HP ProtectTools
Manuel de l'utilisateur

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

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

Première édition : Octobre 2009

Référence du document : 572661-051

Sommaire

1 Introduction à la sécurité

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

Cette console permet à l'administrateur local d'effectuer les tâches suivantes :

- Activer ou désactiver les fonctions de sécurité
- Inscrire des empreintes digitales pour les utilisateurs de cet ordinateur
- Configurer une Smart Card
- Spécifier les informations de connexion requises pour l'authentification
- Gérer les utilisateurs de l'ordinateur
- Régler les paramètres spécifiques aux périphériques
- Configurer les applications de Security Manager installées
- Ajouter des applications de Security Manager supplémentaires

Les modules logiciels disponibles pour votre ordinateur peuvent varier en fonction de votre modèle.

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

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

Fonctions HP ProtectTools

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

Module	Principales fonctions
Credential Manager for HP ProtectTools	• Le Gestionnaire de mots de passe protège vos mots de passe et rationalise le processus d'authentification avec la fonction d'authentification unique (Single Sign On), qui mémorise et applique automatiquement les informations d'identification de l'utilisateur. • La fonction d'authentification unique offre également une protection supplémentaire en exigeant l'authentification au moyen de différentes technologies de sécurité combinées, par exemple des cartes Java™ Card ou des lecteurs biométriques. • Le stockage des mots de passe est protégé par un cryptage logiciel et peut être amélioré par le recours à une authentification au moyen de dispositifs de sécurité, par exemple des cartes Java Card ou des lecteurs biométriques. **REMARQUE :** Pour accéder à Credential Manager, sélectionnez l'option Gestionnaire de mots de passe dans HP ProtectTools Security Manager.
Drive Encryption for HP ProtectTools (certains modèles)	• Drive Encryption permet le cryptage total d'un disque dur sur l'ensemble du volume. • Drive Encryption force l'authentification au préamorçage afin de décrypter et accéder aux données.
Privacy Manager pour HP ProtectTools (certains modèles)	• Privacy Manager a recours à des techniques d'authentification avancées pour vérifier la source, l'intégrité et la sécurité des communications lorsque la messagerie, les documents Microsoft® Office ou la messagerie instantanée sont utilisés.
File Sanitizer pour HP ProtectTools	• File Sanitizer est un outil qui vous permet de détruire des ressources en toute sécurité (des informations confidentielles telles que des fichiers informatiques, historiques et données Web ou autres) se trouvant sur votre ordinateur et de nettoyer régulièrement le disque dur.
Device Access Manager pour HP ProtectTools (certains modèles)	• Device Access Manager permet aux responsables des départements informatiques de contrôler l'accès aux périphériques en fonction de profils utilisateur. • Device Access Manager empêche les utilisateurs non autorisés de retirer des données à l'aide de supports de stockage externes et d'introduire des virus dans le système via des supports externes. • L'administrateur peut interdire l'accès aux périphériques inscriptibles à des utilisateurs ou à des groupes d'utilisateurs sélectionnés.

Objectifs de sécurité fondamentaux

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

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

Protection contre le vol ciblé

Un exemple de vol ciblé consisterait à dérober un ordinateur contenant des données confidentielles et des informations client au niveau du point de contrôle d'un aéroport. Les fonctions suivantes permettent de vous protéger contre le vol ciblé :

- L'authentification au préamorçage, lorsqu'elle est activée, empêche tout accès au système d'exploitation. Voir les procédures suivantes :
  - Security Manager
  - Drive Encryption

Limitation de l'accès aux données confidentielles

Supposons qu'un auditeur de contrats travaille sur site et bénéficie d'un accès à des données financières confidentielles ; vous ne souhaitez pas que l'auditeur puisse imprimer les fichiers ni les enregistrer sur un support tel qu'un CD à l'aide d'un dispositif de gravure. Les fonctions suivantes vous aident à limiter l'accès aux données :

- Device Access Manager pour HP ProtectTools permet aux responsables informatiques de limiter l'accès aux périphériques de gravure pour empêcher l'impression ou la copie d'informations confidentielles depuis le disque dur vers un support amovible.

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

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

- L'authentification au préamorçage, lorsqu'elle est activée, empêche tout accès au système d'exploitation. Voir les procédures suivantes :
  - Gestionnaire de mots de passe
  - Drive Encryption
- Le Gestionnaire de mots de passe veille à ce que les utilisateurs non-autorisés ne puissent pas obtenir les mots de passe ou accéder aux applications protégées par mot de passe.

- Device Access Manager pour HP ProtectTools permet aux responsables informatiques de limiter l'accès aux périphériques de gravure pour empêcher la copie d'informations confidentielles depuis le disque dur.
- DriveLock veille à ce que les données ne puissent pas être lues, même si le disque dur est retiré et installé sur un système non sécurisé.

Création de stratégies de mots de passe complexes

Si l'utilisation d'une stratégie de mots de passe complexes est requise pour des dizaines de bases de données et d'applications Web, Security Manager fournit un référentiel sécurisé pour les mots de passe et permet de bénéficier de la fonction d'authentification unique.

Éléments de sécurité supplémentaires

Attribution des rôles de sécurité

Dans la gestion de la sécurité informatique (particulièrement dans le cas d'organisations de grande taille), une pratique importante consiste à répartir les responsabilités et les droits parmi divers types d'administrateurs et d'utilisateurs.

REMARQUE : Dans une petite organisation ou pour une utilisation individuelle, ces rôles peuvent être tenus par la même personne.

Dans le cas de HP ProtectTools, les responsabilités et les privilèges de sécurité peuvent être répartis suivant les rôles ci-dessous :

- Responsable de la sécurité : Définit le niveau de sécurité de l'entreprise ou du réseau et détermine les fonctions de sécurité à déployer, telles que les cartes Java™ Card, les lecteurs biométriques ou les jetons USB.

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

- Administrateur informatique : Applique et gère les fonctions de sécurité définies par le responsable de la sécurité. Il peut également activer et désactiver certaines fonctions. Par exemple, si le responsable de la sécurité a décidé de déployer des cartes Java Card, l'administrateur informatique peut activer le mode de sécurité BIOS de la Java Card.

- Utilisateur : Utilise les fonctions de sécurité. Par exemple, si le responsable de la sécurité et l'administrateur informatique ont activé des cartes Java Card pour le système, l'utilisateur peut définir le code PIN de la Java Card et utiliser la carte à des fins d'authentification.

△ **ATTENTION :** Les administrateurs sont encouragés à suivre les meilleures pratiques et à réduire les droits et l'accès des utilisateurs finaux.

Les utilisateurs non-autorisés ne doivent pas bénéficier de droits d'administration.

Gestion de mots de passe HP ProtectTools

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

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

Mot de passe HP ProtectTools	Défini dans ce module HP ProtectTools	Fonction
Mot de passe de connexion au module Security Manager	Security Manager	Ce mot de passe propose 2 options : • Il peut être utilisé pour la connexion à Security Manager après une connexion à Windows. • Il peut être utilisé pour autoriser l'accès à Windows et Security Manager simultanément.

Mot de passe HP ProtectTools	Défini dans ce module HP ProtectTools	Fonction
Mot de passe du fichier de restauration Security Manager	Security Manager, par l'administrateur informatique	Protège l'accès au fichier de restauration Security Manager.
Code PIN de la carte Java™ Card	Java Card Security	Protège l'accès au contenu de la Java Card et authentifie les utilisateurs de celle-ci. Lorsqu'il est utilisé pour l'authentification à la mise sous tension, le code PIN de Java Card protège également l'accès à l'utilitaire de configuration de l'ordinateur et au contenu de l'ordinateur. Authentifie les utilisateurs de Drive Encryption en cas de sélection du jeton Java Card.
Mot de passe de connexion Windows	Panneau de configuration Windows®	Peut être utilisé dans une connexion manuelle ou enregistré sur la Java Card.

Création d'un mot de passe sécurisé

Lorsque vous créez des mots de passe, vous devez d'abord suivre toutes les instructions définies par le programme. Toutefois, vous devez généralement prendre en compte les points suivants afin de pouvoir créer des mots de passe forts et réduire les risques de corruption de votre mot de passe :

- Utilisez des mots de passe contenant plus de 6 caractères et préférablement plus de 8.
- Utilisez des majuscules et des minuscules dans l'ensemble du mot de passe.
- Chaque fois que cela est possible, mélangez les caractères alphanumériques et incluez des caractères spéciaux et des signes de ponctuation.
- Remplacez les lettres d'un mot clé par des nombres ou caractères spéciaux. Par exemple, vous pouvez utiliser le chiffre 1 pour la lettre I ou L.
- Associez des mots de 2 langues ou plus.
- Divisez un mot ou une phrase par des nombres ou des caractères spéciaux au milieu. Par exemple, «Mary2-2Cat45».
- N'utilisez pas un mot de passe figurant dans un dictionnaire.
- N'utilisez pas votre nom comme mot de passe, ou toute autre information personnelle, telle qu'une date de naissance, le nom de votre chien ou le nom de jeune fille de votre mère, même en l'épelant à l'envers.
- Modifiez les mots de passe régulièrement. Vous pouvez souhaiter ne modifier que quelques caractères par incrément.
- Si vous notez votre mot de passe, ne le placez pas en un lieu visible, à proximité de l'ordinateur.
- N'enregistrez pas le mot de passe dans un fichier, tel qu'un message électronique, sur l'ordinateur.
- Ne partagez pas de comptes et ne communiquez votre mot de passe à personne.

Sauvegarde et restauration des informations d'authentification de HP ProtectTools

Vous pouvez utiliser Drive Encryption for HP ProtectTools pour sélectionner et sauvegarder les informations d'authentification de HP ProtectTools.

2 Mise en route

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

L'Assistant d'installation de HP ProtectTools vous guide dans la configuration des fonctions les plus courantes de Security Manager. Cependant, vous trouverez un grand nombre de fonctions supplémentaires dans la console d'administration de HP ProtectTools. Les paramètres accessibles dans l'Assistant, ainsi que des fonctions de sécurité supplémentaires, peuvent être configurés dans la console, accessible depuis le menu Démarrer de Windows®. Ces paramètres s'appliquent à l'ordinateur ainsi qu'à tous les utilisateurs qui partagent l'ordinateur.

1. La page de bienvenue permet de désactiver l'affichage de l'Assistant en y sélectionnant l'une des options.
2. Une semaine après la configuration de l'ordinateur, ou lorsque qu'un utilisateur bénéficiant de droits d'administration passe un doigt sur le lecteur d'empreintes digitales pour la première fois, l'Assistant d'installation de HP ProtectTools démarre automatiquement pour vous guider pas à pas dans la configuration du programme. Un didacticiel vidéo présentant la configuration de votre ordinateur démarre automatiquement.
3. Suivez les instructions à l'écran jusqu'à ce que la configuration soit terminée.

Si vous ne suivez pas l'Assistant jusqu'au bout, il se lancera automatiquement deux autres fois. Ensuite, vous pourrez accéder à l'Assistant depuis la bulle de notification qui s'affiche près de la zone de notification de la barre des tâches (sauf si vous l'avez désactivée en suivant l'étape 2 ci-dessus) jusqu'à ce que la configuration soit terminée.

Pour utiliser les applications de HP ProtectTools Security Manager, lancez celui-ci depuis le menu Démarrer ou cliquez avec le bouton droit de la souris sur l'icône Security Manager de la zone de notification, située à l'extrémité droite de la barre des tâches. La console d'administration de HP ProtectTools et ses applications sont accessibles à tous les utilisateurs qui partagent l'ordinateur.

Ouverture de la console d'administration de HP ProtectTools

Pour les tâches administratives, telles que la définition de politiques système ou la configuration du logiciel, ouvrez la console comme suit :

- Cliquez sur **Démarrer**, **Tous les programmes**, **HP**, puis sélectionnez **Console d'administration de HP ProtectTools**.

  – ou –

  Dans le panneau de gauche de Security Manager, cliquez sur **Administration**.

Pour les tâches utilisateur, par exemple l'inscription des empreintes digitales ou l'utilisation de Security Manager, ouvrez la console comme suit :

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

  – ou –

  Double-cliquez sur l'icône **HP ProtectTools Security Manager** dans la zone de notification, à l'extrémité droite de la barre des tâches.

Activation des fonctions de sécurité

L'Assistant d'installation vous demande de vérifier votre identité.

1. Lisez l'écran « Bienvenue », puis cliquez sur **Suivant**.
2. Vérifiez votre identité, soit en saisissant votre mot de passe Windows si vous n'avez pas encore enregistré d'empreinte digitale, soit en analysant votre empreinte digitale avec le lecteur d'empreintes digitales. Cliquez sur **Suivant**.

   Si vous n'avez pas de mot de passe Windows, vous serez invité à en créer un. Un mot de passe Windows est requis afin de protéger l'accès à votre compte Windows par des personnes non autorisées et d'utiliser les fonctions de HP ProtectTools Security Manager.

L'Assistant d'installation vous guide pas à pas pour activer les fonctions de sécurité qui s'appliquent à tous les utilisateurs de l'ordinateur :

- La sécurité de la connexion Windows protège votre ou vos comptes Windows en requérant l'utilisation d'informations d'authentification spécifiques avant d'autoriser l'accès.
- Drive Encryption protège vos données en cryptant votre ou vos disques durs, rendant les informations illisibles pour les personnes ne disposant pas des autorisations requises.
- Pre-boot Security protège votre ordinateur en interdisant l'accès aux personnes non autorisées avant le démarrage de Windows.

Pour activer une fonction de sécurité, sélectionnez la case à cocher correspondante. Plus vous sélectionnez de fonctions, plus votre ordinateur sera sécurisé.

REMARQUE : Pre-Boot Security n'est pas disponible si votre BIOS ne le prend pas en charge.

Inscription de vos empreintes digitales

Si vous avez sélectionné « Empreinte » et que votre ordinateur dispose d'un lecteur d'empreintes digitales intégré ou externe, vous êtes guidé au cours du processus de configuration ou d'inscription de vos empreintes digitales :

1. Une représentation de deux mains est affichée. Les doigts déjà inscrits sont surlignés en vert. Cliquez sur un doigt de la représentation.

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

2. Une fois que vous avez sélectionné un doigt à inscrire, vous êtes invité à analyser cette empreinte jusqu'à ce qu'elle soit correctement inscrite. Un doigt inscrit est surligné en vert sur la représentation.

3. Vous devez inscrire au moins deux doigts. L'index ou le majeur sont préférables. Répétez les étapes 1 à 3 pour un autre doigt.

4. Cliquez sur **Suivant**.

REMARQUE : Lorsque vous inscrivez des empreintes digitales à l'aide du processus de mise en route, les informations correspondantes ne sont pas enregistrées tant que vous n'avez pas cliqué sur **Suivant**. Si vous laissez l'ordinateur inactif pendant un moment ou que vous fermez le tableau de bord, les modifications que vous avez effectuées **ne sont pas** enregistrées.

Configuration d'une Smart Card

Si vous avez sélectionné « Smart card » et qu'un lecteur de Smart Card est intégré ou connecté à votre ordinateur, l'Assistant d'installation de HP ProtectTools vous invite à configurer un code PIN pour la Smart Card.

Pour configurer un code PIN de Smart Card :

1. Sur la page « Configurer une Smart Card », saisissez et confirmez un code PIN.

   Vous pouvez également modifier votre code PIN. Fournissez votre ancien code PIN, puis choisissez-en un nouveau.

2. Pour continuer, cliquez sur **Suivant**.

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.

La console se compose des éléments suivants :

- **Outils**—Affiche les catégories suivantes de configuration de la sécurité sur votre ordinateur :
  - **Accueil**—Vous permet de sélectionner les tâches de sécurité à effectuer.
  - **Système**—Vous permet de configurer les fonctions de sécurité et l'authentification pour les utilisateurs et les périphériques.
  - **Applications**—Affiche les paramètres généraux de HP ProtectTools Security Manager et des applications de Security Manager.
  - **Données**—Propose un menu expansible de liens vers les applications de Security Manager qui protègent vos données.
- **Outils de gestion**—Fournit des informations sur des outils supplémentaires. Le panneau du dessous affiche les choix suivants :
  - **Assistant d'installation de HP ProtectTools** : Vous guide pas à pas pour configurer HP ProtectTools Security Manager.
  - **Aide** : Affiche le fichier d'aide, qui fournit des informations sur Security Manager et ses applications préinstallées. L'aide des applications que vous ajoutez au fur et à mesure se trouve au sein de ces applications.
  - **À propos de**—Affiche des informations sur HP ProtectTools Security Manager, telles que le numéro de version et les informations sur les droits d'auteur.
- **Zone principale**—Affiche les écrans spécifiques aux applications.

Pour ouvrir la console d'administration de HP ProtectTools, cliquez sur **Démarrer**, **Tous les programmes**, **HP**, puis sélectionnez **Console d'administration de HP ProtectTools**.

3 Configuration de votre système

Le groupe Système est accessible via le panneau du menu Outils, situé à gauche de l'écran 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.
- **Périphériques**—Gérez les paramètres des périphériques de sécurité intégrés ou connectés à l'ordinateur.

Configuration de l'authentification pour votre ordinateur

Dans l'application Authentification, vous pouvez sélectionner les fonctions de sécurité à mettre en place sur cet ordinateur, définir les règles d'accès à l'ordinateur et configurer des paramètres avancés supplémentaires. Vous pouvez spécifier les informations de connexion 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 menu du panneau Sécurité, cliquez sur **Authentification**.
2. Pour configurer l'authentification de la connexion, cliquez sur l'onglet **Règles de connexion**, effectuez les modifications et cliquez sur **Appliquer**.
3. Pour configurer l'authentification de la session, cliquez sur l'onglet **Règles de session**, effectuez les modifications et 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 menu Outils, cliquez sur **Sécurité**, puis sur **Authentification**.
2. Dans l'onglet **Règles de connexion**, cliquez sur une catégorie d'utilisateur.
3. Spécifiez les informations d'authentification requises pour la catégorie d'utilisateur sélectionnée. Vous devez spécifier au moins une information.
4. Indiquez si une seule des informations d'authentification est requise pour authentifier un utilisateur ou si elles sont toutes requises. Vous pouvez également empêcher tous les utilisateurs d'accéder à l'ordinateur.
5. Cliquez sur **Appliquer**.

Règles de session

Pour définir les règles relatives aux informations d'authentification requises pour accéder aux applications de HP ProtectTools au cours d'une session Windows :

1. Dans le menu Outils, cliquez sur **Sécurité**, puis sur **Authentification**.
2. Dans l'onglet **Règles de session**, cliquez sur une catégorie d'utilisateur.
3. Spécifiez les informations d'authentification requises pour la catégorie d'utilisateur sélectionnée.
4. Indiquez si une seule des informations d'authentification est requise pour authentifier un utilisateur ou si elles sont toutes requises. Pour pouvez également ne demander aucune authentification pour accéder au logiciel HP ProtectTools.
5. Cliquez sur **Appliquer**.

Paramètres

Vous pouvez autoriser un ou plusieurs des paramètres de sécurité suivants :

- **Autoriser la connexion directe**—Permet aux utilisateurs de cet ordinateur d'ignorer la connexion Windows si l'authentification a été effectuée au niveau du BIOS ou du disque crypté.
- **Autoriser l'authentification HP SpareKey pour la connexion Windows**—Permet aux utilisateurs de cet ordinateur d'utiliser la fonction HP SpareKey pour se connecter à Windows en dépit de toute autre règle d'authentification requise par Security Manager.

Pour modifier les paramètres :

1. Cliquez pour activer ou désactiver un paramètre spécifique.
2. Cliquez sur **Appliquer** pour enregistrer les modifications effectuées.

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 ajouter des utilisateurs supplémentaires, cliquez sur **Ajouter**.

Pour supprimer un utilisateur, cliquez sur celui-ci, puis sur **Supprimer**.

Pour inscrire des empreintes digitales ou configurer des informations d'authentification supplémentaires pour l'utilisateur, cliquez sur celui-ci, puis sur **Enregistrement**.

Pour afficher les règles d'un utilisateur spécifique, sélectionnez ce dernier, puis cliquez sur **Afficher les règles**.

Spécification des paramètres de périphérique

Dans l'application Périphérique, vous pouvez spécifier les paramètres disponibles pour tous les périphériques de sécurité intégrés ou externes reconnus par HP ProtectTools Security Manager.

Empreintes digitales

La page Empreintes digitales comporte trois onglets : Enregistrement, Sensibilité et Avancé.

Enregistrement

Vous pouvez choisir 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.

⚠ **AVERTISSEMENT !** Les données relatives aux empreintes digitales de tous les utilisateurs, administrateurs compris, seront intégralement supprimées. Si les règles de connexion requièrent uniquement les empreintes digitales, cette suppression risque d'empêcher tous les utilisateurs de se connecter à l'ordinateur.

Sensibilité

Déplacez le curseur pour régler la sensibilité du lecteur d'empreintes digitales lors de l'analyse de vos empreintes digitales.

Si votre empreinte digitale n'est pas reconnue à chaque passage, un paramètre de sensibilité plus faible est peut-être nécessaire. Un paramètre élevé augmente la sensibilité aux variations des analyses de l'empreinte digitale et réduit par conséquent la possibilité d'une acceptation erronée. Le paramètre Moyen-Élevé offre un bon compromis de sécurité et de confort.

Avancé

Vous pouvez configurer le lecteur d'empreintes digitales pour qu'il économise l'énergie lorsque l'ordinateur fonctionne sur batterie.

Smart Card

Vous pouvez configurer l'ordinateur pour qu'il se verrouille automatiquement lorsqu'une Smart Card est retirée. Cependant, 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.

- Sélectionnez la case à cocher pour activer ou désactiver le verrouillage de l'ordinateur lors du retrait de la Smart Card.

4 Configuration de vos applications

Le groupe Applications est accessible via le panneau du menu Applications de sécurité, situé à gauche de la console d'administration de HP ProtectTools. Vous pouvez utiliser Paramètres pour personnaliser le comportement des applications de HP ProtectTools Security Manager actuellement installées.

Pour modifier vos paramètres d'application :

1. Dans le menu Outils, depuis le groupe **Applications**, cliquez sur **Paramètres**.
2. Cliquez pour activer ou désactiver un paramètre spécifique.
3. Cliquez sur **Appliquer** pour enregistrer les modifications effectuées.

Onglet Général

Les paramètres suivants sont disponibles dans l'onglet Général :

- **Do not automatically launch the Setup Wizard for administrators** (Ne pas lancer automatiquement l'Assistant d'installation pour les administrateurs) : Sélectionnez cette option pour empêcher l'ouverture automatique de l'Assistant 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.

Onglet Applications

Les paramètres affichés ici peuvent changer lors de l'ajout de nouvelles applications à Security Manager. Les paramètres minimaux affichés par défaut sont les suivants :

- **Security Manager** : Active l'application Security Manager pour tous les utilisateurs de l'ordinateur.
- **Activer le bouton En découvrir plus** : Permet à tous les utilisateurs de cet ordinateur d'ajouter des applications à HP ProtectTools Security Manager en cliquant sur le bouton **[+] En découvrir plus**.

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

5 Ajout d'outils de gestion

Des applications supplémentaires peuvent être disponibles pour l'ajout de nouveaux outils de gestion à Security Manager. L'administrateur de cet ordinateur peut désactiver cette fonction via l'application Paramètres.

Pour ajouter des outils de gestion, cliquez sur **[+] Outils de gestion**.

Vous pouvez accéder au site Web de DigitalPersona, pour y rechercher de nouvelles applications, ou planifier des mises à jour automatiques.

6 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 vos connexion et 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
- Configurer une Smart Card pour l'authentification
- Sauvegarder et restaurer les données du programme
- Ajouter des applications

Procédures de configuration

Mise en route

L'Assistant d'installation de HP ProtectTools s'affiche automatiquement comme page par défaut de HP ProtectTools Security Manager tant que la configuration n'a pas été terminée.

Pour configurer Security Manager, procédez comme suit :

REMARQUE : Si ni le lecteur d'empreintes digitales, ni la Smart Card ne sont disponibles, effectuez uniquement les étapes 1, 5 et 6.

1. Dans la page de bienvenue, cliquez sur **Suivant**.
2. La page suivante répertorie les méthodes d'authentification disponibles sur cet ordinateur. Cliquez sur **Suivant** pour poursuivre.
3. Dans la page Vérifiez votre identité, entrez votre mot de passe Windows, puis cliquez sur **Suivant**.
4. Voir une ou plusieurs des rubriques suivantes selon la configuration de votre ordinateur.
   - Si un lecteur d'empreintes digitales est disponible, reportez-vous à la section Inscription de vos empreintes digitales à la page 24.
   - Si une carte Smart Card est disponible, reportez-vous à la section Configuration d'une Smart Card à la page 25.
5. Si ni le lecteur d'empreintes digitales, ni la Smart Card ne sont disponibles, vous serez invité à saisir votre mot de passe Windows. Vous utiliserez ensuite ce mot de passe chaque fois qu'une authentification sera requise.
6. Dans la dernière page de l'Assistant, cliquez sur **Terminer**.

   Le tableau de bord de Security Manager s'affiche.

Enregistrement d'informations d'authentification

Vous pouvez utiliser la page « Mon identité » pour enregistrer vos diverses méthodes ou informations d'authentification. Une fois ces éléments enregistrés, vous pouvez les utiliser pour vous connecter à Security Manager.

Inscription de vos empreintes digitales

Si un lecteur d'empreintes digitales est intégré ou connecté à votre ordinateur, l'Assistant d'installation de HP ProtectTools vous guide pas à pas pour configurer ou inscrire vos empreintes digitales.

1. Lisez l'écran « Bienvenue », puis cliquez sur **Suivant**.
2. Vérifiez votre identité, soit en saisissant votre mot de passe Windows si vous n'avez pas encore enregistré d'empreinte digitale, soit en analysant votre empreinte digitale avec le lecteur d'empreintes digitales. Cliquez sur **Suivant**.

   Si vous n'avez pas de mot de passe Windows, vous serez invité à en créer un. Un mot de passe Windows est requis afin de protéger l'accès à votre compte Windows par des personnes non autorisées et d'utiliser les fonctions de HP ProtectTools Security Manager.

3. La silhouette de deux mains est affichée. Les empreintes déjà inscrites sont surlignées en vert. Cliquez sur une empreinte sur la silhouette.

REMARQUE : Pour supprimer une empreinte inscrites, cliquez sur l'empreinte correspondante.

4. Une fois que vous avez sélectionné un doigt à inscrire, vous êtes invité à analyser cette empreinte jusqu'à ce qu'elle soit correctement inscrite. Un doigt inscrit est surligné en vert sur la silhouette.

5. Vous devez inscrire au moins deux doigts. L'index ou le majeur sont préférables. Répétez les étapes 3 et 4 pour un autre doigt.

6. Cliquez sur **Suivant**.

REMARQUE : Lorsque vous inscrivez des empreintes digitales à l'aide du processus de mise en route, 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 tableau de bord, les modifications que vous avez effectuées **ne sont pas** enregistrées.

Modification du 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 le tableau de bord de Security Manager, cliquez sur **Mon identité**, sur **Informations d'authentification**, 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 Smart Card

Si un lecteur de Smart Card est intégré ou connecté à l'ordinateur, Security Manager vous invite à configurer un code PIN (Personal Identification Number, numéro d'identification personnel) de Smart Card.

- Pour définir le code PIN d'une Smart Card : sur la page « Configurer une Smart Card », saisissez et confirmez un code PIN.

- Pour modifier votre code PIN : saisissez tout d'abord l'ancien code PIN, puis choisissez-en un nouveau.

Utilisation du tableau de bord de Security Manager

Le tableau de bord de Security Manager est l'emplacement central qui permet d'accéder aisément aux fonctionnalités, applications et paramètres de Security Manager.

Le tableau de bord se compose des éléments suivants :

- **Carte d'identité** : affiche le nom d'utilisateur Windows et une image sélectionnée identifiant le compte utilisateur connecté.
- **Applications de sécurité** : affiche un menu expansible des liens de configuration des catégories de sécurité suivantes :
  - **Mon identité**
  - **Mes données**
  - **Poste de travail**
- **En découvrir plus** : ouvre une page dans laquelle vous pouvez trouver des applications supplémentaires pour améliorer la sécurité de votre identité, de vos données et de vos communications.
- **Zone principale** : affiche les écrans spécifiques aux applications.
- **Administration** : ouvre la console d'administration de HP ProtectTools.
- **Bouton Aide** : affiche des informations sur l'écran actuel.
- **Avancé** : vous permet d'accéder aux options suivantes :
  - **Préférences** : vous permet de personnaliser les paramètres de Security Manager.
  - **Sauvegarder et restaurer** : vous permet de sauvegarder ou de restaurer les données.
  - **À propos de** : affiche des informations de version à propos de Security Manager.

Pour ouvrir le tableau de bord de Security Manager, cliquez sur **Démarrer**, **Tous les programmes**, **HP**, puis sélectionnez **HP ProtectTools Security Manager**.

Ouverture de HP ProtectTools Security Manager

Vous pouvez ouvrir HP ProtectTools Security Manager en procédant de l'une des façons suivantes :

- Cliquez sur **Démarrer**, **Tous les programmes**, **HP**, puis sélectionnez **HP ProtectTools Security Manager**.
- Double-cliquez sur l'icône **HP ProtectTools** dans la zone de notification, à l'extrémité droite de la barre des tâches.
- Cliquez avec le bouton droit de la souris sur l'icône **HP ProtectTools**, puis sur **Ouvrir HP ProtectTools Security Manager**.
- Cliquez sur le gadget **Carte d'identité de Security Manager** dans la barre latérale de Windows.
- Appuyez sur la combinaison de touches d'accès rapide ctrl+alt+h pour ouvrir le menu Liens rapides de Security Manager.

Tâches générales

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

- **Security Manager** : Crée et gère les liens rapides, qui vous permettent de lancer et de vous connecter à des sites Web et programmes en vous authentifiant à l'aide de votre mot de passe Windows, votre empreinte digitale ou votre carte Smart Card.
- **Informations d'authentification** : fournit un moyen de changer aisément votre mot de passe Windows, d'inscrire vos empreintes digitales ou de configurer une Smart Card.

Pour ajouter d'autres applications, cliquez sur le bouton [+] **En découvrir plus** dans le coin inférieur gauche du tableau de bord. Ce bouton peut être désactivé par l'administrateur.

Gestionnaire de mots de passe

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 rapidement avec une empreinte digitale, une Smart Card ou votre mot de passe Windows.

Le Gestionnaire de mots de passe offre les options suivantes :

- Ajout, modification ou suppression des connexions de l'onglet Gérer.
- Utilisation de 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.
- Voir en un seul coup d'œil si certains de vos mots de passe présentent un risque de sécurité et générer automatiquement un mot de passe fort complexe à utiliser pour de nouveaux sites.

Les fonctionnalités du Gestionnaire de mots de passe sont également disponibles à partir de l'icône Gestionnaire de mots de passe affichée lorsqu'une page Web ou un écran de connexion au programme est actif. Cliquez sur l'icône pour afficher un menu contextuel dans lequel vous pouvez choisir parmi les options suivantes.

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

Les options suivantes apparaissent 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** : vous permet d'indiquer les conditions d'affichage de l'icône Gestionnaire de mots de passe.
- **Aide** : affiche l'aide du logiciel Gestionnaire de mots de passe.

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

Les options suivantes apparaissent dans le menu contextuel :

- **Remplir les données de connexion** : place vos données de connexion dans les champs de connexion, puis soumet la page (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 les données de connexion pour ce site Web.
- **Ajouter un nouveau compte** : vous permet d'ajouter un compte à une connexion.
- **Ouvrir le Gestionnaire de mots de passe** : lance le Gestionnaire de mots de passe.
- **Aide** : affiche l'aide du logiciel Gestionnaire de mots de passe.

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

Pour ajouter une connexion :

1. Ouvrez l'écran de connexion d'un site Web ou d'un programme.
2. Cliquez sur la flèche située sur l'icône **Gestionnaire de mots de passe**, 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. À l'écran, les champs de connexion et les champs correspondants de la boîte de dialogue sont identifiés par une bordure orange en gras. Vous pouvez également afficher cette boîte de dialogue en cliquant sur **Ajouter une connexion** dans l'onglet **Gestion avec le Gestionnaire de mots de passe**. Certaines options dépendent des périphériques de sécurité connectés à l'ordinateur, par exemple, la touche d'accès rapide ctrl+alt +H, la lecture de votre empreinte digitale, l'insertion d'une Smart Card.
   - Pour remplir un champ de connexion avec l'un des choix préformatés, cliquez sur les flèches à droite du champ.
   - Pour ajouter des champs de connexion dans l'écran, cliquez sur **Choisir d'autres champs**.
   - Pour que les champs de connexion soient remplis, mais non soumis, désactivez la case à cocher **Soumettre les données de connexion**.
   - Pour consulter le mot de passe de cette connexion, cliquez sur **Afficher le mot de passe**.
4. Cliquez sur **OK**.

Le signe plus est supprimé de l'icône Gestionnaire de mots de passe afin de vous indiquer que la connexion a été créée.

Chaque fois que vous accédez à ce site Web ou que vous ouvrez ce programme, l'icône Gestionnaire des mots de passe s'affiche et vous indique que vous pouvez utiliser vos 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 **Gestionnaire de mots de passe**, puis cliquez sur **Modifier la connexion**. À l'écran, les champs de connexion et les champs correspondants de la boîte de dialogue sont identifiés par une bordure orange en gras.

   Vous pouvez également afficher la boîte de dialogue en cliquant sur **Modifier pour obtenir la connexion souhaitée** dans l'onglet **Gestion par le Gestionnaire de mots de passe**.
3. Modifiez vos informations de connexion.
   - Pour remplir un champ de connexion avec l'un des choix préformatés, cliquez sur les flèches à droite du champ.
   - Pour ajouter des champs de connexion dans l'écran, cliquez sur **Choisir d'autres champs**.
   - Pour que les champs de connexion soient remplis, mais non soumis, désactivez la case à cocher **Soumettre les données de connexion**.
   - Pour consulter le mot de passe de cette connexion, cliquez sur **Afficher le mot de passe**.
4. Cliquez sur **OK**.

Utilisation du menu des connexions

Le Gestionnaire de mots de passe 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 **Connexions** ou dans l'onglet **Gérer** du **Gestionnaire de mots de passe** pour ouvrir l'écran de connexion, puis remplissez vos données de connexion.

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

Pour afficher le menu des connexions :

1. Appuyez sur la combinaison de touches d'accès rapide correspondant au **Gestionnaire de mots de passe**. ctrl+alt+h est le paramètre par défaut. Pour changer cette combinaison, 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).

Organisation des connexions en catégories

Les catégories vous permettent de classer les connexions, que vous en ayez créé une ou plusieurs. Ensuite, faites glisser et déposez les connexions dans les catégories correspondantes.

Pour ajouter une catégorie :

1. Dans le tableau de bord 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 seront mises en surbrillance à mesure que vous déplacerez la souris au-dessus d'elles.
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

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

La liste de vos connexions se trouve 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 le tableau de bord de Security Manager, cliquez sur **Gestionnaire de mots de passe**, puis sur l'onglet **Gérer**.

- **Pour ajouter une connexion** : cliquez sur **Ajouter une connexion** et suivez les instructions à l'écran.
- **Pour modifier une connexion** : cliquez sur une connexion, puis sur **Modifier** et changez les données de connexion.
- **Pour supprimer une connexion** : cliquez sur une connexion, puis sur **Supprimer**.

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 du **Gestionnaire de mots de passe** pour afficher son menu contextuel.
3. Cliquez sur **Ajouter une connexion**, puis suivez les instructions à l'écran.

Évaluation de la complexité 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.

Le Gestionnaire de mots de passe 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.

Paramètres de l'icône du Gestionnaire de mots de passe

Le Gestionnaire de mots de passe tente d'identifier les écrans de connexion pour les sites Web et les programmes. Lorsqu'il détecte un écran de connexion pour lequel aucune connexion n'a été créée, le Gestionnaire de mots de passe vous invite à ajouter une connexion pour l'écran en affichant l'icône du Gestionnaire de mots de passe avec un signe +.

Cliquez sur la flèche de 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 enregistré s'affiche.
- **Exclure cet écran** : sélectionnez la case à cocher pour que le Gestionnaire de mots de passe ne vous invite pas à nouveau à ajouter une connexion pour cet écran de connexion.

Pour accéder aux paramètres supplémentaires du Gestionnaire de mots de passe, cliquez sur **Gestionnaire de mots de passe**, puis sur **Paramètres** dans le tableau de bord de Security Manager.

Paramètres

Vous pouvez définir des paramètres permettant de personnaliser HP ProtectTools Security Manager :

1. **Inviter à ajouter des connexions aux écrans de connexion** : l'icône du Gestionnaire de mots de passe s'affiche avec un signe plus 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 à l'ensemble des mots de passe. Pour désactiver cette fonctionnalité, dans la boîte de dialogue **Paramètres de l'icône**, désélectionnez la case à cocher en regard de **Inviter à ajouter des connexions aux écrans de connexion**.
2. **Ouvrir Security Manager avec ctrl-alt-H** : la combinaison de touches d'accès rapide par défaut qui ouvre le menu Liens rapides du Gestionnaire de mots de passe est ctrl+alt+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.

Informations d'authentification

Vous utilisez les informations d'authentification de Security Manager pour confirmer qu'il s'agit bien de vous. L'administrateur local 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 peuvent varier selon les périphériques de sécurité intégrés ou branchés à cet ordinateur. Chaque information d'authentification prise en charge aura une entrée dans le groupe **Mon identité, Informations d'authentification**.

Les informations d'authentification, les conditions et le statut actuel sont répertoriés et peuvent inclure les éléments suivants :

- Empreintes digitales
- Mot de passe
- Smart Card

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

Votre carte d'identité personnelle

Votre carte d'identité 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 et sous forme de gadget dans la barre latérale de Windows.

Pour accéder rapidement à Security Manager, vous pouvez notamment cliquer sur votre carte d'identité dans la barre latérale de Windows.

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

Pour changer le nom affiché :

1. Dans le tableau de bord de Security Manager, cliquez sur **Carte d'identité** dans le coin supérieur gauche.
2. Cliquez sur la zone affichant le nom que vous avez entré pour votre compte Windows. Le système affiche votre nom d'utilisateur Windows pour ce compte.
3. Pour le modifier, saisissez le nouveau nom, puis cliquez sur le bouton **Enregistrer**.

Pour changer la photo affichée :

1. Dans le tableau de bord de Security Manager, cliquez sur **Mon identité**, puis sur **Carte d'identité** dans le coin supérieur gauche.
2. Cliquez sur le bouton **Choisir une image**, sur une image, puis sur le bouton **Enregistrer**.

Définition de vos préférences

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

Général

Les paramètres suivants sont disponibles dans l'onglet Général :

Apparence :**afficher l'icône dans 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, désélectionnez la case à cocher correspondante.

Empreinte

Les paramètres suivants sont disponibles dans l'onglet Empreinte digitale :

Actions rapides : les actions rapides vous permettent de sélectionner la tâche Security Manager à effectuer lorsque vous maintenez enfoncée la touche spécifiée tout en lisant votre empreinte digitale.

Pour attribuer une action rapide à l'une des touches répertoriées :

- Cliquez sur une option **(Touche)+Empreinte digitale**, puis cliquez sur l'une des tâches disponibles dans le menu.

Retour d'empreinte numérique : s'affiche uniquement si un lecteur d'empreintes digitales est disponible. Ce paramètre permet d'ajuster le retour obtenu lors de la lecture de l'empreinte digitale.

- **Activer le retour audio** : Security Manager vous donne un retour audio lorsqu'une empreinte digitale a été lue et il joue différents sons selon les événements de programme. Vous pouvez attribuer de nouveaux sons à ces événements dans l'onglet Sons du Panneau de configuration Windows ou désactiver le retour audio en désactivant cette option.
- **Afficher le retour qualité de la lecture** : par défaut, Security Manager affiche une image de l'empreinte digitale avec un point d'interrogation dès que la qualité de la lecture est insuffisante pour permettre votre authentification. Vous pouvez désactiver l'affichage de cette image en désélectionnant cette option.

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 données sont sauvegardées lorsque vous utilisez cette fonctionnalité.

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. Dans le panneau de gauche, cliquez sur **Avancé**, puis sur **Sauvegarder et restaurer**.
2. Cliquez sur **Sauvegarder les données**.
3. Sélectionnez les modules à inclure dans la sauvegarde. Dans la plupart des cas, vous les sélectionnerez tous.
4. 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.
5. Entrez un mot de passe pour protéger le fichier.
6. Vérifiez votre identité.
7. Cliquez sur **Terminer**.

Pour restaurer les données :

1. Dans le panneau de gauche, cliquez sur **Avancé**, puis sur **Sauvegarder et restaurer**.
2. Cliquez sur **Restaurer les données**.
3. Sélectionnez le fichier de stockage créé. Vous pouvez entrer son chemin d'accès dans le champ fourni ou cliquer sur **Modifier**.

4. Entrez le mot de passe utilisé pour protéger le fichier.
5. Sélectionnez les modules pour lesquels vous souhaitez restaurer les données. Dans la plupart des cas, il s'agit de tous les modules répertoriés.
6. Cliquez sur **Terminer**.

Ajout d'applications

Il est possible que des applications supplémentaires offrant de nouvelles fonctionnalités pour ce programme soient disponibles.

Dans le tableau de bord de Security Manager, cliquez sur **[+] En découvrir plus** pour parcourir les applications supplémentaires.

REMARQUE : Si aucun lien **[+] En découvrir plus** ne s'affiche dans la partie inférieure gauche du tableau de bord, c'est qu'il a été désactivé par l'administrateur de l'ordinateur.

État des applications de sécurité

La page d'état des applications de Security Manager affiche l'état global des applications de sécurité installées. Il indique les applications configurées, ainsi que l'état de configuration de chacune d'entre elles. Le récapitulatif s'affiche automatiquement lorsque vous ouvrez le tableau de bord de Security Manager ou que vous cliquez sur **Applications de sécurité**.

7 Drive Encryption for HP ProtectTools (certains modèles)

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

Le module Drive Encryption for HP ProtectTools fournit une protection complète de vos données en cryptant le disque dur de votre ordinateur. Lorsque Drive Encryption est activé, vous devez vous connecter via l'écran de connexion de Drive Encryption, qui s'affiche avant le démarrage du système d'exploitation Windows®.

L'Assistant d'installation de HP ProtectTools permet aux administrateurs Windows d'activer Drive Encryption, de sauvegarder la clé de cryptage, d'ajouter ou de supprimer des utilisateurs et de désactiver Drive Encryption. Pour plus d'informations, reportez-vous à l'aide du logiciel HP ProtectTools Security Manager.

Les tâches suivantes peuvent être effectuées avec Drive Encryption :

- Gestion du cryptage
  - Cryptage ou décryptage d'unités individuelles

    REMARQUE : Seuls les disques durs internes peuvent être cryptés.
- Restauration
  - Création de clés de sauvegarde
  - Exécution d'une restauration

Procédures de configuration

Ouverture de Drive Encryption

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

Tâches générales

Activation de Drive Encryption

Utilisez l'Assistant d'installation de HP ProtectTools pour activer Drive Encryption.

REMARQUE : Cet Assistant permet également d'ajouter et de supprimer des utilisateurs.

– ou –

1. Cliquez sur **Démarrer**, **Tous les programmes**, **HP**, puis sélectionnez **Console d'administration de HP ProtectTools**.
2. Dans le volet gauche, cliquez sur **Sécurité**, puis sur **Fonctions**.
3. Cochez la case **Drive Encryption**, puis cliquez sur **Suivant**.
4. Sous **Unités à crypter**, cochez la case en regard du disque dur que vous souhaitez crypter.
5. Insérez le périphérique de stockage dans le connecteur approprié.

   REMARQUE : Pour enregistrer la clé de cryptage, vous devez utiliser un périphérique de stockage USB au format FAT32.

6. Sous **Périphérique de stockage externe pour enregistrer la clé de cryptage**, cochez la case en regard du périphérique de stockage dans lequel sera enregistrée la clé de cryptage.
7. Cliquez sur **Appliquer**.

   Le cryptage de l'unité commence.

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

Désactivation de Drive Encryption

Utilisez l'Assistant d'installation de HP ProtectTools pour désactiver Drive Encryption. Pour plus d'informations, reportez-vous à l'aide du logiciel HP ProtectTools Security Manager.

– ou –

1. Cliquez sur **Démarrer**, **Tous les programmes**, **HP**, puis sélectionnez **Console d'administration de HP ProtectTools**.
2. Dans le volet gauche, cliquez sur **Sécurité**, puis sur **Fonctions**.
3. Décochez la case **Drive Encryption**, puis cliquez sur **Appliquer**.

   Le décryptage de l'unité commence.

Connexion après l'activation de Drive Encryption

Si vous allumez l'ordinateur après avoir activé Drive Encryption et enregistré votre compte d'utilisateur, vous devez vous connecter à partir de l'écran de connexion de Drive Encryption :

REMARQUE : Si l'administrateur Windows a activé Pre-boot Security dans HP ProtectTools Security Manager, vous vous connectez à l'ordinateur immédiatement après le démarrage de l'ordinateur et non sur l'écran de connexion de Drive Encryption.

1. Cliquez sur votre nom d'utilisateur, puis saisissez votre mot de passe Windows ou le code PIN de Java™ Card ; vous pouvez également passer votre doigt si votre empreinte est inscrite.
2. Cliquez sur **OK**.

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

Protection des données par cryptage du disque dur

Utilisez l'Assistant d'installation de HP ProtectTools pour protéger vos données en cryptant votre disque dur :

1. Dans Security Manager, cliquez sur **Mise en route**, puis cliquez sur l'icône **Configuration de Security Manager**. Une démonstration présentant les fonctions de Security Manager démarre. (Vous pouvez également démarrer Security Manager à partir de la page « Drive Encryption ».)
2. Dans le volet gauche, cliquez sur **Drive Encryption**, puis sur **Gestion du cryptage**.
3. Cliquez sur **Modifier le cryptage**.
4. Sélectionnez la ou les unités à crypter.

REMARQUE : Il est vivement recommandé de crypter le disque dur.

Affichage de l'état de cryptage

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

REMARQUE : Les modifications de l'état du cryptage doivent être effectuées en utilisant la console d'administration de HP ProtectTools.

1. Ouvrez **HP ProtectTools Security Manager**.
2. Sous **Mes données**, cliquez sur **État du cryptage**.

   Si Drive Encryption est actif, l'état de l'unité affiche l'un des codes d'état suivants :

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

   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.

Tâches avancées

Gestion de Drive Encryption (administrateur uniquement)

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

- Si son état est défini sur Inactif, cela signifie que Drive Encryption n'a pas encore été activé dans HP ProtectTools Security Manager par l'administrateur Windows et ne protège donc pas le disque dur. Utilisez l'Assistant d'installation de HP ProtectTools Security Manager pour activer Drive Encryption.
- Si l'état est Actif, Drive Encryption a été activé et configuré. L'unité est dans l'un des états suivants :
  - Non cryptée
  - Cryptée
  - En cours de cryptage
  - En cours de décryptage

Cryptage ou décryptage des unités individuelles

Pour crypter un ou plusieurs disques durs sur l'ordinateur ou décrypter un disque qui a déjà été crypté, utilisez la fonction Modifier le cryptage :

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

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

Sauvegarde et restauration (tâche de l'administrateur)

La page « Restauration » permet aux administrateurs de sauvegarder et de restaurer des clés de cryptage.

Sauvegarde de clé Drive Encryption locale : vous permet de sauvegarder des clés de cryptage sur un support amovible lorsque Drive Encryption est activé.

Création de clés de sauvegarde

Vous pouvez sauvegarder la clé de cryptage d'une unité cryptée sur un périphérique de stockage amovible :

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

1. Ouvrez **Console d'administration de HP ProtectTools**, cliquez sur **Drive Encryption**, puis sur **Restauration**.
2. Cliquez sur **Sauvegarder les clés**.
3. Sur la page « Sélection du disque de sauvegarde », cochez la case en regard du périphérique sur lequel vous souhaitez stocker la clé de cryptage, puis cliquez sur **Suivant**.
4. Lisez les informations affichées sur la page qui suit, puis cliquez sur **Suivant**. La clé de cryptage est enregistrée sur le périphérique de stockage que vous avez sélectionné.
5. Lorsque la boîte de dialogue de confirmation s'affiche, cliquez sur **Terminer**.

Exécution d'une restauration

Procédez comme suit pour effectuer une restauration si vous avez oublié votre mot de passe :

1. Mettez l'ordinateur sous tension.
2. Insérez le périphérique de stockage amovible contenant la clé de sauvegarde.
3. Lorsque la boîte de dialogue de connexion de Drive Encryption for HP ProtectTools s'affiche, cliquez sur **Annuler**.
4. Cliquez sur **Options** dans le coin inférieur gauche de l'écran puis sur **Restauration**.
5. Sélectionnez le fichier contenant la clé de sauvegarde ou cliquez sur **Parcourir** pour la rechercher, puis cliquez sur **Suivant**.
6. Lorsque la boîte de dialogue de confirmation s'affiche, cliquez sur **OK**.

   Votre ordinateur démarre.

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

8 Privacy Manager pour HP ProtectTools (certains modèles)

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

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

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

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

Privacy Manager requiert la configuration suivante :

- HP ProtectTools Security Manager 5.00 ou version supérieure
- Système d'exploitation Windows® 7, Windows Vista® ou Windows XP
- Microsoft Outlook 2007 ou Microsoft Outlook 2003
- Compte de messagerie électronique valide

REMARQUE : Un certificat Privacy Manager (certificat numérique) doit être demandé et installé depuis le programme Privacy Manager pour que vous puissiez accéder aux fonctions de sécurité. Pour plus d'informations sur la demande d'un certificat Privacy Manager, reportez-vous à la section Demande et installation d'un certificat Privacy Manager à la page 43.

Procédures de configuration

Ouverture de Privacy Manager

Pour ouvrir Privacy Manager :

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

– ou –

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

– ou –

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

– ou –

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

Gestion des certificats Privacy Manager

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

Vous pouvez réaliser les tâches suivantes :

- demander et installer un certificat Privacy Manager ;
- afficher les détails d'un certificat Privacy Manager ;
- renouveler les certificats Privacy Manager ;
- lorsque plusieurs certificats sont disponibles, définir un certificat Privacy Manager par défaut que Privacy Manager doit utiliser ;
- supprimer et révoquer un certificat Privacy Manager (avancé).

Demande et installation d'un certificat Privacy Manager

Avant de pouvoir utiliser les fonctions de Privacy Manager, vous devez demander et installer un certificat Privacy Manager (depuis le programme Privacy Manager) à l'aide d'une adresse électronique valide.

Cette adresse électronique doit être configurée sous la forme d'un compte dans Microsoft Outlook sur le même ordinateur que celui qui demande le certificat Privacy Manager.

Demande d'un certificat Privacy Manager

1. Ouvrez Privacy Manager, puis cliquez sur **Certificats**.
2. Cliquez sur **Demander un certificat Privacy Manager**.
3. Sur la page de bienvenue, lisez le texte, puis cliquez sur **Suivant**.
4. Sur la page du contrat de licence, lisez les termes du contrat.
5. Vérifiez que la case en regard du texte **Cochez cette case pour accepter les termes du contrat de licence** est cochée, puis cliquez sur **Suivant**.
6. Sur la page des détails de votre certificat, saisissez les informations requises, puis cliquez sur **Suivant**.
7. Sur la page d'acceptation de la demande de certificat, cliquez sur **Terminer**.
8. Cliquez sur **OK** pour fermer le certificat.

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

Obtention d'un certificat d'entreprise Privacy Manager préassigné

1. Dans Outlook, ouvrez le courrier électronique que vous avez reçu vous indiquant qu'un certificat d'entreprise vous a été préattribué.
2. Cliquez sur **Obtenir**.
3. Vous recevrez un courrier électronique Microsoft Outlook avec votre certificat Privacy Manager joint.
4. Pour installer le certificat, reportez-vous à la section Installation d'un certificat Privacy Manager à la page 44

Installation d'un certificat Privacy Manager

1. À réception du courrier électronique contenant votre certificat Privacy Manager en pièce jointe, ouvrez le courrier électronique et cliquez sur le bouton **Installer** situé dans le coin inférieur droit du message dans Outlook 2007 ou dans le coin supérieur gauche dans Outlook 2003.
2. Authentifiez-vous à l'aide de la méthode de connexion sécurisée choisie.
3. Sur la page indiquant que le certificat est installé, cliquez sur **Suivant**.
4. Sur la page de sauvegarde du certificat, saisissez un nom et un emplacement pour le fichier de sauvegarde ou cliquez sur **Parcourir** pour rechercher un emplacement.

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

5. Saisissez et confirmez un mot de passe, puis cliquez sur **Suivant**.

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

7. Si vous choisissez de démarrer le processus d'invitation de contact authentifié, suivez les instructions à l'écran en commençant par la deuxième étape de la section Ajout de contacts authentifiés à l'aide des contacts Microsoft Outlook à la page 48.

   – ou –

   Si vous cliquez sur **Annuler**, reportez-vous à la section Ajout d'un contact authentifié à la page 47 pour plus d'informations sur l'ajout ultérieur d'un contact authentifié.

Affichage des détails d'un certificat Privacy Manager

1. Ouvrez Privacy Manager, puis cliquez sur **Certificats**.
2. Cliquez sur un certificat Privacy Manager.
3. Cliquez sur **Détails du certificat**.
4. Lorsque vous avez terminé de visualiser les détails, cliquez sur **OK**.

Renouvellement d'un certificat Privacy Manager

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

1. Ouvrez Privacy Manager, puis cliquez sur **Certificats**.
2. Cliquez sur **Renouveler le certificat**.
3. Suivez les instructions à l'écran pour acheter un nouveau certificat Privacy Manager.

REMARQUE : Le processus de renouvellement d'un certificat Privacy Manager ne remplace pas l'ancien certificat Privacy Manager. Vous devez acheter un nouveau certificat Privacy Manager et l'installer à l'aide des mêmes procédures que dans la section Demande et installation d'un certificat Privacy Manager à la page 43.

Définition d'un certificat Privacy Manager par défaut

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

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

1. Ouvrez Privacy Manager, puis cliquez sur **Certificats**.
2. Cliquez sur le certificat Privacy Manager à utiliser comme certificat par défaut, puis cliquez sur **Définir par défaut**.
3. Cliquez sur **OK**.

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

Suppression d'un certificat Privacy Manager

Si vous supprimez un certificat Privacy Manager, vous ne pouvez ni ouvrir les fichiers ni afficher les données que vous avez cryptés à l'aide de ce certificat. Si vous supprimez accidentellement un certificat Privacy Manager, vous pouvez le restaurer à l'aide du fichier de sauvegarde créé au moment de l'installation du certificat. Pour plus d'informations, reportez-vous à la section Restauration d'un certificat Privacy Manager à la page 46.

Pour supprimer un certificat Privacy Manager :

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

Restauration d'un certificat Privacy Manager

Vous devez créer une copie de sauvegarde du certificat Privacy Manager durant son installation. Vous pouvez également créer une copie de sauvegarde à partir de la page Migration. Cette copie peut servir lors de la migration vers un autre ordinateur ou pour la restauration d'un certificat sur un même ordinateur.

1. Ouvrez Privacy Manager, puis cliquez sur **Migration**.
2. Cliquez sur **Restaurer**.
3. Sur la page du fichier de migration, cliquez sur **Parcourir** pour rechercher le fichier .dppsm créé durant le processus de sauvegarde, puis cliquez sur **Suivant**.
4. Saisissez le mot de passe utilisé lors de la création de la sauvegarde, puis cliquez sur **Suivant**.
5. Cliquez sur **Terminer**.
6. Cliquez sur **OK**.

Pour plus d'informations, reportez-vous à la section Installation d'un certificat Privacy Manager à la page 44 ou Sauvegarde de certificats Privacy Manager et de contacts authentifiés à la page 61.

Révocation de votre certificat Privacy Manager

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

REMARQUE : Un certificat Privacy Manager révoqué n'est pas supprimé. Le certificat peut toujours être utilisé pour afficher les fichiers cryptés.

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

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

6. Suivez les instructions à l'écran.

Gestion des contacts authentifiés

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

Le gestionnaire de contacts authentifiés permet de réaliser les tâches suivantes :

- afficher les détails d'un contact authentifié ;
- supprimer des contacts authentifiés ;
- vérifier l'état de révocation des contacts authentifiés (avancé).

Ajout de contacts authentifiés

L'ajout de contacts authentifiés est un processus en trois étapes :

1. Vous envoyez une invitation par courrier électronique à un destinataire de contact authentifié.
2. Le destinataire de contact authentifié répond au courrier électronique.
3. Vous recevez la réponse par courrier électronique du destinataire de contact authentifié et vous cliquez sur **Accepter**.

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

Reportez-vous aux sections suivantes pour savoir comment ajouter des contacts authentifiés.

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

Ajout d'un contact authentifié

1. Ouvrez Privacy Manager, cliquez sur **Gestionnaire de contacts authentifiés**, puis sur **Inviter des contacts**.

   – ou –

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

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

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

   Un courrier électronique est automatiquement généré.

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

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

6. Cliquez sur **Envoyer**.

REMARQUE : Si vous n'avez pas obtenu de certificat Privacy Manager, un message vous informe que vous devez disposer d'un certificat Privacy Manager pour envoyer une demande de contact authentifié. Cliquez sur **OK** pour lancer l'Assistant Demande de certificat. Pour plus d'informations, reportez-vous à la section Demande et installation d'un certificat Privacy Manager à la page 43.

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

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

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

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

9. Cliquez sur **OK**.

Ajout de contacts authentifiés à l'aide des contacts Microsoft Outlook

1. Ouvrez Privacy Manager, cliquez sur **Gestionnaire de contacts authentifiés**, puis sur **Inviter des contacts**.

   – ou –

   Dans la barre d'outils de Microsoft Outlook, cliquez sur la flèche vers le bas située en regard de **Envoyer en toute sécurité**, puis cliquez sur **Inviter mes contacts Outlook**.

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

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

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

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

5. Cliquez sur **Envoyer**.

REMARQUE : Si vous n'avez pas obtenu de certificat Privacy Manager, un message vous informe que vous devez disposer d'un certificat Privacy Manager pour envoyer une demande de contact authentifié. Cliquez sur **OK** pour lancer l'Assistant Demande de certificat. Pour plus d'informations, reportez-vous à la section Demande et installation d'un certificat Privacy Manager à la page 43.

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

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

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

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

8. Cliquez sur **OK**.

Affichage des détails d'un contact authentifié

1. Ouvrez Privacy Manager, puis cliquez sur **Contacts authentifiés**.
2. Cliquez sur un contact authentifié.
3. Cliquez sur **Détails du contact**.
4. Lorsque vous avez terminé de visualiser les détails, cliquez sur **OK**.

Suppression d'un contact authentifié

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

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

Pour savoir si un contact authentifié a révoqué son certificat Privacy Manager :

1. Ouvrez Privacy Manager, puis cliquez sur **Contacts authentifiés**.
2. Cliquez sur un contact authentifié.
3. Cliquez sur le bouton **Avancé**.

   La boîte de dialogue de gestion avancée des contacts authentifiés s'affiche.

4. Cliquez sur **Vérifier la révocation**.
5. Cliquez sur **Fermer**.

Tâches générales

Vous pouvez utiliser Privacy Manager avec les produits Microsoft suivants :

- Microsoft Outlook
- Microsoft Office
- Windows Live Messenger

Utilisation de Privacy Manager dans Microsoft Outlook

Lorsque Privacy Manager est installé, un bouton Confidentialité apparaît dans la barre d'outils de Microsoft Outlook et un bouton Envoyer en toute sécurité apparaît dans la barre d'outils de chaque message électronique Microsoft Outlook. Lorsque vous cliquez sur la flèche vers le bas située en regard de **Confidentialité** ou de **Envoyer en toute sécurité**, vous pouvez choisir l'une des options suivantes :

- Signer et envoyer (bouton Envoyer en toute sécurité uniquement) : Cette option ajoute une signature numérique au courrier électronique et l'envoie après votre authentification, selon la méthode de connexion sécurisée choisie.
- Sceller pour les contacts authentifiés et envoyer (bouton Envoyer en toute sécurité uniquement) : Cette option ajoute une signature numérique, crypte le courrier électronique et l'envoie après votre authentification, selon la méthode de connexion sécurisée choisie.
- Inviter des contacts : Cette option permet d'envoyer une invitation de contact authentifié. Pour plus d'informations, reportez-vous à la section Ajout d'un contact authentifié à la page 47.
- Inviter mes contacts Outlook : Cette option permet d'envoyer une invitation de contact authentifié à tous les contacts de votre carnet d'adresses Microsoft Outlook. Pour plus d'informations, reportez-vous à la section Ajout de contacts authentifiés à l'aide des contacts Microsoft Outlook à la page 48.
- Open the Privacy Manager software (Ouvrir le logiciel Privacy Manager) : Les options Certificats, Contacts authentifiés et Paramètres permettent d'ouvrir le logiciel Privacy Manager pour ajouter, afficher ou modifier les paramètres actuels. Pour plus d'informations, reportez-vous à la section Configuration de Privacy Manager pour Microsoft Outlook à la page 50.

Configuration de Privacy Manager pour Microsoft Outlook

1. Ouvrez Privacy Manager, cliquez sur **Paramètres**, puis sélectionnez l'onglet **Adresse électronique**.

   – ou –

   Dans la barre d'outils principale de Microsoft Outlook, cliquez sur la flèche vers le bas située en regard de **Envoyer en toute sécurité** (**Confidentialité** dans Outlook 2003), puis sélectionnez **Paramètres**.

   – ou –

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

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

Signature et envoi d'un message électronique

1. Dans Microsoft Outlook, cliquez sur **Nouveau** ou sur **Répondre**.
2. Saisissez votre message électronique.
3. Cliquez sur la flèche vers le bas située en regard de **Envoyer en toute sécurité** (**Confidentialité** dans Outlook 2003), puis sélectionnez **Signer et envoyer**.
4. Authentifiez-vous à l'aide de la méthode de connexion sécurisée choisie.

Scellage et envoi d'un message électronique

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

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

1. Dans Microsoft Outlook, cliquez sur **Nouveau** ou sur **Répondre**.
2. Saisissez votre message électronique.
3. Cliquez sur la flèche vers le bas située en regard de **Envoyer en toute sécurité** (**Confidentialité** dans Outlook 2003), puis sélectionnez **Sceller pour les contacts authentifiés et envoyer**.
4. Authentifiez-vous à l'aide de la méthode de connexion sécurisée choisie.

Affichage d'un message électronique scellé

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

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

Utilisation de Privacy Manager dans un document Microsoft Office 2007

REMARQUE : Privacy Manager peut uniquement être utilisé avec les documents Microsoft Office 2007.

Après l'installation de votre certificat Privacy Manager, un bouton Signer et crypter apparaît sur le côté droit de la barre d'outils de tous les documents Microsoft Word, Microsoft Excel et Microsoft PowerPoint. Lorsque vous cliquez sur la flèche vers le bas située en regard de **Signer et crypter**, vous pouvez choisir l'une des options suivantes :

- Signer le document : Cette option ajoute votre signature numérique au document.
- Ajouter une ligne de signature avant de signer (Microsoft Word et Microsoft Excel uniquement) : Par défaut, une ligne de signature est ajoutée lorsqu'un document Microsoft Word ou Microsoft Excel est signé ou crypté. Pour désactiver cette option, cliquez sur **Ajouter une ligne de signature avant de signer** pour décocher la case.
- Crypter le document : Cette option ajoute votre signature numérique et crypte le document.

- Supprimer le cryptage : Cette option supprime le cryptage du document.
- Open the Privacy Manager software (Ouvrir le logiciel Privacy Manager) : Les options Certificats, Contacts authentifiés et Paramètres permettent d'ouvrir le logiciel Privacy Manager pour ajouter, afficher ou modifier les paramètres actuels. Pour plus d'informations, reportez-vous à la section Gestion des certificats Privacy Manager à la page 43, Gestion des contacts authentifiés à la page 47 ou Configuration de Privacy Manager pour Microsoft Office à la page 52.

Configuration de Privacy Manager pour Microsoft Office

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

   – ou –

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

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

Signature d'un document Microsoft Office

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

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

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

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

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

1. Dans Microsoft Word ou Microsoft Excel, créez et enregistrez un document.
2. Cliquez sur le menu **Accueil**.
3. Cliquez sur la flèche vers le bas située en regard de **Signer et crypter**, puis sélectionnez **Ajouter une ligne de signature avant de signer**.

REMARQUE : Une coche apparaît en regard de l'option Ajouter une ligne de signature avant de signer lorsque cette option est sélectionnée. Par défaut, cette option est activée.

4. Cliquez sur la flèche vers le bas située en regard de **Signer et crypter**, puis sélectionnez **Signer le document**.

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

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

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

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

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

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

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

   La boîte de dialogue Configuration de signature s'affiche.

4. Dans la zone sous **Signataire suggéré**, saisissez le nom du signataire suggéré.

5. Dans la zone sous **Instructions destinées au signataire**, saisissez un message pour ce signataire suggéré.

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

6. Cochez la case **Afficher la date dans la ligne de signature** pour afficher la date.

7. Cochez la case **Afficher le titre du signataire dans la ligne de signature** pour afficher le titre.

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

8. Cliquez sur **OK**.

Ajout d'une ligne de signature de signataire suggéré

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

Pour signer le document :

1. Double-cliquez sur la ligne de signature appropriée.

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

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

Cryptage d'un document Microsoft Office

Vous pouvez crypter un document Microsoft Office pour vous-même et vos contacts authentifiés. Lorsque vous cryptez un document et le fermez, vous-même et les contacts authentifiés sélectionnés dans la liste devez vous authentifier avant l'ouverture.

Pour crypter un document Microsoft Office :

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

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

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

5. Cliquez sur **OK**.

Si vous décidez par la suite de modifier le document, suivez les étapes présentées à la section Suppression du cryptage d'un document Microsoft Office à la page 54. Lorsque le cryptage est supprimé, vous pouvez modifier le document. Suivez les étapes de cette section pour crypter à nouveau le document.

Suppression du cryptage d'un document Microsoft Office

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

Pour supprimer le cryptage d'un document Microsoft Office :

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

Envoi d'un document Microsoft Office crypté

Vous pouvez joindre un document Microsoft Office crypté à un message électronique sans avoir à signer ni à crypter le message en lui-même. Pour cela, créez et envoyez un courrier électronique contenant un document signé et crypté exactement de la même façon que pour un courrier électronique classique contenant une pièce jointe.

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

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

1. Dans Microsoft Outlook, cliquez sur **Nouveau** ou sur **Répondre**.
2. Saisissez votre message électronique.
3. Joignez le document Microsoft Office.
4. Pour obtenir plus d'instructions, reportez-vous à la section Scellage et envoi d'un message électronique à la page 51.

Affichage d'un document Microsoft Office signé

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

Lorsqu'un document Microsoft Office signé est ouvert, une icône de signature numérique apparaît dans la barre d'état située en bas de la fenêtre du document.

1. Cliquez sur cette icône pour afficher la boîte de dialogue Signatures, qui répertorie le nom de tous les utilisateurs qui ont signé le document et la date de leur signature.
2. Pour obtenir des détails supplémentaires sur chaque signature, cliquez avec le bouton droit sur un nom de la boîte de dialogue Signatures et sélectionnez Signature Details (Détails de la signature).

Affichage d'un document Microsoft Office crypté

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

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

Utilisation de Privacy Manager dans Windows Live Messenger

Privacy Manager ajoute les fonctions de communication sécurisée suivantes à Windows Live Messenger :

- **Secure chat** (Chat sécurisé) : Les messages sont transmis à l'aide du protocole SSL/TLS (Secure Sockets Layer/Transport Layer Security) sur XML, la même technologie que celle utilisée pour garantir la sécurité des opérations commerciales en ligne.
- **Recipient identification** (Identification du destinataire) : Vous pouvez vérifier la présence et l'identité d'une personne avant d'envoyer un message.
- **Signed messages** (Messages signés) : Vous pouvez signer électroniquement vos messages. Ensuite, si le message est falsifié, il est marqué comme non valide lorsque le destinataire le reçoit.
- **Fonction Hide/show** (Masquer/afficher) : Vous pouvez masquer certains ou tous les messages d'une fenêtre Privacy Manager Chat. Vous pouvez également envoyer un message dans lequel le contenu est masqué. L'authentification est requise avant l'affichage du message.

- **Secure chat history** (Historique de chat sécurisé) : Les journaux de vos sessions de chat sont cryptés avant d'être enregistrés et requièrent une authentification pour être affichés.
- **Automatic locking/unlocking** (Verrouillage/déverrouillage automatique) : Vous pouvez verrouiller et déverrouiller la fenêtre Privacy Manager Chat ou la configurer de façon à ce qu'elle soit automatiquement verrouillée après une certaine période d'inactivité.

Démarrage d'une session de Privacy Manager Chat

REMARQUE : Pour utiliser Privacy Manager Chat, les deux parties doivent installer Privacy Manager et posséder un certificat Privacy Manager. Pour plus d'informations sur l'installation d'un certificat Privacy Manager, reportez-vous à la section Demande et installation d'un certificat Privacy Manager à la page 43.

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

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

   b. Cliquez sur **Envoyer un message instantané**.

   – ou –

   a. Double-cliquez sur un contact en ligne dans Live Messenger, puis cliquez sur le menu **Voir la liste des activités**.

   b. Cliquez sur **Actions**, puis sélectionnez **Envoyer un message instantané**.

   – ou –

   a. Cliquez avec le bouton droit sur l'icône ProtectTools dans la zone de notification, sélectionnez **Privacy Manager pour HP ProtectTools**, puis cliquez sur **Envoyer un message instantané**.

   b. Dans Live Messenger, cliquez sur **Actions : Démarrer une activité**, puis sélectionnez **Privacy Manager Chat**.

   REMARQUE : Chaque utilisateur doit être en ligne dans Live Messenger et figurer dans la fenêtre des utilisateurs en ligne de Live Messenger. Cliquez pour sélectionner un utilisateur en ligne.

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

2. Cliquez sur **Démarrer** pour commencer une session de chat sécurisé.

Configuration de Privacy Manager pour Windows Live Messenger

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

   – ou –

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

   – ou –

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

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

3. Pour préciser un dossier d'historique pour vos sessions de chat, cliquez sur **Parcourir** pour rechercher un dossier, puis sélectionnez **OK**.

4. Pour crypter et enregistrer automatiquement vos sessions lorsque vous les fermez, cochez la case **Enregistrer automatiquement l'historique de chat sécurisé**.

5. Cliquez sur **OK**.

Chat dans la fenêtre Privacy Manager Chat

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

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

Affichage de l'historique de chat

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

La visionneuse permet de réaliser les tâches suivantes :

- Révélation de toutes les sessions à la page 58
- Révélation des sessions d'un compte spécifique à la page 58
- Affichage d'un ID de session à la page 59
- Affichage d'une session à la page 59
- Recherche de texte spécifique dans des sessions à la page 59
- Suppression d'une session à la page 59
- Ajout ou suppression de colonnes à la page 60
- Sessions affichées par filtre à la page 60

Pour démarrer la visionneuse d'historique Live Messenger :

▲ Dans la zone de notification, à l'extrémité droite de la barre des tâches, cliquez avec le bouton droit sur l'icône **HP ProtectTools**, sélectionnez **Privacy Manager : pour HP ProtectTools**, puis cliquez sur **Visionneuse d'historique Live Messenger**.

– ou –

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

Révélation de toutes les sessions

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

Pour révéler toutes les sessions d'historique de chat enregistrées :

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

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

Révélation des sessions d'un compte spécifique

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

Pour révéler une session d'historique de chat spécifique :

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

   Le nom d'écran du contact est décrypté.
3. Double-cliquez sur la session révélée pour afficher son contenu.

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

Affichage d'un ID de session

Pour afficher un ID de session :

- Dans l'affichage de l'historique Live Messenger, cliquez avec le bouton droit sur une session révélée de votre choix, puis sélectionnez **Afficher l'ID de session**.

Affichage d'une session

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

Pour afficher une session d'historique Live Messenger :

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

   Le contenu de la session est décrypté.

Recherche de texte spécifique dans des sessions

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

Pour rechercher du texte dans des sessions d'historique de chat :

1. Dans la visionneuse d'historique Live Messenger, cliquez sur le bouton **Recherche**.
2. Saisissez le texte de la recherche, configurez les paramètres de recherche souhaités, puis cliquez sur **OK**.

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

Suppression d'une session

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

Ajout ou suppression de colonnes

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

Pour ajouter des colonnes à l'affichage :

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

Pour supprimer des colonnes de l'affichage :

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

Sessions affichées par filtre

Une liste des sessions de tous vos comptes est affichée dans la visionneuse d'historique Live Messenger. Vous pouvez également filtrer les sessions affichées en fonction des éléments suivants :

- Comptes spécifiques. Pour plus de détails, reportez-vous à la section Affichage des sessions d'un compte spécifique à la page 60.
- Plage de dates. Pour plus de détails, reportez-vous à la section Affichage des sessions pour une plage de dates à la page 60.
- Différents dossiers. Pour plus de détails, reportez-vous à la section Affichage des sessions enregistrées dans un dossier autre que le dossier par défaut à la page 60.

Affichage des sessions d'un compte spécifique

▲ Dans la visionneuse d'historique Live Messenger, sélectionnez un compte dans le menu **Afficher l'historique de**.

Affichage des sessions pour une plage de dates

1. Dans la visionneuse d'historique Live Messenger, cliquez sur l'icône **Filtre avancé**.

   La boîte de dialogue Filtre avancé s'affiche.

2. Cochez la case **Afficher uniquement les sessions de la plage de dates spécifiée**.
3. Dans les cases **De** et **À**, saisissez le jour, le mois et/ou l'année ou cliquez sur la flèche située en regard du calendrier pour sélectionner les dates.
4. Cliquez sur **OK**.

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

1. Dans la visionneuse d'historique Live Messenger, cliquez sur l'icône **Filtre avancé**.
2. Cochez la case **Utiliser un autre dossier de fichiers d'historique**.

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

Tâches avancées

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

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

Sauvegarde de certificats Privacy Manager et de contacts authentifiés

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

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

REMARQUE : Conservez ce mot de passe dans un endroit sûr car il sera nécessaire pour restaurer le fichier de migration.

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

Restauration de certificats Privacy Manager et de contacts authentifiés

Pour restaurer vos certificats Privacy Manager et contacts authentifiés sur un autre ordinateur dans le cadre du processus de migration ou sur le même ordinateur, procédez comme suit :

1. Ouvrez Privacy Manager, puis cliquez sur **Migration**.
2. Cliquez sur **Restaurer**.
3. Sur la page du fichier de migration, cliquez sur **Parcourir** pour rechercher le fichier, puis cliquez sur **Suivant**.
4. Saisissez le mot de passe utilisé lors de la création du fichier de sauvegarde, puis cliquez sur **Suivant**.
5. Sur la page du fichier de migration, cliquez sur **Terminer**.

Administration centrale de Privacy Manager

Il est possible que votre installation de Privacy Manager fasse partie d'une installation centralisée personnalisée par votre administrateur. Une ou plusieurs des fonctions suivantes peuvent être activées ou désactivées :

- **Politique d'utilisation du certificat** : il est possible que vous puissiez utiliser uniquement les certificats Privacy Manager émis par Comodo ou que vous puissiez utiliser les certificats numériques émis par d'autres autorités de certification.
- **Politique de cryptage** : les possibilités de cryptage peuvent être activées ou désactivées individuellement dans Microsoft Office ou Outlook, ainsi que dans Windows Live Messenger.

9 File Sanitizer pour HP ProtectTools

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

REMARQUE : Cette version de File Sanitizer ne prend en charge que le disque dur système.

Destruction

La destruction diffère d'une suppression standard sous Windows® (également dénommée destruction simple dans File Sanitizer), dans le sens où lorsque vous détruisez une ressource à l'aide de File Sanitizer, un algorithme qui masque les données est invoqué, de manière à rendre virtuellement impossible la récupération de la ressource d'origine. Une suppression simple Windows peut laisser le fichier (ou la ressource) intact(e) sur le disque dur ou dans un état permettant une récupération du fichier (ou de la ressource) à l'aide de méthodes de criminalistique informatique.

Lorsque vous choisissez un profil de destruction (Haute sécurité, Sécurité moyenne ou Sécurité basse), une liste prédéfinie de ressources et une méthode d'effacement sont automatiquement sélectionnées pour la destruction. Vous pouvez également personnaliser un profil de destruction, qui vous permet de définir le nombre de cycles de destruction, les ressources à inclure pour la destruction, les ressources à confirmer avant la destruction et les ressources à exclure de la destruction. Pour plus d'informations, reportez-vous à la section Sélection ou création d'un profil de destruction à la page 67.

Vous pouvez configurer une programmation de destruction automatique et détruire manuellement des ressources dès que vous le souhaitez. Pour plus d'informations, reportez-vous à la section Configuration d'une planification de destruction à la page 66, Destruction manuelle d'une ressource à la page 71 ou Destruction manuelle de tous les éléments sélectionnés à la page 72.

REMARQUE : Un fichier .dll n'est détruit et supprimé du système que s'il a été déplacé vers la corbeille.

Nettoyage de l'espace libre

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

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

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

Vous pouvez configurer une programmation de nettoyage automatique de l'espace libre ou activer manuellement le nettoyage de l'espace libre à l'aide de l'icône **HP ProtectTools** dans la zone de notification, à l'extrémité droite de la barre des tâches. Pour plus d'informations, reportez-vous à la section Configuration d'une planification de nettoyage de l'espace libre à la page 67 ou Activation manuelle du nettoyage de l'espace libre à la page 72.

Procédures de configuration

Ouverture de File Sanitizer

Pour ouvrir File Sanitizer :

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

– ou –

- Double-cliquez sur l'icône **File Sanitizer** située sur votre bureau.

– ou –

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

Configuration d'une planification de destruction

REMARQUE : Pour plus d'informations sur la sélection d'un profil de destruction prédéfini ou la création d'un profil de destruction, consultez la section Sélection ou création d'un profil de destruction à la page 67.

REMARQUE : Pour plus d'informations sur la destruction manuelle de ressources, reportez-vous à la section Destruction manuelle d'une ressource à la page 71.

1. Ouvrez File Sanitizer, puis cliquez sur **Détruire**.
2. Sélectionnez une option de destruction :
   - **Arrêt de Windows** : cette option permet de détruire toutes les ressources sélectionnées à l'arrêt de Windows.

     REMARQUE : Lorsque cette option est sélectionnée, une boîte de dialogue est affichée à l'arrêt. Elle vous demande si vous souhaitez poursuivre la destruction des ressources sélectionnées ou ignorer la procédure. Cliquez sur **Oui** pour ignorer la procédure de destruction ou sur **Non** afin de poursuivre la destruction.
   - **Ouverture de navigateur Web** : cette option permet de détruire toutes les ressources Web sélectionnées, telles que l'historique des adresses URL, lorsque vous ouvrez un navigateur Web.
   - **Fermeture de navigateur Web** : cette option permet de détruire toutes les ressources Web sélectionnées, telles que l'historique des adresses URL, lorsque vous fermez un navigateur Web.
   - **Séquence de touches** : cette option permet de démarrer la procédure de destruction à l'aide d'une séquence de touches.
   - **Planificateur** : cochez la case **Activer le planificateur**, entrez votre mot de passe Windows, puis un jour et une heure de destruction des ressources sélectionnées.

REMARQUE : Un fichier .dll n'est détruit et supprimé du système que s'il a été déplacé vers la corbeille.

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

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

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

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

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

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

Sélection ou création d'un profil de destruction

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

Sélection d'un profil de destruction prédéfini

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

Pour sélectionner un profil de destruction prédéfini :

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

Personnalisation d'un profil de destruction

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

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

REMARQUE : Le nombre de cycles de destruction sélectionné sera effectué pour chaque ressource. Par exemple, si vous choisissez 3 cycles de destruction, un algorithme qui masque les données est exécuté 3 fois. Si vous choisissez les cycles de destruction à sécurité renforcée, l'opération peut être beaucoup plus longue. Néanmoins, plus le nombre de cycles définis est élevé, moins les données sont susceptibles d'être récupérées.

3. Sélectionnez les ressources à détruire :
   a. Sous **Options de destruction disponibles**, cliquez sur une ressource, puis sur **Ajouter**.
   b. Pour ajouter une ressource personnalisée, cliquez sur **Ajouter une option personnalisée**, puis naviguez ou saisissez le chemin d'accès au nom du fichier ou dossier. Cliquez sur **Ouvrir**, puis sur **OK**. Sous **Options de destruction disponibles**, cliquez sur la ressource personnalisée, puis sur **Ajouter**.

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

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

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

5. Pour protéger les fichiers ou dossiers d'une destruction automatique, sous **Ne pas détruire les éléments suivants**, cliquez sur **Ajouter**, puis naviguez ou saisissez le chemin d'accès au fichier ou dossier. Cliquez sur **Ouvrir**, puis sur **OK**.

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

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

Personnalisation d'un profil de suppression simple

Le profil de destruction simple permet une suppression de ressource standard sans destruction. Lorsque vous personnalisez un profil de suppression simple, vous pouvez définir les ressources à inclure pour une suppression simple, les ressources à confirmer avant d'exécuter une suppression simple et les ressources à exclure d'une suppression simple.

REMARQUE : Si vous utilisez l'option de suppression simple, un nettoyage de l'espace libre peut parfois être exécuté sur les ressources qui ont été supprimées manuellement en utilisant la corbeille de Windows.

Pour personnaliser un profil de destruction simple :

1. Ouvrez File Sanitizer, cliquez sur **Paramètres**, cliquez sur **Paramètre de suppression simple**, puis sur **Détails**.
2. Sélectionnez les ressources à supprimer :
   a. Sous **Options de suppression disponibles**, cliquez sur une ressource, puis sur **Ajouter**.
   b. Pour ajouter une ressource personnalisée, cliquez sur **Ajouter une option personnalisée**, saisissez un nom de fichier ou de dossier, puis cliquez sur **OK**. Cliquez sur la ressource personnalisée, puis sur **Ajouter**.

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

3. Sous **Supprimer les éléments suivants**, cochez la case en regard de chaque ressource pour laquelle vous souhaitez demander confirmation avant la suppression.

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

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

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

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

Tâches générales

Vous pouvez utiliser File Sanitizer pour réaliser les tâches suivantes :

- Utiliser une séquence de touches pour démarrer la destruction : Cette fonction permet de créer une séquence de touches (par exemple, ctrl+alt+s) pour démarrer la destruction. Pour plus de détails, reportez-vous à la section Utilisation d'une séquence de touches pour démarrer la destruction à la page 70.
- Utiliser l'icône File Sanitizer pour démarrer la destruction : Cette fonction est similaire à la fonction de glisser-déplacer de Windows. Pour plus de détails, reportez-vous à la section Utilisation de l'icône File Sanitizer à la page 71.
- Détruire manuellement une ressource spécifique ou toutes les ressources sélectionnées : Cette fonction permet de détruire manuellement des éléments sans attendre que la destruction planifiée soit invoquée. Pour plus de détails, reportez-vous à la section Destruction manuelle d'une ressource à la page 71 ou Destruction manuelle de tous les éléments sélectionnés à la page 72.
- Activer manuellement le nettoyage de l'espace libre : Cette fonction permet d'activer manuellement le nettoyage de l'espace libre. Pour plus de détails, reportez-vous à la section Activation manuelle du nettoyage de l'espace libre à la page 72.
- Annuler une opération de destruction ou de nettoyage de l'espace libre : Cette fonction permet d'arrêter une opération de destruction ou de nettoyage de l'espace libre. Pour plus de détails, reportez-vous à la section Annulation d'une opération de destruction ou de nettoyage de l'espace libre à la page 72.
- Afficher les fichiers journaux : Cette fonction permet d'afficher les fichiers journaux de destruction et de nettoyage de l'espace libre contenant des erreurs ou des échecs ayant eu lieu lors de la dernière opération de destruction ou de nettoyage de l'espace libre. Pour plus de détails, reportez-vous à la section Affichage des fichiers journaux à la page 72.

REMARQUE : L'opération de destruction ou de nettoyage de l'espace libre peut durer un certain temps. Bien que la destruction et le nettoyage de l'espace libre soient exécutés en arrière-plan, votre ordinateur peut être plus lent en raison de l'utilisation plus importante du processeur.

Utilisation d'une séquence de touches pour démarrer la destruction

Pour spécifier une séquence de touches, procédez comme suit :

1. Ouvrez File Sanitizer, puis cliquez sur **Détruire**.
2. Cochez la case **Séquence de touches**.
3. Saisissez un caractère dans la case disponible.
4. Cochez la case **CTRL** ou **ALT**, puis la case **MAJ**.

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

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

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

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

Utilisation de l'icône File Sanitizer

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

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

Destruction manuelle d'une ressource

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

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

   REMARQUE : La ressource que vous sélectionnez peut être un fichier ou un dossier.

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

– ou –

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

– ou –

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

Destruction manuelle de tous les éléments sélectionnés

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

– ou –

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

– ou –

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

Activation manuelle du nettoyage de l'espace libre

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

– ou –

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

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

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

Pour annuler l'opération :

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

Affichage des fichiers journaux

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

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

Un fichier journal est créé pour les opérations de destruction et un autre, pour les opérations de nettoyage d'espace libre. Les deux fichiers journal se trouvent sur le disque, à l'adresse :

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

10 Device Access Manager pour HP ProtectTools (certains modèles)

Les administrateurs du système d'exploitation Windows® ont recours à Device Access Manager pour HP ProtectTools afin de contrôler l'accès aux périphériques d'un système et de le protéger contre tout accès non autorisé :

- Des profils de périphériques sont créés pour chaque utilisateur dans le but de définir les périphériques auxquels ils sont autorisés ou non à accéder.
- Les utilisateurs sont également organisés en groupes, tel que le groupe Administrateurs de périphériques prédéfini, ou des groupes peuvent être définis à partir de l'option Gestion de l'ordinateur de la section Outils d'administration du Panneau de configuration.
- L'accès aux périphériques peut être octroyé ou refusé sur la base de l'appartenance à un groupe.
- Pour les classes de périphériques telles que les lecteurs de CD-ROM et de DVD, l'accès en lecture et en écriture peut être autorisé ou refusé séparément.

Les utilisateurs limités peuvent également être autorisés à lire et à modifier la règle de contrôle d'accès aux périphériques.

Procédures de configuration

Ouverture de Device Access Manager

Pour ouvrir Device Access Manager, procédez comme suit :

1. Cliquez sur **Démarrer**, **Tous les programmes**, **HP**, puis sélectionnez **Console d'administration de HP ProtectTools**.
2. Dans le volet gauche, cliquez sur **Device Access Manager**.

Configuration de l'accès aux périphériques

Device Access Manager pour HP ProtectTools offre trois vues :

- La vue Configuration simple permet d'octroyer ou de refuser l'accès à des classes de périphériques pour des membres du groupe Administrateurs de périphériques.
- La vue Configuration de classe de périphérique permet d'octroyer ou de refuser l'accès à des types de périphériques ou des périphériques spécifiques pour des utilisateurs ou des groupes spécifiques.
- La vue Paramètres d'accès utilisateur permet de spécifier les utilisateurs autorisés à afficher ou modifier les informations des vues Configuration simple et Configuration de classe de périphérique.

Groupe Administrateurs de périphériques

Lors de l'installation de Device Access Manager, un groupe Administrateurs de périphériques est créé.

L'administrateur système peut mettre en place une simple stratégie de contrôle d'accès aux périphériques en refusant l'accès à un ensemble de classes de périphériques si l'utilisateur n'est pas authentifié. Pour distinguer les utilisateurs de périphériques authentifiés de ceux qui ne sont pas authentifiés, il est recommandé d'ajouter tous les utilisateurs de périphériques authentifiés au groupe Administrateurs de périphériques. Octroyez ensuite aux membres de ce groupe l'accès aux périphériques dans les vues Configuration simple ou Configuration de classe de périphérique pour assurer aux utilisateurs de périphériques authentifiés un accès complet à l'ensemble spécifié de classes de périphériques.

REMARQUE : Lorsque vous ajoutez un utilisateur au groupe Administrateurs de périphériques, celui-ci n'est pas automatiquement autorisé à accéder aux périphériques. Cependant, vous pouvez utiliser la vue Configuration simple pour octroyer l'accès à l'ensemble de classes de périphériques aux utilisateurs authentifiés.

Pour ajouter des utilisateurs au groupe Administrateurs de périphériques, procédez comme suit :

- Pour Windows 7, Vista ou XP Professionnel, utilisez le composant MMC « Utilisateurs et groupes locaux ».
- Pour Windows 7, Vista® ou XP Édition familiale, depuis un compte privilégié, tapez ce qui suit dans la fenêtre d'invite de commande :

```
c:\> net localgroup "Administrateurs de périphériques" username /ADD
```

Configuration simple

Les administrateurs et utilisateurs autorisés peuvent utiliser la vue Configuration simple pour modifier l'accès aux classes de périphériques suivantes pour tous les utilisateurs n'appartenant pas au groupe Administrateurs de périphériques :

REMARQUE : Pour pouvoir utiliser cette vue et lire les informations sur l'accès aux périphériques, l'utilisateur ou groupe doit bénéficier des droits en lecture dans la vue **Paramètres d'accès utilisateur**. Pour pouvoir utiliser cette vue et modifier les informations sur l'accès aux périphériques, l'utilisateur ou groupe doit bénéficier des droits en modification dans la vue **Paramètres d'accès utilisateur**.

- Tous les supports amovibles (disquettes, unités flash USB, etc.)
- Tous les lecteurs de DVD/CD-ROM
- Tous les ports série et parallèles
- Tous les périphériques Bluetooth®
- Tous les périphériques à infrarouge
- Tous les modems
- Tous les périphériques PCMCIA
- Tous les périphériques 1394

Pour octroyer ou refuser l'accès à une classe de périphérique à tous les utilisateurs n'appartenant pas au groupe Administrateurs de périphériques, procédez comme suit :

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

   Si une case est grisée, les valeurs ayant trait à l'accès ont été modifiées dans la vue Configuration de classe de périphérique. Pour restaurer les paramètres simples, cliquez sur la case à cocher et sélectionnez **Oui** pour confirmer.
3. Cliquez sur l'icône **Enregistrer**.

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

Démarrage du service en arrière-plan

Avant de pouvoir appliquer des profils de périphérique, HP ProtectTools Security Manager ouvre une boîte de dialogue pour vous demander si vous souhaitez démarrer le service en arrière-plan de verrouillage des périphériques/audition HP ProtectTools. Cliquez sur **Oui**. Le service en arrière-plan démarre et, par la suite, est automatiquement exécuté au démarrage du système.

REMARQUE : Un profil de périphérique doit être défini avant l'affichage de l'invite du service en arrière-plan.

Les administrateurs peuvent également démarrer ou arrêter ce service :

1. Cliquez sur **Démarrer**, puis sélectionnez **Panneau de configuration**.
2. Cliquez sur **Outils d'administration** et sélectionnez **Services**.
3. Recherchez le service **Verrouillage des périphériques/Audition HP ProtectTools**.

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

- Service Verrouillage des périphériques/Audition
- Pilote DAMDrv.sys

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

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

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

Configuration de classe de périphérique

Les administrateurs et les utilisateurs autorisés peuvent afficher et modifier les listes d'utilisateurs et groupes autorisés ou non-autorisés à accéder à des classes de périphériques ou à des périphériques spécifiques.

REMARQUE : Pour pouvoir utiliser cette vue et lire les informations sur l'accès aux périphériques, l'utilisateur ou groupe doit bénéficier des droits en lecture dans la vue **Paramètres d'accès utilisateur**. Pour pouvoir utiliser cette vue et modifier les informations sur l'accès aux périphériques, l'utilisateur ou groupe doit bénéficier des droits en modification dans la vue **Paramètres d'accès utilisateur**.

La vue Configuration de classe de périphérique possède les sections suivantes :

- **Liste des périphériques** : Affiche les classes de périphériques et les périphériques installés sur le système ou qui ont été installés sur le système précédemment.
  - La protection s'applique généralement à une classe de périphérique. Un utilisateur ou groupe sélectionné peut accéder à tous les périphériques de la classe de périphérique.
  - La protection peut également s'appliquer à des périphériques spécifiques.
- **User List** (Liste des utilisateurs) : Affiche les utilisateurs et groupes autorisés ou non à accéder à la classe de périphérique ou au périphérique spécifique sélectionné.
  - Cette liste peut s'appliquer à un utilisateur spécifique ou à un groupe auquel appartient l'utilisateur.
  - Si un utilisateur ou groupe de la liste n'est pas disponible, le paramètre est hérité de la classe de périphérique affichée dans la liste des périphériques ou du dossier Classe.
  - Certaines classes de périphériques, par exemple DVD et CD-ROM, peuvent être contrôlées plus précisément en autorisant ou refusant séparément les accès en lecture et en écriture.

    Comme pour les autres périphériques et classes, les droits d'accès en lecture et en écriture peuvent être hérités. Par exemple, l'accès en lecture peut être hérité depuis une classe

supérieure, mais l'accès en écriture peut être explicitement refusé pour un utilisateur ou un groupe.

REMARQUE : Si la case Lecture est décochée, l'entrée de contrôle d'accès n'a aucun effet sur l'accès en lecture au périphérique. Elle n'octroie ni ne refuse l'accès au périphérique.

Exemple 1 : Si un utilisateur ou un groupe se voit refuser l'accès en écriture à un périphérique ou à une classe de périphériques :

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

Exemple 2 : Si un utilisateur ou un groupe se voit octroyer l'accès en écriture à un périphérique ou à une classe de périphériques :

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

Exemple 3 : Si un utilisateur ou un groupe se voit octroyer l'accès en lecture à un périphérique ou à une classe de périphériques :

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

Exemple 4 : Si un utilisateur ou un groupe se voit refuser l'accès en lecture à un périphérique ou à une classe de périphériques :

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

Exemple 5 : Si un utilisateur ou un groupe se voit octroyer l'accès en lecture+écriture à un périphérique ou à une classe de périphériques :

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

Exemple 6 : Si un utilisateur ou un groupe se voit refuser l'accès en lecture+écriture à un périphérique ou à une classe de périphériques :

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

Refus d'accès à un utilisateur ou groupe

Pour empêcher un utilisateur ou un groupe d'accéder à un périphérique ou à une classe de périphérique, procédez comme suit :

1. Dans le volet de gauche de **Console d'administration de HP ProtectTools**, cliquez sur **Device Access Manager**, puis sélectionnez **Configuration de classe de périphérique**.
2. Dans la liste de périphériques, cliquez sur la classe de périphérique à configurer.
   - Classe de périphérique
   - Tous les périphériques
   - Un seul périphérique
3. Sous **User/Groups** (Utilisateur/Groupe), cliquez sur l'utilisateur ou groupe auquel refuser l'accès.
4. Cliquez sur **Refuser** en regard d'un utilisateur ou d'un groupe.
5. Cliquez sur l'icône **Enregistrer**.

REMARQUE : Lorsque les paramètres d'autorisation et de refus sont définis au même niveau de périphérique pour un utilisateur, le refus d'accès est prioritaire sur l'autorisation d'accès.

Octroi d'accès pour un utilisateur ou un groupe

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

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

   La boîte de dialogue **Select Users or Groups** (Sélection d'utilisateurs ou groupes) s'affiche.
4. Cliquez sur **Advanced** (Avancé), puis sélectionnez **Find Now** (Rechercher maintenant) pour rechercher des utilisateurs et des groupes à ajouter.
5. Cliquez sur un utilisateur ou un groupe à ajouter à la liste des utilisateurs et groupes disponibles, puis cliquez sur **OK**.
6. Cliquez sur de nouveau sur **OK**.
7. Cliquez sur **Autoriser** pour octroyer l'accès à cet utilisateur ou groupe.
8. Cliquez sur l'icône **Enregistrer**.

Retrait de l'accès pour un utilisateur ou un groupe

Pour retirer à un utilisateur ou un groupe l'autorisation d'accéder à un périphérique ou à une classe de périphérique, procédez comme suit :

1. Dans le volet de gauche de **Console d'administration de HP ProtectTools**, cliquez sur **Device Access Manager**, puis sélectionnez **Configuration de classe de périphérique**.
2. Dans la liste de périphériques, cliquez sur la classe de périphérique à configurer.
   - Classe de périphérique
   - Tous les périphériques
   - Un seul périphérique
3. Sous **User/Groups** (Utilisateur/Groupes), cliquez sur l'utilisateur ou groupe à supprimer, puis cliquez sur **Supprimer**.
4. Cliquez sur l'icône **Enregistrer**.

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

Pour octroyer à un utilisateur l'autorisation d'accéder à une classe de périphérique tout en refusant l'accès à tous les autres membres du groupe de cet utilisateur, procédez comme suit :

1. Dans le volet de gauche de **Console d'administration de HP ProtectTools**, cliquez sur **Device Access Manager**, puis sélectionnez **Configuration de classe de périphérique**.
2. Dans la liste de périphériques, cliquez sur la classe de périphérique à configurer.
   - Classe de périphérique
   - Tous les périphériques
   - Un seul périphérique
3. Sous **User/Groups** (Utilisateur/Groupes), sélectionnez le groupe auquel refuser l'accès, puis cliquez sur **Refuser**.
4. Naviguez vers le dossier au-dessous de la classe requise et ajoutez l'utilisateur spécifique.
5. Cliquez sur **Autoriser** pour octroyer l'accès à cet utilisateur.
6. Cliquez sur l'icône **Enregistrer**.

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

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

1. Dans le volet de gauche de **Console d'administration de HP ProtectTools**, cliquez sur **Device Access Manager**, puis sélectionnez **Configuration de classe de périphérique**.
2. Dans la liste de périphériques, cliquez sur la classe de périphérique à configurer, puis naviguez vers le dossier au-dessous.
3. Cliquez sur **Ajouter**. La boîte de dialogue **Select Users or Groups** (Sélection d'utilisateurs ou groupes) s'affiche.

4. Cliquez sur **Advanced** (Avancé), puis sélectionnez **Find Now** (Rechercher maintenant) pour rechercher le groupe de l'utilisateur auquel vous souhaitez refuser l'accès à tous les périphériques de la classe.
5. Sélectionnez le groupe, puis cliquez sur **OK**.
6. Dabs la classe de périphérique, accédez au périphérique spécifique pour lequel vous souhaitez octroyer l'accès à l'utilisateur.
7. Cliquez sur **Ajouter**. La boîte de dialogue **Select Users or Groups** (Sélection d'utilisateurs ou groupes) s'affiche.
8. Cliquez sur **Advanced** (Avancé), puis sélectionnez **Find Now** (Rechercher maintenant) pour rechercher des utilisateurs et des groupes à ajouter.
9. Cliquez sur l'utilisateur auquel octroyer l'accès, puis cliquez sur **OK**.
10. Cliquez sur **Autoriser** pour octroyer l'accès à cet utilisateur.
11. Cliquez sur l'icône **Enregistrer**.

Réinitialisation de la configuration

△ **ATTENTION :** La réinitialisation de la configuration permet d'annuler toutes les modifications apportées à la configuration des périphériques et de rétablir toutes les valeurs définies en usine.

Pour rétablir les valeurs définies en usine, procédez comme suit :

1. Dans le volet de gauche de **Console d'administration de HP ProtectTools**, cliquez sur **Device Access Manager**, puis sélectionnez **Configuration de classe de périphérique**.
2. Sélectionnez le bouton **Réinitialiser**.
3. Cliquez sur **Oui** pour confirmer.
4. Cliquez sur l'icône **Enregistrer**.

Tâches avancées

Contrôle de l'accès aux paramètres de configuration

Dans la vue **Paramètres d'accès utilisateur**, les administrateurs spécifient les groupes ou utilisateurs qui sont autorisés à utiliser les pages Configuration simple et Configuration de classe de périphérique.

REMARQUE : Un utilisateur ou un groupe doit bénéficier des droits complets d'administrateur utilisateur pour modifier les paramètres de la vue Paramètres d'accès utilisateur.

- Un utilisateur ou un groupe doit bénéficier des droits d'affichage (en lecture seule) des paramètres de configuration dans la vue Paramètres d'accès utilisateur pour visionner les informations des vues Configuration simple et Configuration de classe de périphérique.
- Un utilisateur ou un groupe doit bénéficier des droits de modification des paramètres de configuration dans la vue Paramètres d'accès utilisateur pour modifier les informations des vues Configuration simple et Configuration de classe de périphérique.

REMARQUE : Même les membres du groupe d'administrateurs doivent bénéficier des droits en lecture pour visionner les vues Configuration simple et Configuration de classe de périphérique et des droits en modification pour modifier les données des vues Configuration simple et Configuration de classe de périphérique.

REMARQUE : Après l'évaluation des niveaux d'accès de tous les utilisateurs et groupes, si les options Autoriser ou Refuser ne sont pas sélectionnées pour un utilisateur à un niveau d'accès donné, l'utilisateur se voit refuser l'accès à ce niveau.

Octroi d'accès à un groupe ou utilisateur existant

Pour octroyer à un utilisateur ou un groupe existant l'autorisation d'afficher ou de modifier les paramètres de configuration, procédez comme suit :

1. Dans le volet de gauche de **HP ProtectTools Administrative Console** (Console d'administration de HP ProtectTools), cliquez sur **Device Access Manager**, puis sélectionnez **Paramètres d'accès utilisateur**.
2. Cliquez sur un groupe ou utilisateur auquel octroyer l'accès.
3. Sous **Permissions** (Autorisations), cliquez sur **Autoriser** pour chaque type d'autorisation à octroyer pour le groupe ou utilisateur sélectionné :

   REMARQUE : Les autorisations octroyées se cumulent. Par exemple, un utilisateur qui bénéficie des droits de modification des paramètres de configuration bénéficie automatiquement des droits d'affichage (en lecture seule) des paramètres de configuration. Un utilisateur qui bénéficie des droits complets d'administrateur utilisateur bénéficie également des droits de modification des paramètres de configuration et des droits d'affichage (en lecture seule) des paramètres de configuration.

   - Droits complets d'administrateur utilisateur
   - Droits de modification des paramètres de configuration
   - Droits d'affichage (en lecture seule) des paramètres de configuration
4. Cliquez sur l'icône **Enregistrer**.

Refus d'accès à un groupe ou utilisateur existant

Pour refuser à un utilisateur ou un groupe existant l'autorisation d'afficher ou de modifier les paramètres de configuration, procédez comme suit :

1. Dans le volet de gauche de **HP ProtectTools Administrative Console** (Console d'administration de HP ProtectTools), cliquez sur **Device Access Manager**, puis sélectionnez **Paramètres d'accès utilisateur**.
2. Cliquez sur un groupe ou utilisateur auquel refuser l'accès.
3. Sous **Permissions** (Autorisations), cliquez sur **Refuser** pour chaque type d'autorisation à refuser pour le groupe ou utilisateur sélectionné :
   - Droits complets d'administrateur utilisateur
   - Droits de modification des paramètres de configuration
   - Droits d'affichage (en lecture seule) des paramètres de configuration
4. Cliquez sur l'icône **Enregistrer**.

Ajout d'un nouveau groupe ou utilisateur

Pour octroyer à un nouvel utilisateur ou un nouveau groupe l'autorisation d'afficher ou de modifier les paramètres de configuration, procédez comme suit :

1. Dans le volet de gauche de **HP ProtectTools Administrative Console** (Console d'administration de HP ProtectTools), cliquez sur **Device Access Manager**, puis sélectionnez **Paramètres d'accès utilisateur**.
2. Cliquez sur **Ajouter**. La boîte de dialogue **Select Users or Groups** (Sélection d'utilisateurs ou groupes) s'affiche.
3. Cliquez sur **Advanced** (Avancé), puis sélectionnez **Find Now** (Rechercher maintenant) pour rechercher des utilisateurs et des groupes à ajouter.
4. Cliquez sur un groupe ou un utilisateur, cliquez sur **OK** et cliquez de nouveau sur **OK**.
5. Cliquez sur **Autoriser** pour octroyer l'accès à cet utilisateur.
6. Cliquez sur l'icône **Enregistrer**.

Retrait de l'accès d'un groupe ou d'un utilisateur

Pour retirer à un utilisateur ou un groupe l'autorisation d'afficher ou de modifier les paramètres de configuration, procédez comme suit :

1. Dans le volet de gauche de **HP ProtectTools Administrative Console** (Console d'administration de HP ProtectTools), cliquez sur **Device Access Manager**, puis sélectionnez **Paramètres d'accès utilisateur**.
2. Sélectionnez un groupe ou un utilisateur, puis cliquez sur **Supprimer**.
3. Cliquez sur l'icône **Enregistrer**.

Documentation connexe

Device Access Manager pour HP ProtectTools est compatible avec l'application professionnelle HP ProtectTools Enterprise Device Access Manager. Utilisé conjointement avec l'application professionnelle, Device Access Manager pour HP ProtectTools autorise un accès en lecture seule à ses propres fonctions.

Pour plus d'informations sur Device Access Manager pour HP ProtectTools, reportez-vous au site Web http://www.hp.com/hps/security/products.

11 LoJack Pro for HP ProtectTools

Computrace LoJack Pro, optimisé par Absolute Software (vendu séparément), permet de résoudre le problème croissant de la perte et du vol des ordinateurs.

L'activation de ce logiciel déclenche l'agent Computrace, qui reste actif dans votre ordinateur même en cas de reformatage ou de remplacement du disque dur.

LoJack Pro permet de réaliser à distance un contrôle, une gestion et un suivi de votre ordinateur. En cas de perte ou de vol de votre ordinateur, vous bénéficierez de l'assistance de l'équipe de restauration d'Absolute Software.*

REMARQUE : *Cette fonctionnalité dépend de votre situation géographique. Reportez-vous au contrat de souscription d'Absolute Software pour plus de détails.

12 Résolution de problèmes

HP ProtectTools Security Manager

Brève description	Détails	Solution
Les cartes Smart Card et les jetons USB ne sont pas disponibles dans Security Manager si leur installation est postérieure à celle de Security Manager.	Pour utiliser des cartes Smart Card ou des jetons USB dans Security Manager, le logiciel de prise en charge (pilote, fournisseur de services PKCS#11, etc.) doit être installé avant l'installation de Security Manager. Si Security Manager est déjà installé, procédez comme suit après l'installation du logiciel de prise en charge de la carte Smart Card ou du jeton USB :	Connectez-vous au Gestionnaire de mots de passe. Dans HP ProtectTools Security Manager, cliquez sur **Gestionnaire de mots de passe**, **Informations d'authentification**, puis sélectionnez **Smart Card** Si vous y êtes invité, redémarrez votre ordinateur.
Certaines pages Web d'application créent des erreurs qui empêchent l'utilisateur d'exécuter ou de terminer des tâches.	Certaines applications Web arrêtent de fonctionner et signalent des erreurs dues à la désactivation du modèle d'authentification unique (SSO). Par exemple, un **!** dans un triangle jaune apparaît dans Internet Explorer, indiquant qu'une erreur est survenue.	La fonction d'authentification unique n'est pas compatible avec toutes les interfaces Web. Désactivez la fonction d'authentification unique sur ces pages Web. Reportez-vous à la documentation complète sur la fonction d'authentification unique, disponible dans les fichiers d'aide de Security Manager. S'il n'est pas possible de désactiver l'authentification unique pour une application donnée, contactez l'assistance technique HP et demandez une assistance de niveau 3 au technicien HP.
L'option **Browse for Virtual Token** (Rechercher un jeton virtuel) ne s'affiche pas pendant la procédure de connexion.	L'utilisateur ne parvient pas à déplacer l'emplacement d'un jeton virtuel enregistré dans le Gestionnaire de mots de passe car l'option de navigation a été supprimée pour des raisons de sécurité.	L'option de navigation a été supprimée car elle permettait à des non utilisateurs de supprimer et de renommer des fichiers, puis de prendre le contrôle de Windows.
Les administrateurs de domaines ne peuvent pas changer le mot de passe Windows, même avec autorisation.	Cette situation se produit lorsqu'un administrateur de domaine se connecte à un domaine et enregistre l'identité du domaine dans le Gestionnaire de mots de passe à l'aide d'un compte doté de droits d'administration sur le domaine et l'ordinateur local. Lorsque l'administrateur de domaine tente de modifier le mot de passe Windows dans le Gestionnaire de mots de passe, un message d'erreur s'affiche : **User account restriction** (Restriction du compte utilisateur).	Le Gestionnaire de mots de passe ne peut pas modifier le mot de passe du compte d'un utilisateur de domaine via l'option **Modifiez le mot de passe Windows**. Security Manager peut uniquement modifier les mots de passe des comptes des PC locaux. L'utilisateur de domaine ne peut pas changer son mot de passe via l'option **Modifier le mot de passe** de **Sécurité de Windows**, mais comme il ne possède pas de compte physique sur le PC local, le Gestionnaire de mots de passe peut uniquement utiliser le mot de passe utilisé pour la connexion.
Le Gestionnaire de mots de passe rencontre des	Si l'utilisateur se connecte au Gestionnaire de mots de passe, crée un	HP recherche actuellement une solution pour les prochaines versions du logiciel.

Brève description	Détails	Solution
problèmes d'incompatibilité avec la bibliothèque d'authentification et d'identification graphique Corel WordPerfect 12.	document dans WordPerfect et l'enregistre en le protégeant avec un mot de passe, le Gestionnaire ne peut pas détecter ou reconnaître (manuellement ou automatiquement) la bibliothèque d'authentification et d'identification graphique.	
Le Gestionnaire de mots de passe ne reconnaît pas le bouton **Connecter** à l'écran.	Si les informations d'authentification unique pour une Connexion Bureau à distance sont définies sur **Connecter**, lorsque la fonction d'authentification unique est relancée, elle indique toujours **Enregistrer sous** au lieu de **Connecter**.	HP recherche actuellement une solution pour les prochaines versions du logiciel.
L'utilisateur ne parvient pas à se connecter au Gestionnaire de mots de passe après être passé du mode veille au mode veille prolongée sous Windows XP (Service Pack 1 uniquement).	Après avoir autorisé le système à passer du mode veille au mode veille prolongée, l'administrateur ou l'utilisateur ne parvient pas à se connecter au Gestionnaire de mots de passe et l'écran de connexion Windows reste affiché, quelles que soient les informations d'authentification (mot de passe, empreinte digitale ou carte Java Card) sélectionnées.	Effectuez la mise à jour de Windows en appliquant le correctif Service Pack 2 via Windows Update. Pour plus d'informations sur l'origine du problème, consultez la base de connaissances de Microsoft (article 813301) à l'adresse http://www.microsoft.com. Pour se connecter, l'utilisateur doit sélectionner le Gestionnaire de mots de passe et s'authentifier. Une fois connecté au Gestionnaire de mots de passe, l'utilisateur est invité à se connecter à Windows (l'utilisateur peut être amené à sélectionner l'option de connexion Windows) afin de terminer le processus de connexion. Si l'utilisateur se connecte en premier à Windows, il doit se connecter manuellement au Gestionnaire de mots de passe.
Le processus de sécurité **Restauration d'identité** perd l'association avec le jeton virtuel.	Lorsque l'utilisateur restaure une identité, le Gestionnaire de mots de passe peut perdre l'association avec l'emplacement du jeton virtuel dans l'écran de connexion. Même si un jeton virtuel est enregistré dans le Gestionnaire de mots de passe, l'utilisateur doit enregistrer de nouveau le jeton pour restaurer l'association.	Le système est ainsi conçu. Lors d'une désinstallation de Security Manager sans préservation des identités, la partie système (serveur) du jeton est détruite ; le jeton ne peut alors plus être utilisé pour la connexion, même si la partie client du jeton est restaurée par le biais de la restauration d'identité. HP recherche des solutions à long terme.

Device Access Manager pour HP ProtectTools

Des utilisateurs se sont vus refuser l'accès à des périphériques dans Device Access Manager mais ceux-ci sont toujours accessibles.

- **Explication :** La vue Configuration simple et/ou Configuration de classe de périphérique a été utilisée dans Device Access Manager pour refuser aux utilisateurs l'accès aux périphériques. Malgré l'interdiction, les utilisateurs peuvent toujours accéder aux périphériques.
- **Solution :**
  - Vérifiez que le service Verrouillage des périphériques/Audition HP ProtectTools a démarré.
  - En tant qu'utilisateur administratif, cliquez sur **Panneau de configuration**, puis sur **Système et maintenance**. Dans la fenêtre Outils d'administration, cliquez sur **Services** et recherchez le service **Verrouillage des périphériques/Audition HP ProtectTools**. Assurez-vous que le service a démarré et que le type de démarrage est défini sur **Automatique**

Un utilisateur se voit accorder ou refuser de manière inattendue l'accès à un périphérique.

- **Explication :** Device Access Manager a été utilisé pour refuser l'accès à certains périphériques à l'utilisateur et lui accorder l'accès à d'autres périphériques. Lorsque l'utilisateur utilise le système, il peut accéder à des périphériques pour lesquels il pense que Device Access Manager lui a refusé l'accès et ne peut pas accéder à des périphériques pour lesquels il pense que Device Access Manager lui a accordé l'accès.
- **Solution :**
  - Utilisez la vue Configuration de classe de périphérique dans Device Access Manager pour vérifier les paramètres de périphériques de l'utilisateur.
  - Cliquez sur **Security Manager**, sur **Device Access Manager** puis sur **Configuration de classe de périphérique**. Développez les niveaux de l'arborescence Classe de périphérique et vérifiez les paramètres applicables à cet utilisateur. Examinez les droits « Refuser » pouvant être définis pour l'utilisateur ou tout groupe Windows duquel il est membre (par exemple, Utilisateurs ou Administrateurs).

Autorisation ou interdiction. Lequel est prioritaire ?

- **Explication :** Dans la vue Configuration de classe de périphérique, la configuration suivante a été définie :
  - Le droit « Autoriser » a été défini pour un groupe Windows (par exemple, BUILTIN \Administrateurs) et le droit « Refuser » a été défini pour un autre groupe Windows (par exemple, BUILTIN\Utilisateurs) situé au même niveau dans la hiérarchie des classes de périphériques (par exemple, Lecteurs de DVD/CD-ROM).
  - Si un utilisateur est membre de ces deux groupes (par exemple, Administrateur), lequel est prioritaire ?
- **Solution :**
  - L'utilisateur se voit refuser l'accès au périphérique. L'interdiction est prioritaire sur l'autorisation.
  - L'accès est refusé à cause de la manière dont Windows traite le droit effectif pour le périphérique. L'un des groupes se voit accorder l'accès et l'autre non, mais l'utilisateur appartient aux deux groupes. L'utilisateur se voit refuser l'accès car l'interdiction est prioritaire sur l'autorisation.
  - Une solution de contournement consiste à refuser l'accès au groupe Utilisateurs au niveau Lecteurs de DVD/CD-ROM et à autoriser l'accès au groupe Administrateurs au même niveau.
  - Une autre solution consiste à créer des groupes Windows spécifiques, l'un pour autoriser l'accès aux DVD/CD et l'autre pour en refuser l'accès. Des utilisateurs spécifiques peuvent ensuite être ajoutés au groupe approprié.

La vue Configuration simple a été utilisée pour définir une règle de contrôle d'accès aux périphériques mais les utilisateurs administratifs ne peuvent pas accéder aux périphériques.

- **Explication :** La vue Configuration simple refuse l'accès aux Utilisateurs et aux Invités et autorise l'accès aux Administrateurs de périphériques.
- **Solution :** Ajoutez l'utilisateur administratif au groupe Administrateurs de périphériques.

Divers

Logiciel affecté — Brève description	Détails	Solution
Security Manager - Avertissement reçu : **Cette application de sécurité ne peut pas être installée avant que HP ProtectTools Security Manager soit installé**.	Toutes les applications de sécurité, telles que Java Card Security et les lecteurs biométriques, sont des modules extensibles pour l'interface de Security Manager. Security Manager doit être installé pour qu'un module de sécurité agréé HP puisse être chargé.	Le logiciel Security Manager doit être installé avant toute installation d'un module de sécurité.
Une erreur se produit parfois lors de la fermeture de l'interface du Security Manager.	Occasionnellement (1 fois sur 12) une erreur se produit en cliquant sur l'icône de fermeture dans l'angle supérieur droit de la fenêtre du Security Manager avant que le chargement des applications additionnelles soit terminé.	Ce problème est en relation avec le temps de chargement des applications additionnelles lors de la fermeture et du redémarrage du Security Manager. Étant donné que PTHOST.exe est le programme principal couvrant les autres applications additionnelles, il dépend du temps de chargement des autres applications (services). Le fait de fermer le programme principal avant qu'un service soit complètement chargé est la cause première de l'erreur. Autorisez Security Manager à finaliser le chargement des services (message affiché en haut de la fenêtre Security Manager) et de tous les modules répertoriés dans la colonne de gauche. Pour éviter un échec, prévoyez un temps de chargement raisonnable pour les modules.
HP ProtectTools : Les privilèges d'accès non restreint ou d'administrateur non contrôlés entraînent des risques de sécurité.	De nombreux risques existent avec un accès au PC client non restreint, notamment les suivants : • Suppression du lecteur sécurisé personnel • Modification malveillante des paramètres utilisateur • Désactivation des stratégies et fonctions de sécurité	Les administrateurs sont encouragés à suivre les meilleures pratiques et à réduire les droits et l'accès des utilisateurs finaux. Les utilisateurs non-autorisés ne doivent pas bénéficier de droits d'administration.

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 *Voir* 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 qui permet le recryptage de clés utilisateur de base d'une clé de propriétaire de plateforme à une autre.

ATM Automatic Technology Manager, qui permet aux administrateurs réseau de gérer des systèmes à distance au niveau du BIOS.

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

authentification à la mise sous tension Fonction de sécurité qui requiert une certaine forme d'authentification, telle qu'une Java Card, une puce de sécurité ou un mot de passe, lors la mise sous tension de l'ordinateur.

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

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

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

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

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

carte d'identité Gadget du Volet Windows qui permet d'identifier visuellement votre bureau avec votre nom d'utilisateur et une photo de votre choix. Cliquez sur la carte d'identité pour ouvrir la console d'administration de HP ProtectTools.

certificat numérique Informations d'authentification électroniques qui confirment l'identité d'un individu ou d'une société en reliant l'identité du propriétaire du certificat numérique à une paire de clés électroniques utilisées pour signer des informations numériques.

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

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

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

compte réseau Compte d'utilisateur ou d'administrateur Windows, sur un ordinateur local, dans un groupe de travail ou sur un domaine.

compte utilisateur Windows Profil d'un individu autorisé à se connecter à un réseau ou à un ordinateur individuel.

connexion Objet de Security Manager qui est composé d'un nom d'utilisateur et d'un mot de passe (et parfois d'autres informations) qui peut être utilisé pour la connexion aux sites Web ou à d'autres programmes.

console Emplacement central permettant d'accéder aux fonctions et paramètres de ce programme et de les gérer.

contact authentifié Personne ayant accepté une invitation de contact authentifié.

cryptage Procédure, telle que l'utilisation d'un algorithme, employée en cryptographie pour convertir un texte normal en un texte crypté afin d'empêcher la lecture des données par des destinataires non autorisés. Il existe plusieurs types de cryptage de données, qui forment la base de la sécurité du réseau. Les types courants incluent DES (Data Encryption Standard) et le cryptage de clés publiques.

cryptographie Pratique de cryptage et décryptage de données afin qu'elles ne puissent être décodées que par des individus spécifiques.

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

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

destinataire de contact authentifié Personne recevant une invitation à devenir un contact authentifié.

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

destruction automatique Destruction planifiée que l'utilisateur configure dans File Sanitizer.

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

domaine Groupe d'ordinateurs qui font partie d'un réseau et qui partagent une base de données de répertoires communs. Chaque domaine possède un nom unique et dispose d'un ensemble de règles et procédures communes.

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 lie l'unité de disque dur à un utilisateur et nécessite que celui-ci entre correctement le mot de passe DriveLock au démarrage de l'ordinateur.

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

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

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.

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

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

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

HP SpareKey Copie de sauvegarde de la clé Drive Encryption.

identité Dans l'utilitaire HP ProtectTools Security Manager, groupe d'informations d'authentification et de paramètres qui est traité comme un compte ou un profil pour un utilisateur donné.

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

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

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

jeton Voir méthode de connexion sécurisée.

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

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

lecteur sécurisé personnel Lecteur sécurisé personnel qui fournit une zone de stockage protégée aux données confidentielles.

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

liste des contacts authentifiés Liste complète des contacts authentifiés.

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

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

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

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

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

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

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

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

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.

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

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.

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

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

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

service en arrière-plan Service en arrière-plan de verrouillage des périphériques/audition HP ProtectTools, qui doit être en cours d'exécution pour appliquer les stratégies de contrôle d'accès aux périphériques. Il est accessible dans l'application Services, en sélectionnant l'option Outils d'administration du Panneau de configuration. Si le service n'est pas en cours d'exécution, HP ProtectTools Security Manager tente de le démarrer lorsque les stratégies de contrôle d'accès sont appliquées.

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

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

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

Smart Card Petite pièce de matériel, de mêmes taille et forme qu'une carte bancaire, qui stocke des informations d'identification concernant le propriétaire. Utilisée pour authentifier le propriétaire sur un ordinateur.

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

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

tableau de bord Emplacement central permettant d'accéder aux fonctions et paramètres de ce programme et de les gérer.

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

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

utilisateur autorisé Utilisateur autorisé, dans la vue Paramètres d'accès utilisateur, à afficher ou modifier les paramètres de configuration des vues Configuration simple et Configuration de classe de périphérique.

visionneuse d'historique Live Messenger Composant de Privacy Manager Chat permettant de rechercher et d'afficher des sessions d'historique de messagerie instantanée cryptées.

Index