carte sans contact, une carte de proximité, un téléphone Bluetooth ou un code PIN.

Les administrateurs peuvent accéder à des informations sur les autres applications de sécurité disponibles en cliquant sur **Administration**, puis sur **Gestion centralisée** dans le coin inférieur gauche du tableau de bord.

Password Manager

Il est plus facile et plus sûr de se connecter à Windows, à des sites Web et à des applications lorsque vous utilisez le Gestionnaire de mots de passe. Vous pouvez l'utiliser pour créer des mots de passe plus forts que vous n'aurez pas à noter ni à mémoriser, puis pour vous connecter facilement et rapidement avec une empreinte digitale ou faciale, une Smart Card, une carte de proximité, une carte sans contact, un code PIN ou votre mot de passe Windows.

Password Manager offre les options suivantes :

Onglet Gérer

- Ajouter, modifier ou supprimer des connexions.
- Utiliser des liens rapides afin de lancer le navigateur par défaut et de vous connecter à tout site Web ou programme après sa configuration.
- Glisser-déposer pour organiser vos liens rapides en catégories.
- Déterminer instantanément si certains de vos mots de passe présentent un risque de sécurité.

Onglet Force du mot de passe

- Vérifier la force des différents mots de passe utilisés pour les sites Web et les applications ainsi que la force globale des mots de passe.
- La force des mots de passe est illustrée par des indicateurs d'état rouge, jaune et vert.

L'icône **Password Manager** s'affiche dans le coin supérieur gauche d'une page Web ou de l'écran de connexion d'une application. Si aucune connexion n'a encore été créée pour ce site Web ou cette application, un signe plus s'affiche sur l'icône.

▲ Cliquez sur l'icône **Password Manager** pour afficher un menu contextuel proposant les options suivantes :

- Ajouter [undomaine.com] au Gestionnaire de mots de passe
- Ouvrir le Gestionnaire de mots de passe
- Paramètres de l'icône
- Aide

Si aucune connexion n'a été créée pour les pages Web ou les programmes

Les options suivantes s'affichent dans le menu contextuel :

- **Ajouter [undomaine.com] au Gestionnaire de mots de passe**—Vous permet d'ajouter une connexion à l'écran de connexion actuel.
- **Ouvrir le Gestionnaire de mots de passe**—Lance le Gestionnaire de mots de passe.
- **Paramètres de l'icône**—Permet d'indiquer les conditions d'affichage de l'icône **Gestionnaire de mots de passe**.
- **Aide**—Affiche l'aide de Security Manager.

Si une connexion a déjà été créée pour les pages Web ou les programmes

Les options suivantes s'affichent dans le menu contextuel :

- **Remplir les données de connexion**—Affiche la page Vérifiez votre identité. Si l'authentification aboutit, vos données de connexion sont automatiquement entrées dans les champs de connexion, puis la page est soumise (si la soumission a été spécifiée lors de la création de la connexion ou de sa dernière modification).
- **Modifier la connexion**—Vous permet de modifier vos données de connexion pour ce site Web.
- **Ajouter une connexion**—Vous permet d'ajouter un compte au Gestionnaire de mots de passe.
- **Ouvrir le Gestionnaire de mots de passe**—Lance le Gestionnaire de mots de passe.
- **Aide**—Affiche l'aide de Security Manager.

REMARQUE : Il est possible que l'administrateur de cet ordinateur ait configuré Security Manager de façon à exiger plusieurs informations d'authentification lors de la vérification de votre identité.

Ajout de connexions

Vous pouvez ajouter aisément une connexion à un site Web ou à un programme en saisissant les informations de connexion une seule fois. Par la suite, Password Manager entre automatiquement ces informations à votre place. Vous pouvez utiliser ces connexions après avoir accédé au site Web ou au programme, ou cliquer sur une connexion à partir du menu **Liens rapides du Gestionnaire de mots de passe** pour que Password Manager ouvre le site Web ou le programme et vous connecte.

Pour ajouter une connexion :

1. Ouvrez l'écran de connexion d'un site Web ou d'un programme.
2. Cliquez sur la flèche de l'icône **Password Manager**, puis cliquez sur l'une des options suivantes en fonction de l'écran de connexion affiché (site Web ou programme) :
   - Pour un site Web, cliquez sur **Ajouter [nom de domaine] au Gestionnaire de mots de passe**.
   - Pour un programme, cliquez sur **Ajouter cet écran de connexion au Gestionnaire de mots de passe**.
3. Saisissez vos données de connexion. Les champs de connexion à l'écran et leurs champs correspondants dans la boîte de dialogue sont identifiés par un liseré orange en gras. Vous pouvez aussi afficher cette boîte de dialogue en cliquant sur **Ajouter une connexion** dans l'onglet **Gérer** de Password Manager, en utilisant la combinaison de touches d'activation ctrl +touche logo Windows+h, ou en faisant glisser votre doigt.
   a. Pour remplir un champ de connexion avec l'un des choix préformatés, cliquez sur les flèches à droite du champ.
   b. Pour consulter le mot de passe de cette connexion, cliquez sur **Afficher le mot de passe**.
   c. Pour que les données des champs de connexion soient fournies sans être envoyées, désactivez la case à cocher **Envoyer automatiquement les données de connexion**.

d. Cliquez sur **OK** pour sélectionner la méthode d'authentification à utiliser (empreintes digitales, visage, Smart Card, carte de proximité, carte sans contact, téléphone Bluetooth, code PIN ou mot de passe), puis connectez-vous à l'aide de la méthode choisie.

   Le signe plus est retiré de l'icône **Password Manager** afin de vous indiquer que la connexion a été créée.

e. Si Password Manager ne détecte aucun champ de connexion, cliquez sur **Plus de champs**.

   - Cochez la case de chaque champ obligatoire pour la connexion ou décochez la case des champs qui ne sont pas obligatoires pour effectuer l'opération.
   - Cliquez sur **Fermer**.

A chaque fois que vous accédez à ce site Web ou ouvrez ce programme, l'icône **Password Manager** s'affiche dans le coin supérieur gauche de l'écran de connexion du site Web ou de l'application, ce qui indique que vous pouvez utiliser les informations d'authentification enregistrées pour vous connecter.

Modification des connexions

Pour modifier une connexion, procédez comme suit :

1. Ouvrez l'écran de connexion d'un site Web ou d'un programme.
2. Pour afficher une boîte de dialogue dans laquelle vous pouvez modifier vos informations de connexion, cliquez sur la flèche située sur l'icône **Password Manager**, puis cliquez sur **Modifier la connexion**. Les champs de connexion à l'écran et leurs champs correspondant dans la boîte de dialogue, sont identifiés par un liseré orange en gras.

   Vous pouvez également afficher la boîte de dialogue en cliquant sur **Modifier pour obtenir la connexion souhaitée** dans l'onglet **Gérer** de Password Manager.
3. Modifiez vos informations de connexion.
   - Pour sélectionner un champ de connexion **Nom d'utilisateur** avec l'un des choix préformatés, cliquez sur la flèche vers le bas à droite du champ.
   - Pour sélectionner un champ de connexion **Mot de passe** avec l'un des choix préformatés, cliquez sur la flèche vers le bas à droite du champ.
   - Pour ajouter des champs de connexion dans l'écran, cliquez sur **Plus de champs**.
   - Pour consulter le mot de passe de cette connexion, cliquez sur **Afficher le mot de passe**.
   - Pour que les données des champs de connexion soient fournies sans être envoyées, désactivez la case à cocher **Envoyer automatiquement les données de connexion**.
4. Cliquez sur **OK**.

Utilisation du menu Liens rapides du Gestionnaire de mots de passe

Password Manager permet de lancer rapidement et aisément les sites Web et les programmes pour lesquels vous avez créé des connexions. Double-cliquez sur une connexion à un programme ou à un site Web dans le menu **Liens rapides du Gestionnaire de mots de passe** ou dans l'onglet **Gérer** de Password Manager pour ouvrir l'écran de connexion, puis indiquez vos données de connexion.

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

Pour afficher le menu **Liens rapides** :

1. Appuyez sur la combinaison de touches d'activation du **Gestionnaire de mots de passe** (ctrl+touche logo Windows+h est le paramètre défini en usine). Pour modifier la combinaison de touches d'activation, dans la Console utilisateur de Security Manager, double-cliquez sur **Gestionnaire de mots de passe**, puis sur **Paramètres**.
2. Procédez à la lecture de votre empreinte digitale (sur les ordinateurs avec un lecteur d'empreintes digitales intégré ou branché) ou entrez votre mot de passe Windows.

Organisation des connexions en catégories

Créez une ou plusieurs catégories afin d'organiser vos connexions. Ensuite, faites glisser et déposez les connexions dans les catégories correspondantes.

Pour ajouter une catégorie :

1. Dans la Console utilisateur de Security Manager, cliquez sur **Gestionnaire de mots de passe**.
2. Cliquez sur l'onglet **Gérer**, puis sur **Ajouter une catégorie**.
3. Entrez le nom de la catégorie.
4. Cliquez sur **OK**.

Pour ajouter une connexion à une catégorie :

1. Placez le pointeur de la souris au-dessus de la connexion concernée.
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 sont mises en surbrillance à mesure que vous déplacez le pointeur de la souris dessus.
4. Relâchez le bouton de la souris une fois la catégorie qui vous intéresse sélectionnée.

Vos connexions ne sont pas déplacées dans la catégorie, mais uniquement copiées vers la catégorie sélectionnée. Vous pouvez ajouter une même connexion à plusieurs catégories et afficher toutes les connexions en cliquant sur **Toutes**.

Gestion de vos connexions

Password Manager facilite la gestion centralisée des informations de connexion pour les noms d'utilisateur, les mots de passe et les comptes à plusieurs connexions.

Vos connexions sont répertoriées dans l’onglet **Gérer**. Si plusieurs connexions ont été créées pour le même site Web, chacune d’entre elles est ensuite répertoriée sous le nom du site Web et indentée dans la liste des connexions.

Pour gérer vos connexions :

▲ Dans la Console utilisateur de Security Manager, cliquez sur **Gestionnaire de mots de passe**, puis sur l'onglet **Gérer**.

- **Ajouter une connexion**—Cliquez sur **Ajouter une connexion**— et suivez les instructions à l'écran.
- **Vos connexions**—Cliquez sur une connexion existante, sélectionnez l'une des options suivantes, puis suivez les instructions à l'écran :
  - **Ouvrir**—Permet d'ouvrir un site Web ou un programme pour lequel il existe une connexion.
  - **Ajouter**—Permet d'ajouter une connexion. Pour plus d'informations, reportez-vous à la section Ajout de connexions à la page 29.
  - **Modifier**—Permet de modifier une connexion. Pour plus d'informations, reportez-vous à la section Modification des connexions à la page 30.
  - **Supprimer**—Permet de supprimer un site Web ou un programme pour lequel il existe une connexion.
- **Ajouter une catégorie**—Cliquez sur **Ajouter une catégorie**, puis suivez les instructions à l'écran. Pour plus d'informations, reportez-vous à la section Organisation des connexions en catégories à la page 31.

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

1. Ouvrez l'écran de connexion du site Web ou du programme.
2. Cliquez sur l'icône **Password Manager** pour afficher son menu contextuel.
3. Cliquez sur **Ajouter une connexion**, puis suivez les instructions à l'écran.

Évaluation de la force de votre mot de passe

L'utilisation de mots de passe forts pour la connexion aux sites Web et aux programmes est un aspect important de la protection de votre identité.

Password Manager facilite le contrôle et l'amélioration de votre sécurité grâce à une analyse instantanée et automatisée de la force de chaque mot de passe utilisé pour la connexion aux sites Web et aux programmes.

Dans l'onglet **Force du mot de passe**, les indicateurs d'état rouge, jaune et vert illustrent la force des différents mots de passe utilisés pour les sites Web et les applications, ainsi que la force globale des mots de passe.

Paramètres de l'icône Password Manager

Password Manager tente d'identifier les écrans de connexion des sites Web et des programmes. Lorsqu'il détecte un écran de connexion pour lequel aucune connexion n'a été créée, Password

Manager vous invite à ajouter une connexion pour l'écran en affichant l'icône **Password Manager** avec un signe plus.

1. Cliquez sur l'icône, puis sur **Paramètres de l'icône** pour personnaliser la manière dont le Gestionnaire de mots de passe va traiter les sites de connexion possibles.

   - **Inviter à ajouter des connexions aux écrans de connexion**—Cliquez sur cette option pour que le Gestionnaire de mots de passe vous invite à ajouter une connexion lorsqu'un écran de connexion qui n'a pas encore été configuré s'affiche.
   - **Exclure cet écran**—Sélectionnez la case à cocher afin que le Gestionnaire de mots de passe ne vous invite plus à ajouter une connexion à cet écran de connexion.

     Pour ajouter une connexion à un écran qui a été précédemment exclu :

     - Lorsque la connexion au site Web ou la page du programme précédemment exclue s'affiche, ouvrez la Console utilisateur de Security Manager, puis cliquez sur **Gestionnaire de mots de passe**.
     - Cliquez sur **Ajouter une connexion**.

       La boîte de dialogue correspondante s'ouvre et affiche l'écran de connexion du site Web ou le programme répertorié dans le champ **Ecran actuel**.
     - Cliquez sur **Continuer**.

       L'écran Ajouter une connexion au Gestionnaire de mots de passe s'affiche.
     - Suivez les instructions à l'écran. Pour plus d'informations, reportez-vous à la section Ajout de connexions à la page 29.
     - L'icône **Password Manager** s'affiche à chaque fois que la connexion à ce site Web ou l'écran de ce programme est ouvert.

     Ne pas inviter à ajouter des connexions pour les écrans de connexion—Sélectionnez cette case d'option.

2. Pour accéder aux paramètres supplémentaires du Gestionnaire de mots de passe, double-cliquez sur **Gestionnaire de mots de passe**, puis sur **Paramètres** dans la Console utilisateur de Security Manager.

Paramètres

Vous pouvez définir des paramètres permettant de personnaliser Password Manager :

1. **Inviter à ajouter des connexions aux écrans de connexion**—Un signe plus apparaît sur l'icône du **Gestionnaire de mots de passe** dès qu'un écran de connexion à un site Web ou à un programme est détecté. Cela indique que vous pouvez ajouter une connexion pour cet écran au menu **Connexions**. Pour désactiver cette fonction, décochez la case **Inviter à ajouter des connexions aux écrans de connexion**.
2. **Ouvrir le Gestionnaire de mots de passe avec ctrl+win+h**—La combinaison de touches d'activation par défaut qui ouvre le menu **Liens rapides du Gestionnaire de mots de passe** est ctrl+touche logo Windows+h. Pour changer cette combinaison, cliquez sur cette option et entrez une nouvelle combinaison. Les combinaisons peuvent inclure une ou plusieurs des touches suivantes : ctrl, alt ou maj et toute autre touche alphabétique ou numérique.
3. Cliquez sur **Appliquer** pour enregistrer les modifications.

Credential Manager

Vous utilisez vos informations d'authentification de Security Manager pour vérifier votre identité. L'administrateur de cet ordinateur peut configurer les informations d'authentification à utiliser pour prouver votre identité lors de la connexion à votre compte Windows, à des sites Web ou à des programmes.

Les informations d'authentification disponibles peuvent varier en fonction des périphériques de sécurité intégrés ou branchés à cet ordinateur. Les informations d'authentification prises en charge, les conditions requises et l'état actuel sont affichés lorsque vous cliquez sur **Credential Manager** sous **Mes connexions** et peuvent inclure les éléments suivantes :

- Mot de passe
- SpareKey
- Empreintes digitales
- Visage
- Smart Card
- Carte sans contact
- Carte de proximité
- Bluetooth
- PIN

Pour inscrire ou changer une information d'authentification, cliquez sur le lien et suivez les instructions à l'écran.

Changement de votre mot de passe Windows

Avec Security Manager, le changement de mot de passe Windows est plus facile et plus rapide qu'avec le panneau de configuration Windows.

Pour changer votre mot de passe Windows, procédez comme suit :

1. Dans la Console utilisateur de Security Manager, cliquez sur **Credential Manager**, puis sur **Mot de passe**.
2. Saisissez votre mot de passe actuel dans la zone de texte **Mot de passe Windows actuel**.
3. Saisissez un nouveau mot de passe dans la zone de texte **Nouveau mot de passe Windows**, puis entrez-le à nouveau dans la zone de texte **Confirmer le nouveau mot de passe**.
4. Cliquez sur **Modifier** pour remplacer immédiatement votre mot de passe actuel par celui que vous venez de saisir.

Configuration d’une SpareKey

Une SpareKey permet d'accéder à l'ordinateur (sur les plates-formes prises en charge) en répondant à trois questions de sécurité dans une liste définie précédemment par l'administrateur.

HP ProtectTools Security Manager vous invite à configurer votre SpareKey personnelle lors de la configuration initiale dans l'Assistant de configuration de HP ProtectTools Security Manager.

Pour configurer votre SpareKey :

1. Sur la page SpareKey de l'assistant, sélectionnez trois questions de sécurité, puis saisissez une réponse pour chaque question.
2. Cliquez sur **Créer**.

Vous pouvez sélectionner des questions différentes ou modifier vos réponses sur la page SpareKey, sous **Credential Manager**.

Une fois la SpareKey configurée, vous pouvez accéder à l'ordinateur avec cette dernière depuis un écran de connexion Préamorçage ou l'écran d'accueil Windows.

Inscription des empreintes digitales

Si l'administrateur a sélectionné Empreintes digitales dans l'écran **Choisissez vos informations d'authentification** et si votre ordinateur dispose d'un lecteur d'empreintes digitales intégré ou externe, l'Assistant de configuration de HP ProtectTools Security Manager vous guide au cours du processus de configuration ou « d'inscription » de vos empreintes digitales : Vous pouvez également inscrire vos empreintes digitales dans la page Empreinte, sous **Credential Manager** dans la Console utilisateur de Security Manager.

1. Sur la page Empreintes digitales de l'assistant, la silhouette de deux mains est affichée. Les empreintes déjà inscrites sont mises en surbrillance. Cliquez sur une empreinte sur la silhouette.

REMARQUE : Pour supprimer une empreinte enregistrée, cliquez sur le doigt correspondant.

2. Vous êtes invités à faire glisser le doigt jusqu'à ce que son empreinte digitale soit bien enregistrée. Un doigt inscrit est mis en surbrillance sur le pourtour.
3. Vous devez inscrire au moins deux doigts. L'index ou le majeur sont préférables. Répétez les étapes 1 et 2 pour un autre doigt.
4. Cliquez sur **Suivant**, puis suivez les instructions à l'écran.

ATTENTION : Lorsque vous enregistrez des empreintes digitales à l'aide de l'assistant, les informations correspondantes ne sont pas enregistrées tant que vous ne cliquez pas sur **Suivant**. Si vous laissez l'ordinateur inactif pendant un moment ou que vous fermez le programme, les modifications que vous avez effectuées **ne sont pas** enregistrées.

Inscription de scènes pour la connexion par reconnaissance faciale

Si vous choisissez la connexion par reconnaissance faciale et si votre ordinateur dispose d'une webcam intégrée ou connectée, l'Assistant de configuration de HP ProtectTools Security Manager vous invite à inscrire des scènes. Vous pouvez également inscrire vos scènes dans la page de connexion Visage, sous **Credential Manager** dans la Console utilisateur de Security Manager.

Vous devez inscrire une ou plusieurs scènes pour utiliser une connexion avec authentification faciale. Une fois que l'inscription s'est déroulée correctement, vous pouvez également inscrire une nouvelle scène si vous avez rencontré des difficultés pendant la connexion en raison d'un changement d'une ou plusieurs des conditions suivantes :

- Votre visage a changé de façon significative depuis votre dernière inscription.
- L'éclairage est très différent par rapport à vos inscriptions précédentes.
- Vous portiez des lunettes (ou non) lors de votre dernière inscription.

REMARQUE : Si vous ne parvenez pas à inscrire des scènes, essayez de rapprocher la webcam.

Pour inscrire une nouvelle scène à partir de l'Assistant de configuration de HP ProtectTools Security Manager :

1. Dans la page de connexion par reconnaissance faciale de l'assistant, cliquez sur **Avancé**, puis configurez des options supplémentaires. Pour plus d'informations, reportez-vous à la section Paramètres utilisateur avancés à la page 37.
2. Cliquez sur **OK**.
3. Cliquez sur **Démarrer** ou sur **Inscrire une nouvelle scène** si vous avez déjà inscrit des scènes.
4. Lors de l'inscription d'une scène, vous pouvez regarder une démonstration en cliquant sur **Lire la vidéo**.

   S'il s'agit de l'inscription initiale, une boîte de dialogue s'affiche, vous demandant si vous souhaitez regarder une vidéo de démonstration. Cliquez sur **Oui** ou sur **Non**.
5. Dans des conditions d'éclairage faible, le logiciel est capable d'augmenter la luminosité de l'écran automatiquement, mais vous avez également la possibilité de modifier la lumière d'arrière-plan en cliquant sur l'icône **Ampoule**.
6. Cliquez sur l'icône **Caméra**, puis suivez les instructions à l'écran pour inscrire votre scène.

REMARQUE : N'oubliez pas de regarder votre image pendant la capture des scènes, en tournant la tête lorsque nécessaire.

7. Cliquez sur **Suivant**.

Vous pouvez également inscrire des scènes depuis la Console utilisateur de Security Manager :

1. Ouvrez la Console utilisateur de Security Manager. Pour plus d'informations, reportez-vous à la section Ouverture de Security Manager à la page 26.
2. Sous **Mes connexions**, cliquez sur **Credential Manager**, puis sur **Visage**.
3. Cliquez sur **Avancé** pour configurer des options supplémentaires. Pour plus d'informations, reportez-vous à la section Paramètres utilisateur avancés à la page 37.
4. Cliquez sur **OK**.
5. Cliquez sur **Démarrer** ou sur **Inscrire une nouvelle scène** si vous avez déjà inscrit des scènes.
6. Si vous êtes invité à entrer votre mot de passe Windows, saisissez-le, puis cliquez sur **Suivant**.
7. Lors de l'inscription d'une scène, vous pouvez regarder une démonstration en cliquant sur **Lire la vidéo**.

   S'il s'agit de l'inscription initiale, une boîte de dialogue s'affiche, vous demandant si vous souhaitez regarder une vidéo de démonstration. Cliquez sur **Oui** ou sur **Non**.
8. Dans des conditions d'éclairage faible, le logiciel est capable d'augmenter la luminosité de l'écran automatiquement, mais vous avez également la possibilité de modifier la lumière d'arrière-plan en cliquant sur l'icône **Ampoule**.
9. Cliquez sur l'icône **Caméra**, puis suivez les instructions à l'écran pour inscrire votre scène.

REMARQUE : N'oubliez pas de regarder votre image pendant la capture des scènes, en tournant la tête lorsque nécessaire.

Pour plus d'informations, consultez l'aide du logiciel Face Recognition en cliquant sur l'icône bleue **?** située dans la partie supérieure droite de la page d'inscription Visage.

Authentification

Après avoir inscrit une ou plusieurs scènes, vous pouvez utiliser votre visage pour authentification lorsque vous vous connectez à l'ordinateur ou lorsque vous démarrez une nouvelle session Windows.

1. Lorsque l'écran d'authentification est lancé et que l'appareil photo détecte votre visage, vous avez 5 secondes pour démarrer le processus de connexion. Si votre visage est reconnu, vous pouvez accéder à l'ordinateur.
2. Si le délai de connexion par reconnaissance faciale est dépassé, Face Recognition se met en pause. Cliquez sur l'icône **Caméra** pour reprendre le processus d'authentification.

REMARQUE : si l'éclairage est insuffisant et que vous ne parvenez pas à vous connecter à l'aide de Face Recognition, vous pouvez entrer votre mot de passe Windows afin de vous connecter à l'ordinateur.

3. Une fois que vous êtes connecté à l'ordinateur, si Face Recognition vous demande d'ajouter des scènes supplémentaires afin d'améliorer votre capacité de connexion durant les sessions ultérieures, cliquez sur **Oui**.

Mode sombre

Si l'éclairage est trop sombre durant le processus de connexion par reconnaissance faciale, l'arrière-plan de l'écran devient automatiquement blanc afin de mieux éclairer le visage.

Pour changer manuellement la couleur d'arrière-plan de l'écran de connexion par reconnaissance faciale, cliquez sur l'icône **Ampoule**.

Apprentissage

Si la connexion par reconnaissance faciale a échoué mais que vous avez bien entré votre mot de passe, vous pouvez être invité à enregistrer une série d'images afin d'augmenter les chances de réussite de la connexion par reconnaissance faciale à l'avenir.

Suppression d'une scène

Pour supprimer une scène actuellement inscrite :

1. Ouvrez la Console utilisateur de Security Manager. Pour plus d'informations, reportez-vous à la section Ouverture de Security Manager à la page 26.
2. Sous **My Logons** (Mes connexions), cliquez sur **Credential Manager**, puis sur **Visage**.
3. Cliquez sur la scène à supprimer, puis cliquez sur l'icône **Trash can** (Poubelle).
4. Cliquez sur **OK** dans la boîte de dialogue de confirmation.

Paramètres utilisateur avancés

1. Ouvrez la Console utilisateur de Security Manager. Pour plus d'informations, reportez-vous à la section Ouverture de Security Manager à la page 26.
2. Sous **Mes connexions**, cliquez sur **Credential Manager**, puis sur **Visage**.

3. Cliquez sur **Avancé** pour configurer les options suivantes :

   Onglet **Autres paramètres**—Sélectionnez la case à cocher pour activer une ou plusieurs des options suivantes ou décochez la case pour désactiver une option. Ces paramètres s'appliquent uniquement à l'utilisateur actuel.

   - **Émettre un son lors des événements de reconnaissance faciale**—Émet un son lorsque la connexion par reconnaissance faciale réussit ou échoue.
   - **Inviter à mettre à jour les scènes en cas d'échec de connexion**—Si la connexion par reconnaissance faciale a échoué alors que vous avez entré votre mot de passe correctement, vous pouvez être invité à enregistrer une série d'images capturées pour augmenter les chances de réussite de la connexion par reconnaissance faciale à l'avenir.
   - **Inviter à inscrire une nouvelle scène en cas d'échec de connexion**—Si la connexion par reconnaissance faciale a échoué alors que vous avez entré votre mot de passe avec succès, vous pouvez être invité à inscrire une nouvelle scène pour augmenter les chances de réussite de la connexion par reconnaissance faciale par la suite.

4. Pour rétablir les paramètres sur leurs valeurs par défaut, cliquez sur **Restaurer les valeurs par défaut**.
5. Cliquez sur **OK**.

Configuration d'une Smart Card

Si un lecteur de Smart Card est intégré ou connecté à votre ordinateur et si l'administrateur a sélectionné une carte Smart Card comme information d'authentification et effectué la procédure décrite dans l'aide du logiciel de la Console d'administration de HP ProtectTools, l'Assistant de configuration de HP ProtectTools Security Manager vous invite à insérer et à configurer une carte Smart Card. Vous pouvez également configurer votre Smart Card dans la page Smart Card, sous **Credential Manager** dans la Console utilisateur de Security Manager.

REMARQUE : Un administrateur doit initialiser la carte Smart Card avant de pouvoir l'utiliser.

Initialisation de la Smart Card

HP ProtectTools Security Manager peut prendre en charge plusieurs Smart Card. Le nombre et le type des caractères utilisés pour le code PIN peuvent varier. Le fabricant de la carte Smart Card doit fournir des outils pour installer un certificat de sécurité et gérer le code PIN que HP ProtectTools utilisera dans son algorithme de sécurité.

Les administrateurs peuvent initialiser la carte Smart Card à l'aide du logiciel' du fabricant et de la Console d'administration de HP ProtectTools. Pour plus d'informations, reportez-vous à l'aide du logiciel de la Console d'administration de HP ProtectTools.

Enregistrement de la Smart Card

Une fois la Smart Card initialisée, les utilisateurs peuvent l'enregistrer dans Security Manager :

1. Ouvrez la Console utilisateur de Security Manager. Pour plus d'informations, reportez-vous à la section Ouverture de Security Manager à la page 26.
2. Cliquez sur **Credential Manager**, puis sur **Smart Card**.
3. Assurez-vous de sélectionner l'option **Configurer**.
4. Entrez votre mot de passe Windows et votre code PIN, puis cliquez sur **Enregistrer**.

Les administrateurs peuvent également enregistrer la Smart Card dans la console d'administration de HP ProtectTools. Pour plus d'informations, consultez l'aide du logiciel de la console d'administration de HP ProtectTools.

Changement du code PIN de la Smart Card

Pour modifier le code PIN de la Smart Card :

1. Insérez une Smart Card précédemment formatée et initialisée.
2. Sélectionnez **Modifier le code PIN de la carte Smart Card**.
3. Entrez l'ancien code PIN, puis saisissez et confirmez un nouveau code PIN.

Carte sans contact

Une carte sans contact est une petite carte en plastique avec une puce informatique intégrée. Si un lecteur de cartes sans contact est connecté à l'ordinateur, si l'administrateur a installé le pilote fourni par le fabricant installé et s'il a indiqué une carte sans contact comme information d'authentification, vous pouvez utiliser une carte sans contact comme information d'authentification. Les types de cartes sans contact suivants sont pris en charge par HP ProtectTools :

- cartes mémoires sans contact iCLASS HID ;
- cartes mémoires sans contact MiFare Classic 1k et 4k, et mini cartes mémoires sans contact.

▲ Pour configurer votre carte sans contact, placez-la tout près du lecteur et suivez les instructions à l'écran, puis cliquez sur **Appliquer**.

Carte de proximité

Une carte de proximité est une petite carte en plastique avec une puce informatique intégrée. Si un lecteur de cartes de proximité est connecté à l'ordinateur, si l'administrateur a installé pilote fourni par le fabricant et s'il a sélectionné une carte de proximité comme information d'authentification, vous pouvez utiliser une carte de proximité en conjonction avec d'autres informations d'authentification pour plus de sécurité.

▲ Pour configurer votre carte de proximité, placez-la tout près du lecteur et suivez les instructions à l'écran, puis cliquez sur **Appliquer**.

Bluetooth

Si l'administrateur a sélectionné Bluetooth comme information d'authentification, vous pouvez configurer un téléphone Bluetooth en conjonction avec d'autres informations d'authentification pour plus de sécurité.

REMARQUE : Les téléphones Bluetooth sont les seuls périphériques Bluetooth pris en charge.

1. Vérifiez que la fonctionnalité Bluetooth est activée sur l'ordinateur et que le téléphone Bluetooth est en mode détection. Pour connecter le téléphone, il est possible que vous deviez saisir un code généré automatiquement sur le clavier du périphérique Bluetooth. En effet, selon les paramètres de configuration du périphérique Bluetooth, il se peut que le code de connexion de l'ordinateur et celui du téléphone doivent être comparés.
2. Pour inscrire le téléphone, sélectionnez-le, puis cliquez sur **Inscrire**.
3. Cliquez sur **OK** dans la boîte de dialogue de confirmation.

PIN

Si l’administrateur a sélectionné PIN comme information d’authentification, vous pouvez configurer un code PIN en conjonction avec d’autres informations d’authentification pour plus de sécurité.

▲ Pour configurer un nouveau code PIN, entrez-le, puis confirmez-le en le saisissant à nouveau.

Administration

Les administrateurs peuvent accéder à la Console d'administration et à la Gestion centralisée en cliquant sur **Administration**, puis en sélectionnant **Console d'administration** dans le panneau inférieur gauche de la Console utilisateur de HP ProtectTools Security Manager.

Pour plus d'informations, reportez-vous à l'aide du logiciel de la Console d'administration de HP ProtectTools.

Avancé

Vous pouvez accéder aux options suivantes en cliquant sur **Avancé** dans le panneau inférieur gauche de la Console utilisateur :

- **Préférences**—Permet de personnaliser les paramètres de Security Manager.
- **Sauvegarder et restaurer**—Permet de sauvegarder et de restaurer vos données de Security Manager.
- **À propos de**—Affiche des informations de version à propos de Security Manager

Définition de vos préférences

Vous pouvez personnaliser les paramètres de HP ProtectTools Security Manager. Dans la Console utilisateur de Security Manager, cliquez sur **Avancé**, puis sur **Préférences**. Les paramètres disponibles sont affichés dans deux onglets : **Général** et **Empreinte**.

Onglet Général

Apparence—Affiche l'icône dans la zone de notification de la barre des tâches

- Pour activer l'affichage de l'icône dans la barre des tâches, sélectionnez la case à cocher correspondante.
- Pour désactiver l'affichage de l'icône dans la barre des tâches, décochez la case correspondante.

Onglet Empreinte

REMARQUE : L'onglet **Empreinte** est disponible uniquement si l'ordinateur est équipé d'un lecteur d'empreintes digitales et que le pilote approprié est installé.

- **Actions rapide**—Utilisez des Actions rapides pour sélectionner la tâche de Security Manager à réaliser lorsque vous maintenez une touche désignée enfoncée tout en faisant glisser votre empreinte digitale.

  Pour attribuer une action rapide à l'une des touches répertoriées, cliquez sur une option **(Touche) + Empreinte digitale**, puis sélectionnez l'une des tâches disponibles dans le menu.

- **Retour d'empreinte digitale**—N'est affiché que lorsqu'un lecteur d'empreinte digitale est disponible. Utilisez ce paramètre pour ajuster le retour qui se produit lorsque vous faites glisser votre empreinte digitale.

  - **Activer le retour audio**—Security Manager vous donne un retour audio lorsqu'une empreinte digitale a été glissée, jouant différents sons pour des événements spécifiques du programme. Vous pouvez attribuer de nouveaux sons à ces événements à l'aide de l'onglet **Sons** dans la section Paramètres audio du Panneau de configuration Windows ou désactiver le retour audio en effaçant cette option.
  - **Afficher le retour qualité de la lecture**

    Pour afficher toutes les analyses, quel que soit le niveau de qualité, cochez la case correspondante.

    Pour afficher uniquement des analyses de bonne qualité, décochez la case.

Sauvegarde et restauration de vos données

Il est recommandé de sauvegarder les données de Security Manager régulièrement. La fréquence de sauvegarde dépend de la fréquence de modification des données. Par exemple, si vous ajoutez de nouvelles connexions tous les jours, il est préférable de sauvegarder les données quotidiennement.

Les sauvegardes peuvent également être utilisées afin d'effectuer les migrations d'un ordinateur à l'autre, c'est-à-dire d'importer et d'exporter des données.

REMARQUE : Seules les informations du Gestionnaire de mots de passe et de Face Recognition sont sauvegardées par cette fonctionnalité. Drive Encryption possède une méthode de sauvegarde indépendante. Les informations d'authentification par empreinte digitale et à Device Access Manager ne sont pas sauvegardées.

HP ProtectTools Security Manager doit être installé sur l'ordinateur qui reçoit les données sauvegardées pour que vous puissiez restaurer les données provenant du fichier de sauvegarde.

Pour sauvegarder les données :

1. Ouvrez la Console utilisateur de Security Manager. Pour plus d'informations, reportez-vous à la section Ouverture de Security Manager à la page 26.
2. Dans le panneau de gauche de la Console utilisateur, cliquez sur **Avancé**, puis sur **Sauvegarder et restaurer**.
3. Cliquez sur **Sauvegarder les données**.
4. Sélectionnez les modules à inclure dans la sauvegarde. Dans la plupart des cas, vous sélectionnez tous les modules.
5. Vérifiez votre identité.
6. Entrez le nom du fichier de stockage. Par défaut, le fichier est enregistré dans le dossier Documents. Cliquez sur **Parcourir** pour choisir un autre emplacement.

7. Entrez un mot de passe pour protéger le fichier.
8. Cliquez sur **Terminer**.

Pour restaurer les données :

1. Ouvrez la Console utilisateur de Security Manager. Pour plus d'informations, reportez-vous à la section Ouverture de Security Manager à la page 26.
2. Dans le panneau de gauche de la Console utilisateur, cliquez sur **Avancé**, puis sur **Sauvegarder et restaurer**.
3. Cliquez sur **Restaurer les données**.
4. Sélectionnez le fichier de stockage créé. Entrez son chemin d'accès dans le champ fourni ou cliquez sur **Parcourir**.
5. Entrez le mot de passe utilisé pour protéger le fichier.
6. Sélectionnez les modules pour lesquels vous souhaitez restaurer les données. Dans la plupart des cas, vous sélectionnez tous les modules répertoriés.
7. Vérifiez votre mot de passe Windows.
8. Cliquez sur **Terminer**.

6 Drive Encryption for HP ProtectTools (certains modèles uniquement)

Drive Encryption for HP ProtectTools fournit une protection complète des données sur votre ordinateur en les cryptant. Lorsque Drive Encryption est activé, vous devez vous connecter via son écran de connexion, qui s'affiche avant le® démarrage du système d'exploitation Windows.

HP ProtectTools Security Manager (Assistant de configuration de HP Client Security, Assistant de configuration avancé ou Console d'administration) permet aux administrateurs Windows d'activer Drive Encryption, de sauvegarder la clé de cryptage et de sélectionner ou désélectionner une ou plusieurs unités ou partitions en vue du cryptage. Pour plus d'informations, reportez-vous à l'aide du logiciel de HP ProtectTools Security Manager.

Les tâches suivantes peuvent être effectuées avec Drive Encryption :

- Sélection des paramètres de Drive Encryption :
  - Activation d'un mot de passe protégé TPM
  - Cryptage ou décryptage d'unités ou de partitions individuelles à l'aide du cryptage logiciel
  - Cryptage ou décryptage d'unités auto-cryptées individuelles à l'aide du cryptage matériel
  - Ajout d'une sécurité supplémentaire via la désactivation du mode Veille afin de s'assurer que l'authentification au préamorçage de Drive Encryption soit toujours requise

REMARQUE : Seuls les disques durs SATA internes et eSATA externes peuvent être cryptés.

- Création de clés de sauvegarde
- Restauration de l’accès à un ordinateur crypté à l’aide des clés de sauvegarde et de HP SpareKey
- Activation de l'authentification au préamorçage de Drive Encryption à l'aide d'un mot de passe, d'une empreinte enregistrée ou d'un code PIN pour sélectionner une carte Smart Card

Ouverture de Drive Encryption

Les administrateurs peuvent accéder à Drive Encryption en ouvrant la Console utilisateur de HP ProtectTools Security Manager.

1. Sur le bureau Windows, double-cliquez sur l'icône **HP ProtectTools** dans la zone de notification, située à l'extrémité droite de la barre des tâches.

   – ou –

   Dans le **Panneau de configuration**, sélectionnez **Système et sécurité**, puis sélectionnez **HP ProtectTools Security Manager**.

2. Dans le volet gauche de la Console utilisateur de HP ProtectTools Security Manager, sélectionnez **Administration**, puis sélectionnez **Console d'administration**.

3. Dans le volet gauche de la Console d'administration de HP ProtectTools, sélectionnez **Drive Encryption**.

Tâches générales

Activation de Drive Encryption pour les disques durs standard

Les disques durs standard sont cryptés à l'aide du cryptage logiciel. Procédez comme suit pour activer Drive Encryption :

1. Ouvrez la **Console d'administration de HP ProtectTools**. Pour plus d'informations, reportez-vous à la section Ouverture de la console d'administration de HP ProtectTools à la page 17.
2. Dans le volet gauche, cliquez sur **Assistant de configuration**.
3. Cochez la case **Drive Encryption**, puis cliquez sur **Suivant**.
4. Pour sauvegarder la clé de cryptage, connecter un périphérique externe pour enregistrer cette clé. Cette clé doit être utilisée pour accéder aux données si les autres méthodes échouent.
5. Sous **Back up Drive Encryption keys** (Sauvegarder les clés Drive Encryption), cochez la case en regard du périphérique de stockage dans lequel sera enregistrée la clé de cryptage.
6. Cliquez sur **Suivant**.

REMARQUE : Vous êtes invité à redémarrer l'ordinateur. Après le redémarrage, l'écran de préamorçage de Drive Encryption s'affiche et requiert une authentification pour pouvoir lancer une session Windows.

Drive Encryption a été activé. Le cryptage des partitions de disque sélectionnées peut prendre plusieurs heures, en fonction de leur nombre et de leur taille.

Pour plus d'informations, reportez-vous à l'aide du logiciel de HP ProtectTools Security Manager.

Activation de Drive Encryption pour les unités auto-cryptées

Les unités auto-cryptées conformes aux spécifications OPAL du Trusted Computing Group relatives à la gestion des unités auto-cryptées peuvent être cryptées à l'aide d'un cryptage logiciel ou matériel. Procédez comme suit afin d'activer Drive Encryption pour les unités auto-cryptées :

REMARQUE : Le cryptage matériel est disponible uniquement si TOUTES les unités de votre ordinateur sont des unités auto-cryptées conformes aux spécifications OPAL du Trusted Computing Group relatives à la gestion des unités auto-cryptées. Dans ce cas, l'option **Utiliser le cryptage des unités matérielles** est disponible et le cryptage matériel ou logiciel peut être utilisé.

Si certaines unités sont auto-cryptées et d'autres sont standard, l'option **Utiliser le cryptage des unités matérielles** n'est pas disponible et seul le cryptage logiciel peut être utilisé. Pour plus d'informations, reportez-vous à la section Activation de Drive Encryption pour les disques durs standard à la page 44.

▲ Utilisez l'Assistant de configuration de HP ProtectTools Security Manager pour activer Drive Encryption.

– ou –

Cryptage logiciel

1. Ouvrez la **Console d'administration de HP ProtectTools**. Pour plus d'informations, reportez-vous à la section Ouverture de la console d'administration de HP ProtectTools à la page 17.
2. Dans le volet gauche, cliquez sur **Assistant de configuration**.

3. Cochez la case **Drive Encryption**, puis cliquez sur **Suivant**.

REMARQUE : Si l'option **Use hardware drive encryption** (Utiliser le cryptage d'unité matériel) est disponible en bas de l'écran, décochez la case.

4. Sous **Unités à crypter**, cochez la case en regard du disque dur à crypter, puis cliquez sur **Suivant**.
5. Pour sauvegarder la clé de cryptage, insérez le périphérique de stockage dans le logement approprié.
6. Sous **Back up Drive Encryption keys** (Sauvegarder les clés Drive Encryption), cochez la case en regard du périphérique de stockage dans lequel sera enregistrée la clé de cryptage.
7. Cliquez sur **Appliquer**.

REMARQUE : L'ordinateur redémarre.

Drive Encryption a été activé. Le cryptage de l'unité peut prendre plusieurs heures, en fonction de sa taille.

Cryptage matériel

1. Ouvrez la **Console d'administration de HP ProtectTools**. Pour plus d'informations, reportez-vous à la section Ouverture de la console d'administration de HP ProtectTools à la page 17.
2. Dans le volet gauche, cliquez sur **Assistant de configuration**.
3. Cochez la case **Drive Encryption**, puis cliquez sur **Suivant**.
4. Si la case à cocher **Use hardware drive encryption** (Utiliser le cryptage d'unité matériel) est disponible en bas de l'écran, assurez-vous qu'elle est sélectionnée.

   Si la case est décochée ou n'est pas disponible, le cryptage logiciel est appliqué. Pour plus d'informations, reportez-vous à la section Activation de Drive Encryption pour les disques durs standard à la page 44.
5. Sous **Unités à crypter**, cochez la case en regard du disque dur à crypter, puis cliquez sur **Suivant**.

REMARQUE : Si une seule unité s'affiche, la case à cocher correspondante est automatiquement cochée et grisée.

Si plusieurs unités sont affichées, le disque 0 sera automatiquement sélectionné et grisé, mais l'option permettant de sélectionner d'autres disques durs pour le cryptage matériel sera également disponible.

Le bouton **Suivant** n'est pas disponible tant qu'au moins une unité n'a pas été sélectionnée.

6. Pour sauvegarder la clé de cryptage, insérez le périphérique de stockage dans le logement approprié.
7. Sous **Back up Drive Encryption keys** (Sauvegarder les clés Drive Encryption), cochez la case en regard du périphérique de stockage dans lequel sera enregistrée la clé de cryptage.
8. Cliquez sur **Appliquer**.

REMARQUE : Vous êtes invité à redémarrer l'ordinateur. Le préamorçage de Drive Encryption sera affiché et nécessitera une authentification pour pouvoir lancer une session Windows.

Drive Encryption a été activé. Le cryptage de l'unité peut prendre plusieurs minutes.

Pour plus d'informations, reportez-vous à l'aide du logiciel de HP ProtectTools Security Manager.

Désactivation de Drive Encryption

Les administrateurs peuvent utiliser l'assistant de configuration de HP ProtectTools Security Manager pour désactiver Drive Encryption. Pour plus d'informations, reportez-vous à l'aide du logiciel de HP ProtectTools Security Manager.

1. Ouvrez la **Console d'administration de HP ProtectTools**. Pour plus d'informations, reportez-vous à la section Ouverture de la console d'administration de HP ProtectTools à la page 17.
2. Dans le volet gauche, cliquez sur **Assistant de configuration**.
3. Décochez la case **Drive Encryption**, puis cliquez sur **Suivant**.

   La désactivation de Drive Encryption commence.

REMARQUE : Si le cryptage logiciel a été utilisé, le décryptage démarre. Cette opération peut prendre plusieurs heures, en fonction de la taille des partitions de disque dur cryptées. Une fois le décryptage terminé, Drive Encryption est désactivé.

Si le cryptage matériel a été utilisé, l'unité est instantanément décryptée et, après quelques minutes, Drive Encryption sera désactivé.

Une fois Drive Encryption désactivé, vous serez invité à arrêter l'ordinateur (en cas de cryptage matériel) ou à le redémarrer (en cas de cryptage logiciel).

Connexion après l'activation de Drive Encryption

Si vous allumez l'ordinateur après que Drive Encryption soit activé et que votre compte utilisateur soit inscrit, vous devez vous connecter sur l'écran de connexion de Drive Encryption :

REMARQUE : Lorsque l'ordinateur sort du mode Veille, l'authentification au préamorçage de Drive Encryption ne s'affiche pas pour le cryptage matériel ou logiciel. Le cryptage matériel propose l'option **Désactiver le mode Veille pour la sécurité ajoutée** qui, lorsqu'elle est sélectionnée, permet d'éviter l'activation du mode Veille.

Lorsque l'ordinateur sort du mode de veille prolongée, l'authentification au préamorçage de Drive Encryption s'affiche pour le cryptage matériel et logiciel.

REMARQUE : Si l'administrateur Windows a activé l'option Sécurité de préamorçage du BIOS dans HP ProtectTools Security Manager et si l'ouverture de session en une étape est activée (par défaut), vous pouvez vous connecter à l'ordinateur immédiatement après l'authentification au préamorçage du BIOS, et ce sans avoir à vous réauthentifier depuis l'écran de connexion de Drive Encryption.

Connexion d'utilisateur unique :

- Sur la page **Connexion**, saisissez votre mot de passe Windows, le code PIN de la carte Smart Card, SpareKey, Face, ou passez votre doigt si votre empreinte est enregistrée.

Connexion d'utilisateurs multiples :

1. Sur la page **Sélectionner un utilisateur à connecter**, sélectionnez l'utilisateur à connecter dans la liste déroulante, puis cliquez sur **Suivant**.
2. Sur la page **Connexion**, saisissez votre mot de passe Windows ou le code PIN de votre carte Smart Card. Vous pouvez également passer votre doigt si votre empreinte est enregistrée.

REMARQUE : Les cartes Smart Card suivantes sont prises en charge :

Cartes Smart Card prises en charge

- ActivIdentity Oberthur Cosmopol IC 64k V5.2
- Gemalto Cyberflex Access 64k V2c
- ActivIdentity Activkey SIM (Gemalto Cyberflex Access 64k V2c)

REMARQUE : Si vous utilisez la clé de récupération pour vous connecter dans l'écran de connexion de Drive Encryption, des informations d'authentification supplémentaires sont requises lors de la connexion à Windows pour accéder aux comptes d'utilisateurs.

Protection de vos données via le cryptage de votre disque dur

Il est vivement recommandé d'utiliser l'Assistant de configuration de HP ProtectTools Security Manager pour protéger vos données en cryptant votre disque dur. Une fois l'activation effectuée, tous les disques durs ou partitions supplémentaires créés peuvent être cryptés en procédant comme suit :

1. Dans le volet gauche, cliquez sur l'icône **+** située à gauche de **Drive Encryption** pour afficher les options disponibles.
2. Cliquez sur **Paramètres**.
3. Pour les unités cryptées par cryptage logiciel, sélectionnez les partitions à crypter.

REMARQUE : Cette opération s'applique également dans les cas où il existe une ou plusieurs unités auto-cryptées et une ou plusieurs unités standard.

– ou –

- ▲ Pour les unités cryptées par cryptage matériel, sélectionnez la ou les unités supplémentaires à crypter.

Tâches avancées

Gestion de Drive Encryption (administrateur uniquement)

Les administrateurs peuvent utiliser la page Paramètres sous Drive Encryption pour afficher et modifier l'état de ce dernier (activé, désactivé ou un cryptage matériel a été activé) ainsi que pour afficher l'état du cryptage de tous les disques durs de l'ordinateur.

REMARQUE : Seuls les disques durs supplémentaires peuvent être sélectionnés ou désélectionnés en vue d'un cryptage matériel sur la page Paramètres de Drive Encryption.

- Si l'état est Désactivé, Drive Encryption n'a pas encore été activé par l'administrateur Windows et ne protège pas le disque dur. Utilisez l'Assistant de configuration de HP ProtectTools Security Manager pour activer Drive Encryption.
- Si l'état est Activé, Drive Encryption a été activé et configuré. L'unité se trouve dans l'un des états suivants :

Cryptage logiciel

- Non cryptée
- Cryptée
- En cours de cryptage
- En cours de décryptage

Cryptage matériel

- Cryptée
- Non cryptée (pour les unités supplémentaires)

Utilisation de la sécurité renforcée avec TPM (sélectionnez les modèles uniquement)

Si le Trusted Platform Module (TPM) est activé et que la fonction de sécurité renforcée de Drive Encryption avec TPM est sélectionnée, le mot de passe de Drive Encryption sera protégé par la puce de sécurité TPM. Si le disque dur est retiré et installé sur un autre ordinateur, son accès est refusé.

ATTENTION : La propriété du TPM ne peut pas être partagée avec Windows TPM.msc.

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

REMARQUE : L'option TPM doit être activée dans la configuration BIOS.

Cryptage ou décryptage de partitions d'unités individuelles (cryptage logiciel uniquement)

Les administrateurs peuvent utiliser la page Paramètres de Drive Encryption pour crypter une ou plusieurs partitions de disque dur sur l'ordinateur ou décrypter des partitions d'unités ayant déjà été cryptées.

1. Ouvrez la **Console d'administration de HP ProtectTools**. Pour plus d'informations, reportez-vous à la section Ouverture de la console d'administration de HP ProtectTools à la page 17.
2. Dans le volet gauche, cliquez sur l'icône **+** située à gauche de **Drive Encryption** pour afficher les options disponibles.
3. Cliquez sur **Paramètres**.
4. Sous **Etat d'unité**, cochez ou décochez la case en regard de chaque disque dur à crypter ou à décrypter, puis cliquez sur **Appliquer**.

REMARQUE : Lorsqu'une partition est en cours de cryptage ou de décryptage, une barre de progression affiche le pourcentage de partition cryptée et le temps restant pour terminer le processus.

REMARQUE : Les partitions dynamiques ne sont pas prises en charge. Si une partition est affichée comme étant disponible, mais qu'elle ne peut pas être cryptée après avoir été sélectionnée, elle est dynamique. Une partition dynamique résulte du rétrécissement d'une partition pour créer une autre partition dans la Gestion des disques.

Un avertissement s'affiche si une partition va être convertie en partition dynamique.

Sauvegarde et restauration (tâche de l'administrateur)

Lorsque Drive Encryption est activé, les administrateurs peuvent utiliser la page de restauration de la clé de cryptage pour sauvegarder les clés de cryptage sur un support amovible et effectuer une restauration.

Sauvegarde des clés de cryptage

Les administrateurs peuvent sauvegarder la clé de cryptage d'une unité cryptée sur un périphérique de stockage amovible.

ATTENTION : Veillez à conserver le périphérique de stockage contenant la clé de cryptage dans un endroit sûr car si vous oubliez votre mot de passe, perdez votre carte Smart Card ou n'avez enregistré aucune empreinte, ce périphérique constitue votre seul accès à votre ordinateur. L'emplacement de stockage doit également être sécurisé car le périphérique de stockage permet d'accéder à Windows.

REMARQUE : Pour enregistrer la clé de cryptage, vous devez utiliser un périphérique de stockage USB au format FAT32 ou FAT16. Une barrette de mémoire USB, une carte mémoire SD (Secure Digital) ou une carte MultiMedia (MMC) peut être utilisée pour la sauvegarde.

1. Ouvrez la **Console d'administration de HP ProtectTools**. Pour plus d'informations, reportez-vous à la section Ouverture de la console d'administration de HP ProtectTools à la page 17.
2. Dans le volet gauche, cliquez sur l'icône **+** située à gauche de **Drive Encryption** pour afficher les options disponibles.
3. Cliquez sur **Sauvegarde des clés de cryptage**.
4. Insérez le périphérique de stockage utilisé pour sauvegarder la clé de cryptage.

   REMARQUE : Pour enregistrer la clé de cryptage, vous devez utiliser un périphérique de stockage USB au format FAT32. Une barrette de mémoire USB, une carte mémoire SD (Secure Digital) ou une carte MultiMedia (MMC) peut être utilisée pour la sauvegarde. Dans certains cas SkyDrive peut être utilisé.
5. Sous **Unité**, cochez la case en regard du périphérique dans lequel vous souhaitez sauvegarder votre clé de cryptage.
6. Cliquez sur **Sauvegarder les clés**.
7. Lisez les informations contenues dans la page qui s'affiche, puis cliquez sur **OK**. La clé de cryptage est enregistrée sur le périphérique de stockage sélectionné.

Restauration de l'accès à un ordinateur activé à l'aide des clés de sauvegarde

Les administrateurs peuvent effectuer une récupération à l'aide de la clé Drive Encryption sauvegardée sur un périphérique de stockage amovible lors de l'activation ou en sélectionnant l'option **Sauvegarde des clés de cryptage de lecteur** dans Security Manager.

1. Insérez le périphérique de stockage amovible contenant la clé de sauvegarde.
2. Mettez l'ordinateur sous tension.
3. Lorsque la boîte de dialogue de connexion Drive Encryption for HP ProtectTools s'affiche, cliquez sur **Options**.
4. Cliquez sur **Restauration**.
5. Entrez le nom ou le chemin d'accès du fichier comprenant votre clé de sauvegarde, puis cliquez sur **Récupérer**.

   – ou –

   Cliquez sur **Parcourir** pour rechercher le fichier de sauvegarde requis, cliquez sur **OK**, puis sur **Récupérer**.
6. Lorsque la boîte de dialogue de confirmation s'affiche, cliquez sur **OK**.

   L'écran de connexion Windows s'affiche.

REMARQUE : Si vous utilisez la clé de récupération pour vous connecter dans l'écran de connexion de Drive Encryption, des informations d'authentification supplémentaires sont requises lors de la connexion à Windows pour accéder aux comptes d'utilisateurs. Il est vivement recommandé de réinitialiser le mot de passe après la restauration.

Récupération de HP SpareKey

Lors de la récupération de SpareKey au cours du préamorçage de Drive Encryption, vous devez répondre correctement à des questions de sécurité pour pouvoir accéder à l'ordinateur. Pour plus d'informations sur la configuration de la récupération de SpareKey, reportez-vous à l'aide du logiciel de Security Manager.

Pour effectuer une récupération de HP SpareKey si vous avez oublié votre mot de passe :

1. Mettez l'ordinateur sous tension.
2. Lorsque la page Drive Encryption for HP ProtectTools s'affiche, accédez à la page de connexion d'utilisateur.
3. Cliquez sur **SpareKey**.

   REMARQUE : Si votre SpareKey n'a pas été initialisée dans Security Manager, le bouton **SpareKey** n'est pas disponible.

4. Répondez correctement aux questions affichées, puis cliquez sur **Connexion**.

   L'écran de connexion Windows s'affiche.

REMARQUE : Si vous utilisez SpareKey pour vous connecter dans l'écran de connexion de Drive Encryption, des informations d'authentification supplémentaires sont requises lors de la connexion à Windows pour accéder aux comptes d'utilisateurs. Il est vivement recommandé de réinitialiser le mot de passe après la restauration.

Affichage de l'état du cryptage

Les utilisateurs peuvent afficher l'état du cryptage à partir de HP ProtectTools Security Manager.

REMARQUE : Les administrateurs peuvent modifier l'état de Drive Encryption à l'aide de la Console d'administration de HP ProtectTools.

1. Ouvrez la **Console utilisateur de HP ProtectTools**. Pour plus d'informations, reportez-vous à la section Ouverture de Security Manager à la page 26.
2. Sous **Mes données**, cliquez sur **Drive Encryption**.

   Dans le cas d'un cryptage logiciel ou matériel, l'un des codes d'état du cryptage d'unité suivants est affiché :

   - Activée
   - Désactivée

   Dans le cas d'un cryptage logiciel, l'un des états de cryptage d'unité suivants est affiché pour chaque disque dur ou partition de disque dur :

   - Non cryptée
   - Crypté
   - Cryptage
   - Décryptage

Dans le cas d’un cryptage matériel, l’un des codes d’état du cryptage d’unité suivants est affiché :

- Non cryptée
- Crypté

Si le disque dur est en cours de cryptage ou de décryptage, une barre de progression affiche le pourcentage achevé et le temps restant pour terminer le cryptage ou le décryptage.

7 Device Access Manager pour HP ProtectTools (certains modèles)

HP ProtectTools Device Access Manager contrôle l'accès aux données en désactivant les périphériques de transfert de données.

REMARQUE : certains périphériques de saisie ou d'interface utilisateur comme une souris, un clavier, un pavé tactile ou un lecteur d'empreintes digitales, ne sont pas contrôlés par Device Access Manager. Pour plus d'informations, reportez-vous à la section Classes de périphériques non gérées à la page 61.

Les administrateurs du système d'exploitation Windows® utilisent HP ProtectTools Device Access Manager pour contrôler l'accès aux périphériques d'un système et pour se protéger contre tout accès non autorisé :

- Des profils de périphérique sont créés pour chaque utilisateur, afin de définir les périphériques auxquels l'accès leur est autorisé ou refusé.
- L'authentification Just-in-time (JITA) permet aux utilisateurs prédéfinis de s'authentifier afin d'accéder aux périphériques, auxquels l'accès est sinon refusé.
- Les administrateurs et les utilisateurs fiables peuvent être exclus des restrictions d'accès imposées par Device Access Manager en les ajoutant au groupe Administrateurs de périphériques. L'adhésion à ce groupe est gérée à l'aide des paramètres avancés.
- L'accès au périphérique peut être octroyé ou refusé sur la base de l'adhésion à un groupe ou pour chaque utilisateur.
- Pour des classes de périphériques comme les lecteurs CD-ROM et DVD, l'accès en lecture ou en écriture peut être autorisé ou refusé séparément.

Ouverture de Device Access Manager

1. Connectez-vous en tant qu'administrateur.
2. Lancer **HP ProtectTools Security Manager** depuis **le tableau de bord de HP Client Security**.

   – ou –

   Sur le bureau Windows, double-cliquez sur l'icône **HP ProtectTools** dans la zone de notification, située à l'extrémité droite de la barre des tâches.

   – ou –

   Dans le **Panneau de configuration**, sélectionnez **Système et sécurité**, puis sélectionnez **HP ProtectTools Security Manager**.
3. Dans le volet gauche de la Console utilisateur de HP ProtectTools Security Manager, cliquez sur **Administration**, puis sélectionnez **Console d'administration**.
4. Dans le volet gauche de la Console d'administration, cliquez sur **Device Access Manager**.

Un utilisateur standard peut voir la stratégie de HP ProtectTools Device Access Manager en utilisant HP ProtectTools Security Manager. Cette console fournit une vue en lecture seule.

Procédures de configuration

Configuration de l'accès aux périphériques

HP ProtectTools Device Access Manager fournit quatre vues :

- **Configuration simple**—Autorise ou refuse l'accès à des classes de périphériques, en fonction de l'adhésion au groupe Administrateurs de périphériques.
- **Configuration de classe de périphérique**—Autorise ou refuse l'accès à des types de périphériques ou à des périphériques spécifiques pour des utilisateurs ou des groupes spécifiques.
- **Configuration JITA**—Configure l'authentification Just-in-time (JITA) qui permet aux utilisateurs sélectionnés d'accéder aux lecteurs de DVD/CD-ROM ou à des supports amovibles en s'authentifiant eux-mêmes.
- **Paramètres avancés**—Configure une liste de lettres d'unités pour lesquelles Device Access Manager ne limitera pas l'accès, comme le C ou l'unité système. L'adhésion au groupe Administrateurs de périphériques peut également se faire depuis cette vue.

Configuration simple

Les administrateurs peuvent utiliser la vue **Configuration simple** pour autoriser ou refuser l'accès aux classes de périphériques suivantes pour tous les non –Administrateurs de périphérique :

- Tous les supports amovibles (disquettes, unités flash USB, etc.).
- Tous les lecteurs de DVD/CD-ROM
- Tous les ports série ou parallèles
- Tous les périphériques Bluetooth

REMARQUE : si des périphériques Bluetooth sont utilisés en tant qu'informations d'authentification, l'accès aux périphériques Bluetooth ne doit pas avoir été restreint dans la stratégie Device Access Manager.

- Tous les modems
- Tous les périphériques PCMCIA/ExpressCard
- Tous les périphériques 1394

Pour autoriser ou refuser l'accès à une classe de périphérique pour tous les non administrateurs de périphériques, procédez comme suit :

1. Dans le volet gauche de la Console d'administration de HP ProtectTools, cliquez sur **Device Access Manager**, puis sur **Configuration simple**.
2. Dans le volet droit, pour refuser l'accès, sélectionnez la case à cocher en regard d'une classe de périphérique ou d'un périphérique spécifique. Désélectionnez la case à cocher pour autoriser l'accès à cette classe de périphérique ou à ce périphérique spécifique.

   Si une case à cocher est grisée, les valeurs affectant le scénario d'accès ont été modifiées dans la vue **Configuration de classe de périphérique**. Pour rétablir les paramètres d'usine, cliquez sur **Réinitialiser** dans la vue **Configuration de classe de périphérique**.

3. Cliquez sur **Appliquer**.

REMARQUE : Si le service d'arrière-plan n'est pas en cours d'exécution, une boîte de dialogue s'ouvre vous demandant si vous souhaitez le démarrer. Cliquez sur **Oui**.

4. Cliquez sur **OK**.

Démarrage du service d'arrière-plan

La première fois qu'une nouvelle stratégie est définie et appliquée, le service d'arrière-plan de HP ProtectTools Device Locking/Auditing démarre automatiquement et il est configuré pour démarrer automatiquement à chaque fois que le système démarre.

REMARQUE : Un profil de périphérique doit être défini avant que l'invite du service d'arrière-plan s'affiche.

Les administrateurs peuvent également démarrer ou arrêter ce service.

L'arrêt du service Verrouillage des périphériques / Audition n'arrête pas le verrouillage des périphériques. Deux composants renforcent le verrouillage des périphériques :

- Le service Verrouillage des périphériques/Audition
- Le pilote DAMDrv.sys

Le démarrage du service lance le pilote du périphérique, mais l'arrêt du service n'arrête pas le pilote.

Pour savoir si le service d'arrière-plan est en cours d'exécution, ouvrez une fenêtre d'invite de commande, puis saisissez `sc query flcdlock`.

Pour savoir si le pilote du périphérique est en cours d'exécution, ouvrez une fenêtre d'invite de commande, puis saisissez `sc query damdrv`.

Configuration de classe de périphérique

Les administrateurs peuvent afficher et modifier les listes des utilisateurs et des groupes pour qui l'accès aux classes de périphériques, ou à des périphériques spécifiques, est autorisé ou refusé.

La vue **Configuration de classe de périphérique** comporte les sections suivantes :

- **Liste des périphériques**—Affiche toutes les classes de périphériques et les périphériques installés sur le système ou pouvant l'avoir été auparavant.
  - La protection s'applique généralement à une classe de périphérique. Un utilisateur ou un groupe sélectionné sera en mesure d'accéder à tous les périphériques de la classe.
  - Une protection peut également être appliquée à des périphériques spécifiques.
- **Liste des utilisateurs**—Affiche tous les utilisateurs et les groupes pour qui l'accès à la classe de périphérique ou à un périphérique spécifique sélectionné est autorisé ou refusé.
  - La saisie dans la liste des utilisateurs peut être faite pour un utilisateur spécifique ou pour un groupe dans lequel l'utilisateur est membre.
  - Si une entrée utilisateur ou groupe de la Liste des utilisateurs n'est pas disponible, le paramètre a été hérité de la classe de périphérique dans la Liste des périphériques ou du dossier Classe.
  - Certaines classes de périphériques, telles que les DVD et les CD-ROM, peuvent être contrôlées de manière plus poussée en autorisant ou en refusant l'accès séparément pour les opérations de lecture et d'écriture.

Pour les autres périphériques et classes, les droits d'accès en lecture ou en écriture peuvent être hérités. Par exemple, l'accès en lecture peut être hérité d'une classe supérieure, alors que l'accès en écriture peut être refusé spécifiquement à un utilisateur ou à un groupe.

REMARQUE : si la case à cocher **Lecture** est vide, la saisie du contrôle d'accès n'a aucun effet sur l'accès en lecture au périphérique, mais l'accès en lecture n'est pas refusé.

REMARQUE : le groupe Administrateurs ne peut pas être ajouté à la liste des utilisateurs. Utilisez plutôt le groupe Administrateurs de périphérique.

Exemple 1—Si un utilisateur ou un groupe se voit refuser un accès en écriture pour un périphérique ou une classe de périphérique :

Le même utilisateur, le même groupe ou un membre du même groupe peut se voir accorder un accès en écriture ou un accès en lecture+écriture uniquement pour un périphérique se trouvant en dessous de ce périphérique dans la hiérarchie.

Exemple 2—Si un utilisateur ou un groupe se voit accorder un accès en écriture pour un périphérique ou une classe de périphérique :

Le même utilisateur, le même groupe ou un membre du même groupe peut se voir refuser un accès en écriture ou un accès en lecture+écriture uniquement pour le même périphérique ou un périphérique se trouvant en dessous de ce périphérique dans la hiérarchie.

Exemple 3—Si un utilisateur ou un groupe se voit accorder un accès en lecture pour un périphérique ou une classe de périphérique :

Le même utilisateur, le même groupe ou un membre du même groupe peut se voir refuser un accès en lecture ou un accès en lecture+écriture uniquement pour le même périphérique ou un périphérique se trouvant en dessous de ce périphérique dans la hiérarchie.

Exemple 4—Si un utilisateur ou un groupe se voit refuser un accès en lecture pour un périphérique ou une classe de périphérique :

Le même utilisateur, le même groupe ou un membre du même groupe peut se voir accorder un accès en lecture ou un accès en lecture+écriture uniquement pour un périphérique se trouvant en dessous de ce périphérique dans la hiérarchie.

Exemple 5—Si un utilisateur ou un groupe se voit accorder un accès en lecture+écriture pour un périphérique ou une classe de périphérique :

Le même utilisateur, le même groupe ou un membre du même groupe peut se voir refuser un accès en écriture ou un accès en lecture+écriture uniquement pour le même périphérique ou un périphérique se trouvant en dessous de ce périphérique dans la hiérarchie.

Exemple 6—Si un utilisateur ou un groupe se voit refuser un accès en lecture+écriture pour un périphérique ou une classe de périphérique :

Le même utilisateur, le même groupe ou un membre du même groupe peut se voir accorder un accès en lecture ou un accès en lecture+écriture uniquement pour un périphérique se trouvant en dessous de ce périphérique dans la hiérarchie.

Interdiction d'accès à un utilisateur ou à un groupe

Pour interdire à un utilisateur ou à un groupe d'accéder à un périphérique ou à une classe de périphérique :

1. Dans le volet gauche de la Console d'administration de HP ProtectTools, cliquez sur **Device Access Manager**, puis sur **Configuration de classe de périphérique**.
2. Dans la liste des périphériques, cliquez sur la classe de périphérique à configurer.
   - **Classe de périphérique**
   - **Tous les périphériques**
   - **Périphérique individuel**
3. Sous **Utilisateurs/Groupes**, cliquez sur l'utilisateur ou le groupe à qui refuser l'accès, puis cliquez sur **Refuser**.
4. Cliquez sur **Appliquer**.

REMARQUE : lorsque des paramètres d'autorisation et d'interdiction sont configurés au même niveau de périphérique pour un utilisateur, l'interdiction d'accès prévaut sur l'autorisation d'accès.

Autorisation d'accès pour un utilisateur ou un groupe

Pour octroyer l'autorisation à un utilisateur ou à un groupe d'accéder à un périphérique ou à une classe de périphérique :

1. Dans le volet gauche de la Console d'administration de HP ProtectTools, cliquez sur **Device Access Manager**, puis sur **Configuration de classe de périphérique**.
2. Dans la liste des périphériques, cliquez sur l'un des éléments suivants :
   - **Classe de périphérique**
   - **Tous les périphériques**
   - **Périphérique individuel**
3. Cliquez sur **Ajouter**.

   La boîte de dialogue **Sélection d'utilisateurs ou de groupes** s'affiche.
4. Cliquez sur **Avancés**, puis sur **Rechercher maintenant** pour rechercher des utilisateurs ou des groupes à ajouter.
5. Cliquez sur un utilisateur ou un groupe à ajouter à la liste des utilisateurs ou des groupes disponibles, puis cliquez sur **OK**.
6. Cliquez de nouveau sur **OK**.
7. Cliquez sur **Autoriser** pour octroyer l'accès à cet utilisateur.
8. Cliquez sur **Appliquer**.

Autorisation de l’accès à une classe de périphérique pour un seul utilisateur d’un groupe

Pour autoriser l'accès d'un utilisateur à une classe de périphérique, tout en le refusant à tous les autres membres de son groupe :

1. Dans le volet gauche de **Console d'administration de HP ProtectTools**, cliquez sur **Device Access Manager**, puis sur **Configuration de classe de périphérique**.
2. Dans la liste des périphériques, cliquez sur la classe de périphérique à configurer.
   - **Classe de périphérique**
   - **Tous les périphériques**
   - **Périphérique individuel**
3. Sous **Utilisateur/groupes**, sélectionnez le groupe pour lequel vous souhaitez refuser l'accès, puis cliquez sur **Refuser**.
4. Naviguez vers le dossier sous celui de la classe requise, puis ajoutez l'utilisateur spécifique.
5. Cliquez sur **Autoriser** pour autoriser l'accès à cet utilisateur.
6. Cliquez sur **Appliquer**.

Autorisation de l'accès à un périphérique spécifique pour un seul utilisateur d'un groupe

Les administrateurs peuvent autoriser l'accès à un périphérique spécifique, tout en le refusant à tous les autres membres du groupe de cet utilisateur pour tous les périphériques de la classe :

1. Dans le volet gauche de la Console d'administration de HP ProtectTools, cliquez sur **Device Access Manager**, puis sur **Configuration de classe de périphérique**.
2. Dans la liste des périphériques, cliquez sur la classe de périphérique à configurer, puis naviguez vers le dossier situé en dessous.
3. Sous **Utilisateur/groupes**, cliquez sur **Autoriser** à côté du groupe pour lequel autoriser l'accès.
4. Cliquez sur **Refuser** à côté du groupe pour lequel refuser l'accès.
5. Naviguez vers le périphérique spécifique auquel l'accès est à autoriser à l'utilisateur dans la liste des périphériques.
6. Cliquez sur **Ajouter**.

   La boîte de dialogue **Sélectionner des utilisateurs ou des groupes** s'ouvre.
7. Cliquez sur **Avancés**, puis sur **Rechercher maintenant** pour rechercher des utilisateurs ou des groupes à ajouter.
8. Cliquez sur un utilisateur pour lequel autoriser l'accès, puis sur **OK**.
9. Cliquez sur **Autoriser** pour autoriser l'accès à cet utilisateur.
10. Cliquez sur **Appliquer**.

Suppression des paramètres pour un utilisateur ou un groupe

Pour supprimer l'accès d'un utilisateur ou d'un groupe à un périphérique ou à une classe de périphérique, procédez comme suit :

1. Dans le volet gauche de la Console d'administration de HP ProtectTools, cliquez sur **Device Access Manager**, puis sur **Configuration de classe de périphérique**.
2. Dans la liste des périphériques, cliquez sur la classe de périphérique à configurer.
   - **Classe de périphérique**
   - **Tous les périphériques**
   - **Périphérique individuel**
3. Sous **Utilisateur/groupes**, cliquez sur l'utilisateur ou le groupe à supprimer, puis sur **Supprimer**.
4. Cliquez sur **Appliquer**.

Réinitialisation de la configuration

ATTENTION : la réinitialisation de la configuration supprime toutes les modifications de configuration des périphériques effectuées et rétablit tous les paramètres d'usine.

REMARQUE : la page Paramètres avancés n'est pas réinitialisée.

Pour rétablir les paramètres d'usine :

1. Dans le volet gauche de la Console d'administration de HP ProtectTools, cliquez sur **Device Access Manager**, puis sur **Configuration de classe de périphérique**.
2. Cliquez sur **Réinitialiser**.
3. Cliquez sur **Oui** à la demande de confirmation.
4. Cliquez sur **Appliquer**.

Configuration JITA

La configuration JITA permet aux administrateurs d'afficher et de modifier les listes des utilisateurs et des groupes auxquels l'accès aux périphériques est autorisé en utilisant l'authentification Just-In-Time (JITA).

Les utilisateurs pour lesquels l'authentification JITA est activée seront en mesure d'accéder à certains périphériques dont les stratégies créées dans la vue **Configuration de classe de périphérique** ou **Configuration simple** leur refusent l'accès.

- **Scénario**—Une stratégie de configuration simple est configurée pour refuser l'accès à tous les non Administrateurs de périphérique au lecteur de DVD/CD-ROM.
- **Résultat**—Un utilisateur pour lequel l'authentification JITA est activée qui tente d'accéder au lecteur de DVD/CD-ROM reçoit le même “message "accès refusé"” qu'un utilisateur n'ayant pas l'authentification JITA activée. Puis un message infobulle s'affiche, demandant si l'utilisateur souhaite un accès JITA. Si l'infobulle est cliquée, la boîte de dialogue d'authentification de l'utilisateur s'affiche. Lorsque l'utilisateur saisit les informations d'authentification avec succès, l'accès au lecteur de DVD/CD-ROM est octroyé.

La période JITA peut être autorisée pour un certain nombre de minutes ou 0 minute. Une période JITA de 0 minute n'expirera pas. Les utilisateurs auront accès au périphérique dès leur authentification jusqu'à ce qu'ils se déconnectent du système.

La période JITA peut également être étendue, si elle est configurée pour ce faire. Dans ce scénario, 1 minute avant l'expiration de la période JITA, les utilisateurs peuvent cliquer sur l'invite pour étendre leur accès sans avoir à s'authentifier à nouveau.

Que l'utilisateur ait une période JITA limitée ou illimitée, dès que l'utilisateur se déconnecte du système ou qu'un autre utilisateur se connecte, la période JITA s'expire. La prochaine fois que l'utilisateur se connecte et tente d'accéder à un périphérique ayant l'authentification JITA activée, une invite de saisie des informations d'authentification s'affiche.

L'authentification JITA est disponible pour les classes de périphérique suivantes :

- Lecteurs de DVD/CD-ROM
- Supports amovibles

Création d'une JITA pour un utilisateur ou un groupe

Les administrateurs peuvent permettre à des utilisateurs ou à des groupes d'accéder à des périphériques en utilisant l'authentification Just-In-Time.

1. Dans le volet gauche de la console d'administration de HP ProtectTools, cliquez sur **Device Access Manager**, puis sur **Configuration JITA**.
2. Depuis le ’menu déroulant du périphérique, sélectionnez **Support amovible** ou **Lecteurs de DVD/CD-ROM**.
3. Cliquez sur **+** pour ajouter un utilisateur ou un groupe à la configuration JITA.
4. Cochez la case **Activée**.
5. Configurez la période JITA sur la durée requise.
6. Cliquez sur **Appliquer**.

L'utilisateur doit se déconnecter puis se reconnecter pour que le nouveau paramètre JITA s'applique.

Création d'une JITA extensible pour un utilisateur ou un groupe

Les administrateurs peuvent permettre à un utilisateur ou à un groupe d'accéder à des périphériques en utilisant l'authentification Just-In-Time, que l'utilisateur peut étendre avant qu'elle n'expire.

1. Dans le volet gauche de la console d'administration de HP ProtectTools, cliquez sur **Device Access Manager**, puis sur **Configuration JITA**.
2. Depuis le ’menu déroulant du périphérique, sélectionnez **support amovible** ou **Lecteurs de DVD/CD-ROM**.
3. Cliquez sur **+** pour ajouter un utilisateur ou un groupe à la configuration JITA.
4. Cochez la case **Activée**.
5. Configurez la période JITA sur la durée requise.
6. Cochez la case **Extensible**.
7. Cliquez sur **Appliquer**.

L'utilisateur doit se déconnecter puis se reconnecter pour que le nouveau paramètre JITA s'applique.

Désactivation d'une JITA pour un utilisateur ou un groupe

Les administrateurs peuvent désactiver l'accès à des périphériques pour des utilisateurs ou des groupes en utilisant l'authentification Just-In-Time.

1. Dans le volet gauche de la console d'administration de HP ProtectTools, cliquez sur **Device Access Manager**, puis sur **Configuration JITA**.
2. Depuis le 'menu déroulant du périphérique, sélectionnez **support amovible** ou **Lecteurs de DVD/CD-ROM**.
3. Sélectionnez l'utilisateur ou le groupe auquel vous souhaitez désactiver l'authentification JITA.
4. Décochez la case **Activée**.
5. Cliquez sur **Appliquer**.

Lorsque l'utilisateur se connecte et tente d'accéder au périphérique, l'accès est refusé.

Paramètres avancés

Les paramètres avancés fournissent les fonctions suivantes :

- Gestion du groupe Administrateurs de périphériques
- Gestion des lettres d'unités auxquelles Device Access Manager ne refuse jamais l'accès.

Le groupe Administrateurs de périphériques est utilisé pour exclure les utilisateurs fiables (fiables par rapport à l'accès à un périphérique) des restrictions imposées par une stratégie de Device Access Manager. Les utilisateurs fiables comprennent généralement les administrateurs système. Pour plus d'informations, reportez-vous à la section Groupe Administrateurs de périphériques à la page 60.

La vue **Paramètres avancés** permet également aux administrateurs de configurer une liste de lettres d'unités auxquelles Device Access Manager ne refusera l'accès à aucun utilisateur.

REMARQUE : Les services d'arrière-plan de Device Access Manager doivent être en cours d'exécution lorsque la liste des lettres d'unités est configurée.

Pour démarrer ces services :

1. Appliquez une stratégie de configuration simple, comme refuser l'accès à tous les non administrateurs de périphériques aux supports amovibles.

   – ou –

   Ouvrez une fenêtre d'invite de commande avec des privilèges administrateurs, puis saisissez :

   ```
   sc start flcdlock
   ```

   Appuyez sur entrée.
2. Lorsque les services sont démarrés, la liste des unités peut être éditée. Entrez les lettres des unités des périphériques que vous ne souhaitez pas que Device Access Manager contrôle.

   Les lettres des unités sont affichées pour les disques durs physiques ou les partitions.

REMARQUE : que l'unité système (généralement C) soit dans la liste ou pas, son accès ne sera jamais refusé, pour tous les utilisateurs.

Groupe Administrateurs de périphériques

Lorsque Device Access Manager est installé, un groupe Administrateurs de périphériques est crée.

Le groupe Administrateurs de périphériques est utilisé pour exclure les utilisateurs fiables (fiables par rapport à l'accès à un périphérique) des restrictions imposées par une stratégie de Device Access Manager. Les utilisateurs fiables comprennent généralement les administrateurs système.

REMARQUE : L'ajout d'un utilisateur au groupe Administrateurs de périphériques n'autorise pas automatiquement l'utilisateur d'accéder aux périphériques. Dans la vue **Configuration de classe de périphérique**, si l'accès à un périphérique est refusé au groupe des utilisateurs, le groupe Administrateurs de périphériques doit octroyer l'accès afin que les membres du groupe aient accès au périphérique. Cependant, la vue **Configuration simple** peut être utilisée pour refuser l'accès à des classes de périphériques pour tous les utilisateurs qui ne sont pas membres du groupe Administrateurs de périphériques.

Pour ajouter des utilisateurs au groupe Administrateurs de périphériques :

1. Dans la vue **Paramètres avancés**, cliquez sur **+**.
2. Entrez le nom d'utilisateur de l'utilisateur fiable.
3. Cliquez sur **OK**.
4. Cliquez sur **Appliquer**.

Assistance périphérique eSATA

Afin que Device Access Manager contrôle les périphériques eSATA, les éléments suivants doivent être configurés :

1. L'unité doit être connectée lors du démarrage du système.
2. En utilisant la vue **Paramètres avancés**, assurez-vous que la lettre de l'unité eSATA n'est pas dans la liste des unités pour lesquelles Device Access Manager ne refusera pas l'accès. Si c'est le cas, supprimez la lettre de l'unité, puis cliquez sur **Appliquer**.
3. Le périphérique peut être contrôlé en utilisant la classe de périphérique Support amovible, en utilisant la vue **Configuration simple** ou la vue **Configuration de classe de périphérique**.

Classes de périphériques non gérées

HP ProtectTools Device Access Manager ne gère pas les classes de périphériques suivantes :

- Périphériques d'entrée/de sortie
  - Biometrique
  - Souris
  - Clavier
  - Imprimante
  - Imprimantes Plug and play (PnP)
  - Mise à niveau d'imprimante
  - Périphériques d'interface utilisateur infrarouge
  - Lecteur de Smart Card
  - Série multi-port
  - Unité de disque
  - Contrôleur de disquette (FDC)

- Contrôleur de disque dur (HDC)
- Classe de périphérique d'interface utilisateur infrarouge (HID)

- Alimentation
  - Batterie
  - Support de gestion de l'alimentation avancé (APM)
- Divers
  - Ordinateur
  - Décodeur
  - Affichage
  - Processeur
  - Système
  - Inconnu
  - Volume
  - Volume instantané
  - Périphériques de sécurité
  - Accélérateur de sécurité
  - Pilote d'affichage unifié Intel®
  - Pilote multimédia
  - Changeur de média
  - Multifonction
  - Legacard
  - Client Net
  - Service Net
  - Net trans
  - Adaptateur SCSI

8 Récupération en cas de vol (certains modèles)

Computrace for HP ProtectTools (acheté séparément) permet de surveiller, de gérer et de suivre l'ordinateur à distance.

Une fois activé, Computrace for HP ProtectTools est configuré depuis le Centre de clientèle Absolute Software. Depuis le Centre de clientèle, l'administrateur peut configurer Computrace for HP ProtectTools pour qu'il surveille ou gère l'ordinateur. Si le système est mal rangé ou volé, le Centre de clientèle peut aider les autorités locales à localiser et à récupérer l'ordinateur. Une fois configuré, Computrace peut continuer à fonctionner même si vous effacez ou remplacez le disque dur.

Pour activer Computrace for HP ProtectTools :

1. Connectez-vous à l'Internet.
2. Ouvrez la Console utilisateur de Security Manager. Pour plus d’informations, reportez-vous à la section Ouverture de Security Manager à la page 26.
3. Dans le volet gauche de Security Manager, cliquez sur **Récupération en cas de vol**.
4. Pour lancer l’Assistant d’activation Computrace, cliquez sur le bouton **Mise en route**.
5. Saisissez vos informations de contact, ainsi que les informations de paiement de votre carte de crédit ou saisissez une clé de produit achetée au préalable.

L’Assistant d’activation procède à la transaction de manière sécurisée et configure votre compte d’utilisateur sur le site Web du Centre de clientèle Absolute Software. Une fois cette opération effectuée, vous recevez un courrier électronique de confirmation contenant les informations de votre compte Centre de Clientèle.

Si vous avez précédemment lancé l'Assistant d'activation de Computrace et si votre compte Centre de Clientèle existe déjà, vous pouvez acheter des licences supplémentaires en contactant le représentant de votre compte HP.

Pour vous connecter au Centre de clientèle :

1. Accédez à https://cc.absolute.com/.
2. Dans les champs **ID de connexion** et **Mot de passe**, saisissez les informations d’authentification que vous avez reçues dans le courrier électronique de confirmation, puis cliquez sur le bouton **Connexion**.

Le Centre de clientèle permet d'effectuer les opérations suivantes :

- Surveiller les ordinateurs.
- Protéger vos données à distance.
- Signaler le vol de n'importe quel ordinateur protégé par Computrace.

▲ Pour plus d'informations sur Computrace for HP ProtectTools, cliquez sur **En savoir plus**.

9 Exceptions de mot de passe localisé

Aux niveaux de la sécurité de préamorçage et de HP Drive Encryption, la prise en charge de la localisation de mot de passe est limitée, comme décrit dans les sections suivantes.

Que faire lorsqu'un mot de passe est rejeté

Les mots de passe peuvent être rejetés pour les raisons suivantes :

- Un utilisateur utilise un IME non pris en charge. Il s'agit là d'une erreur habituelle lorsqu'il s'agit de langages à deux octets (coréen, japonais, chinois). Pour résoudre ce problème :

  1. À l'aide du **Panneau de configuration**, ajoutez une disposition de clavier prise en charge (ajouter un clavier anglais/américain sous langue d'entrée chinois).
  2. Définissez le clavier pris en charge comme entrée par défaut.
  3. Redémarrez HP ProtectTools, puis saisissez à nouveau le mot de passe.

- Un utilisateur utilise un caractère non pris en charge. Pour résoudre ce problème :

  1. Modifiez le mot de passe de Windows de manière à n'utiliser que des caractères pris en charge. Pour plus d'informations sur les caractères non pris en charge, reportez-vous à l'aide du logiciel de la Console d'administration de HP ProtectTools.
  2. Exécutez à nouveau l'Assistant de configuration de HP ProtectTools Security Manager, puis saisissez le nouveau mot de passe de Windows.

Les IME Windows ne sont pas pris en charge aux niveaux de la sécurité de préamorçage et de HP Drive Encryption

Dans Windows, l'utilisateur peut choisir un IME (éditeur de méthode d'entrée) pour saisir des caractères et des symboles complexes, comme des caractères japonais ou chinois, en utilisant un clavier occidental standard.

Les IME ne sont pas pris en charge aux niveaux de la sécurité de préamorçage et de HP Drive Encryption. Un mot de passe Windows ne peut être saisi par le biais d'un IME dans les écrans d'identification Sécurité de préamorçage ou HP Drive Encryption et procéder de la sorte peut générer une situation de blocage. Dans certains cas, Microsoft®Windows n'affiche pas l'IME lorsque l'utilisateur saisit le mot de passe.

La solution consiste à basculer vers l'une des dispositions de clavier prises en charge qui traduit selon la disposition de clavier 00000411 :

- Microsoft IME pour le japonais
- La disposition de clavier japonais
- Office 2007 IME pour le japonais—Si Microsoft ou une tierce partie utilise le terme IME ou un éditeur de méthode d'entrée, la méthode d'entrée peut ne pas être réellement un IME. Cela peut être source de confusion, mais le logiciel lit la représentation du code hexadécimal. Par conséquent, si un IME cartographie vers une disposition de clavier supportée, alors HP ProtectTools peut prendre en charge la configuration.

AVERTISSEMENT ! Lorsque HP ProtectTools est déployé, les mots de passe saisis avec un IME Windows sont rejetés.

Changements de mot de passe à l'aide d'une disposition de clavier également prise en charge

Si le mot de passe est initialement défini à l'aide d'une disposition de clavier particulière, comme celle pour l'anglais américain (409) et que l'utilisateur le modifie à l'aide d'une disposition de clavier différente également prise en charge, comme celle pour l'Amérique latine (080A), le changement de mot de passe fonctionnera dans HP Drive Encryption mais échouera dans le BIOS si l'utilisateur emploie des caractères existants dans la disposition en cours mais pas dans la précédente (par exemple, ē).

REMARQUE : Les administrateurs peuvent résoudre ce problème à l'aide de la fonctionnalité Gérer les utilisateurs de HP ProtectTools pour supprimer l'utilisateur de HP ProtectTools en sélectionnant la disposition de clavier désirée dans le système d'exploitation, puis en exécutant à nouveau l'assistant d'installation de Security Manager pour le même utilisateur. Le BIOS sauvegarde la disposition de clavier désirée, permettant aux mots de passe pouvant être saisis à l'aide de cette disposition de clavier d'être proprement défini dans le BIOS.

Un autre problème possible concerne l'utilisation de différentes dispositions de clavier pouvant chacune produire les mêmes caractères. Par exemple, la disposition de clavier U.S. International (20409) et celle pour l'Amérique latine (080A) peuvent produire le caractère é, même si différentes séquences de frappes peuvent être requises. Si un mot de passe est initialement défini à l'aide de la disposition de clavier pour l'Amérique latine, alors la disposition de clavier pour l'Amérique latine est définie dans le BIOS, même si le mot de passe est modifié par la suite à l'aide de la disposition de clavier U.S. International.

Gestion des touches spéciales

- Chinois, slovaque, français canadien et tchèque.

  Lorsqu'un utilisateur sélectionne l'une des dispositions de clavier précédentes, puis saisit un mot de passe (par exemple, abcdef), le même mot de passe doit être saisi tout en appuyant sur la touche shift pour les minuscules et les touches shift et maj. pour les majuscules dans Sécurité de préamorçage du BIOS et dans HP Drive Encryption. Les mots de passe numériques doivent être saisis à l'aide du pavé numérique.

- Coréen

  Lorsqu'un utilisateur sélectionne une dispositions de clavier coréen prise en charge, puis saisit un mot de passe, le même mot de passe doit être saisi tout en appuyant sur la touche alt de droite pour les minuscules et les touches alt et maj. de droite pour les majuscules dans Sécurité de préamorçage du BIOS et dans HP Drive Encryption.

- Les caractères non pris en charge sont listés dans le tableau suivant :

Langue	Windows	BIOS	Drive Encryption
Arabe	Les touches ﻷ, ﻹ et ﻵ génèrent deux caractères.	Les touches ﻷ, ﻹ et ﻵ génèrent un caractère.	Les touches ﻷ, ﻹ et ﻵ génèrent un caractère.
Français canadien	ç, è, à, et é avec verr maj sont Ç, È, À, et É dans Windows.	ç, è, à, et é avec verr maj sont ç, è, à, et é dans l'option de Sécurité de préamorçage du BIOS.	ç, è, à, et é avec verr maj sont ç, è, à, et é dans HP Drive Encryption.

Langue	Windows	BIOS	Drive Encryption
Espagnol	40a n'est pas pris en charge. Néanmoins, cela fonctionne parce que le logiciel le convertit vers c0a. Cependant, en raison de différences subtiles entre les dispositions de clavier, il est recommandé aux utilisateurs de langue espagnole de modifier la disposition de leur clavier sous Windows afin d'utiliser 1040a (variation espagnole) ou 080a (Amérique latine).	n/a	n/a
US international	◦ Les touches ¡, ¤, ‘, ’, ¥ et × situées sur la ligne du haut sont rejetées. ◦ Les touches å, ®, Þ, ’, ¥ et × situées sur la deuxième ligne sont rejetées. ◦ Les touches á, ð et ø situées sur la troisième ligne sont rejetées. ◦ La touche æ, située sur la ligne du bas est rejetée.	n/a	n/a
Tchèque	◦ La touche ğ est rejetée. ◦ La touche į est rejetée. ◦ La touche ų est rejetée. ◦ Les touches ė, ı, et ż sont rejetées. ◦ Les touches ģ, ķ, ļ, ņet ņ sont rejetées.	n/a	n/a
Slovaque	La touche ż est rejetée.	◦ Les touches š, ś et ş sont rejetées lors de la saisie, mais acceptées si saisies à l'aide du clavier logiciel. ◦ La touche morte ţ génère deux caractères.	n/a
Hongrois	La touche ż est rejetée.	La touche ţ génère deux caractères.	n/a

Langue	Windows	BIOS	Drive Encryption
Slovène	La touche żŻ est rejetée dans Windows et la touche alt génère une touche morte dans le BIOS.	Les touches ú, Ú, ů, Ů, ş, Ş, ś, Ś, š, et Š sont rejetées dans le BIOS.	n/a
Japonais	Un IME Microsoft Office 2007, lorsqu'il est disponible, constitue le meilleur choix. Peu importe le nom de l'IME, c'est réellement la disposition de clavier 411 qui est prise en charge.	n/a	n/a

Glossaire

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

administrateur
Reportez-vous à la section *administrateur Windows*.

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

archive de restauration d'urgence
Zone de stockage protégée permettant de crypter une nouvelle fois des clés utilisateur de base d'une clé de propriétaire de plate-forme à une autre.

authentification
Processus permettant de vérifier si un utilisateur est autorisé à exécuter une tâche, telle que l'accès à un ordinateur, la modification des paramètres d'un programme particulier ou l'affichage des données sécurisées.

authentification à la mise sous tension
Fonction de sécurité nécessitant certaines formes d'authentification (carte Smart Card, puce de sécurité ou mot de passe p. ex) lorsque l'ordinateur est allumé.

authentification unique
Fonction qui stocke des informations d'authentification et qui vous permet d'utiliser Security Manager pour accéder à des applications Internet et Windows nécessitant une authentification par mot de passe.

autorité de certification (AC)
Service chargé d'émettre les certificats requis pour l'exécution d'une infrastructure de clé publique.

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

carte d'identité
Gadget de bureau de Windows servant à identifier visuellement votre bureau à l’aide de votre nom d’utilisateur et d’une image choisie.

classe de périphérique
Tous les périphériques d'un type donné, par exemple les unités.

compte réseau
Compte utilisateur ou 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.

connexion
Objet de Security Manager, constitué d’un nom d’utilisateur et d’un mot de passe (et éventuellement d’autres informations sélectionnées), pouvant être utilisé pour se connecter à des sites Web ou à d’autres programmes.

console d’administration

Emplacement central à partir duquel les administrateurs peuvent accéder aux fonctions et paramètres de HP ProtectTools et les gérer.

cryptage
Une procédure, comme l'utilisation d'un algorithme, utilisée en cryptographie pour convertir du texte brut en texte codé afin d'empêcher la lecture des données par des destinataires non autorisés. Il y a plusieurs types de cryptage de données, ils constituent la base de la sécurité du réseau. Les types les plus courants incluent le cryptage de données standard et le cryptage de clé privée.

cryptographie
Pratique consistant à crypter et à décrypter des données pour qu'elles ne puissent être décodées que par des utilisateurs spécifiques.

décryptage
Procédure utilisée en cryptographie pour convertir les données cryptées en texte brute.

domaine
Groupe d'ordinateurs faisant partie d'un réseau et partageant une base de données d'annuaire commune. Le nom de chaque domaine est unique. Par ailleurs, chaque domaine dispose d'un ensemble de règles et de procédures courantes.

Drive Encryption
Protège vos données en cryptant vos disques durs, rendant ainsi les informations illisibles pour ceux ne disposant pas des autorisations adéquates.

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

écran de connexion de Drive Encryption
Ecran de connexion affiché avant le démarrage de Windows. Les utilisateurs doivent entrer leur nom d'utilisateur Windows, ainsi que leur mot de passe ou le code PIN de la carte Smart Card. Dans la plupart des cas, la saisie des informations correctes sur l'écran de connexion de Drive Encryption permet d'accéder directement à Windows sans avoir à se reconnecter sur l'écran de connexion Windows.

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

empreinte digitale
Extraction numérique de l'image de votre empreinte digitale. L'image réelle de votre empreinte digitale n'est jamais enregistrée par Security Manager.

fournisseur de service cryptographique
Fournisseur ou bibliothèque d'algorithmes de cryptage pouvant être utilisés dans une interface bien définie pour l'exécution de fonctions de cryptographiques particulières.

groupe
Plusieurs utilisateurs possédant le même niveau d'accès ou de refus d'accès à une classe de périphérique ou à un périphérique spécifique.

identité
Dans HP ProtectTools Security Manager, groupe d'informations d'authentification et de paramètres géré comme un compte ou un profil d'un utilisateur spécifique.

informations d'authentification
Moyens utilisés par un utilisateur pour prouver qu'il remplit les conditions requises pour exécuter une tâche particulière lors de l'authentification.

JITA
Authentification Just-In-Time.

méthode de connexion sécurisée
Méthode utilisée pour la connexion à l'ordinateur.

mode du périphérique SATA
Mode de transfert de données entre un ordinateur et des périphériques de stockage de masse (disques durs et lecteurs optiques p. ex).

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

PIN
Code d'identification personnel.

PKI
Norme relative à l'infrastructure de clé publique, définissant les interfaces de création, d'utilisation et d'administration de certificats et de clés cryptographiques.

Puce de sécurité intégrée TPM (Trusted Platform Module)
Terme générique pour désigner la puce de sécurité intégrée de HP ProtectTools. Une puce TPM authentifie un ordinateur, plutôt qu'un utilisateur, en stockant les informations spécifiques au système hôte, telles que les clés de cryptage, les certificats numériques et les mots de passe. Grâce à une TPM, les informations stockées sur l'ordinateur ne risquent pas d'être compromises par un vol physique ou une attaque perpétrée par un pirate externe.

Récupération de HP SpareKey
Possibilité d’accéder à l’ordinateur en répondant correctement aux questions de sécurité.

redémarrage
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.

restauration
Processus qui copie dans le programme actuel les informations sur le programme enregistrées dans un fichier de sauvegarde antérieur.

sauvegarde
Fonction qui permet de conserver une copie des informations importantes d'un programme dans un emplacement situé en dehors du programme. La sauvegarde peut être utilisée pour restaurer les informations à une date ultérieure sur le même ordinateur ou un ordinateur différent.

scène
Image d’un utilisateur inscrit utilisée pour l’authentification.

sécurité de connexion Windows
Protège l'accès à vos comptes Windows en exigeant l'utilisation d'informations d'authentification spécifiques.

service en arrière-plan
Le service d'arrière-plan de HP ProtectTools Device Locking/Auditing, qui doit être en cours d'exécution pour que les stratégies de contrôle d'accès aux périphériques soient appliquées. Il peut être accessible via l'application Services sous l'option Outils d'administration dans le panneau de configuration. S'il n'est pas encours d'exécution, HP ProtectTools Security Manager tente de le démarrer lorsque les stratégies de contrôle de l'accès aux périphériques sont appliquées.

Smart Card

Petit composant matériel, de mêmes dimensions qu'une carte de crédit, qui stocke les informations d'authentification du propriétaire. Permet d'authentifier le propriétaire d'un ordinateur.

stratégie de contrôle d'accès aux périphériques
Liste des périphériques auxquels un utilisateur est autorisé ou non à accéder.

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

utilisateur
Personne inscrite au programme Drive Encryption. Les utilisateurs non administrateurs disposent de droits limités dans Drive Encryption. Ils peuvent seulement s'inscrire (avec l'approbation de l'administrateur) et se connecter.

Index