HP Client Security

Mise en route

Première édition : août 2013

Référence du document : 735339-051

Sommaire

1 Introduction à HP Client Security Manager 1

Fonctions de HP Client Security 1

Description et exemples d'utilisation courante des produits HP Client Security 3

Password Manager 3

HP Drive Encryption (certains modèles uniquement) 4

HP Device Access Manager (certains modèles uniquement) 5

Computrace (vendu séparément) 5

Atteinte des principaux objectifs de sécurité 5

Protection contre le vol ciblé 6

Limitation de l'accès aux données sensibles 6

Blocage de l'accès non autorisé depuis les emplacements internes ou externes 6

Création de règles de mot de passe fort 6

Éléments de sécurité supplémentaires 7

Attribution de rôles de sécurité 7

Gestion des mots de passe dans HP Client Security 7

Création d'un mot de passe sécurisé 8

Sauvegarde des informations et paramètres d'authentification 8

2 Mise en route 9

Ouverture de HP Client Security 10

3 Guide de configuration facile pour les petites entreprises 11

Mise en route 11

Password Manager 11

Affichage et gestion des authentifications enregistrées dans Password Manager 12

HP Device Access Manager 13

HP Drive Encryption 13

4 HP Client Security 14

Fonctions, applications et paramètres d'identité 14

Empreintes digitales 14

Paramètres d'administration des empreintes digitales 15

Paramètres d'utilisateur des empreintes digitales 16

HP SpareKey — Récupération de mot de passe 16

Paramètre SpareKey HP 16

Mot de passe Windows 17

Périphériques Bluetooth 17
Paramètres des périphériques Bluetooth 17
Cartes 18
Paramètres des cartes à puce, de proximité et sans contact 19
PIN 19
Paramètres de PIN 20
RSA SecurID 20
Gestionnaire de mots de passe 20
Si aucune connexion n'a été créée pour les pages Web ou les programmes . . 21
Si une connexion a déjà été créée pour les pages Web ou les programmes … 21
Ajout de connexions 21
Modification des connexions 23
Utilisation du menu Liens rapides du Gestionnaire de mots de passe 23
Organisation des connexions en catégories 24
Gestion de vos connexions 24
Évaluation de la force de votre mot de passe 25
Paramètres de l'icône du Gestionnaire de mots de passe 25
Importation et exportation de connexions 26
Paramètres 27
Paramètres avancés 28
Règles d'administrateur 28
Règles d'utilisateur standard 29
Fonctions de sécurité 29
Utilisateurs 30
Mes règles 30
Sauvegarde et restauration de vos données 31

5 HP Drive Encryption (certains modèles uniquement) 33
Ouverture de Drive Encryption 33
Tâches générales 34
Activation de Drive Encryption pour les disques durs standard 34
Activation de Drive Encryption pour les unités auto-cryptées 34
Désactivation de Drive Encryption 35
Connexion après l'activation de Drive Encryption 35
Cryptage de disques durs supplémentaires 36
Tâches avancées 36
Gestion de Drive Encryption (administrateur uniquement) 36
Cryptage ou décryptage de partitions d’unités individuelles (cryptage logiciel uniquement) 37
Gestion des disques 37
Sauvegarde et restauration (tâche administrateur) 37

Sauvegarde des clés de cryptage 37
Restauration de l’accès à un ordinateur activé à l’aide des clés de sauvegarde 38
Récupération de HP SpareKey 38

6 Assainisseur de fichiers HP (certains modèles uniquement) 40
Destruction 40
Nettoyage de l'espace libre 40
Ouverture de l'Assainisseur de fichiers 41
Procédures de configuration 41
Définition d'une programmation de destruction 42
Définition d'une programmation de nettoyage de l'espace libre 43
Protéger des fichiers d'une destruction 43
Tâches générales 43
Utilisation de l'icône File Sanitizer 44
Destruction par bouton droit 44
Lancement manuel d'une opération de destruction 44
Lancement manuel du nettoyage de l'espace libre 45
Affichage des fichiers journaux 45

7 HP Device Access Manager (certains modèles uniquement) 46
Ouverture de Device Access Manager 47
Vue utilisateur 47
Vue système 47
Configuration JITA 49
Création d'une politique JITA pour un utilisateur ou un groupe 49
Désactivation d'une politique JITA pour un utilisateur ou un groupe 49
Paramètres 49
Classes de périphériques non gérées 50

8 HP Trust Circles 52
Ouverture de Trust Circles 52
Mise en route 52
Trust Circles 53
Ajout de dossiers à un cercle de confiance 53
Ajout de membres à un cercle de confiance 54
Ajout de fichiers à un cercle de confiance 54
Dossiers cryptés 55
Suppression de dossiers placés dans un cercle de confiance 55
Suppression d'un fichier placé dans un cercle de confiance 55

Retrait de membres d'un cercle de confiance 55
Suppression d'un cercle de confiance 56
Configuration des préférences 56

9 Récupération en cas de vol (certains modèles) 58

10 Exceptions de mot de passe localisé 59
Que faire lorsqu'un mot de passe est rejeté 59
Les IME Windows ne sont pas pris en charge au niveau de l'Authentification à la mise sous tension ou de Drive Encryption 59
Changements de mot de passe à l'aide d'une disposition de clavier également prise en charge 60
Gestion des touches spéciales 60

Glossaire 63

Index 67

1 Introduction à HP Client Security Manager

HP Client Security vous permet de protéger vos données, votre périphérique, et votre identité, augmentant ainsi la sécurité de votre ordinateur.

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

Les modules logiciels de HP Client Manager sont préinstallés, préchargés ou téléchargeables depuis le site Web de HP. Pour plus d'informations, reportez-vous à la section http://www.hp.com.

REMARQUE : Les instructions fournies dans ce guide présupposent que vous avez déjà installé les modules logiciels de HP Client Security en question.

Fonctions de HP Client Security

Le tableau suivant répertorie les principales fonctions des modules de HP Client Security.

Module	Fonctions principales
HP Client Security Manager	Les administrateurs peuvent exécuter les fonctions suivantes : • Protéger votre ordinateur avant que Windows® ne démarre • Protéger votre compte Windows en utilisant une authentification stricte • Gérer votre connexion et vos mots de passe pour des sites web et des applications • Changer facilement le mot de passe de votre système d'exploitation Windows • Utiliser les empreintes digitales pour une sécurité et un confort supplémentaires • Configurer une carte Smart Card, une carte sans contact ou une carte de proximité pour l'authentification • Utiliser votre téléphone Bluetooth comme méthode d'identification • Définir un code PIN pour étendre vos choix d'authentification • Configurer les règles de connexion et de session • Sauvegarder et restaurer vos données de programme • Ajouter de nouvelles applications, telles que HP Drive Encryption, HP File Sanitizer, HP Trust Circles, HP Device Access Manager, et HP Computrace Les utilisateurs généraux peuvent effectuer les fonctions suivantes : • Afficher les paramètres pour l'état du cryptage et Device Access Manager. • Activer Computrace. • Configurer les préférences et les options de sauvegarde et de restauration.
Password Manager	Les utilisateurs généraux peuvent exécuter les fonctions suivantes : • Organiser et configurer les noms d’utilisateur et les mots de passe. • Créer des mots de passe plus forts pour une sécurité accrue de compte pour les comptes de messagerie et Web. Password Manager remplit et envoie les informations automatiquement. • Rationnaliser le processus de connexion avec la fonction d’authentification unique, qui mémorise et applique automatiquement les informations d’authentification de l’utilisateur. • Marquer un compte comme compromis, afin que vous puissiez être alerté pour d'autres compte(s) avec des informations d'identification similaires. • Importer des données de connexion depuis un navigateur pris en charge.

Module	Fonctions principales
HP Drive Encryption (certains modèles uniquement)	• Fournit un cryptage du volume complet du disque dur. • Permet de forcer une authentification au préamorçage afin de décrypter les données et d'y accéder. • Offre la possibilité d'activer des unités autocryptées (certains modèles uniquement).
HP Device Access Manager	• Permet aux responsables informatiques de contrôler l'accès aux périphériques en fonction des profils des utilisateurs. • Empêche les utilisateurs non autorisés de supprimer des données en les transférant sur un support de stockage externe et d'introduire des virus dans le système à partir d'un support externe. • Permet aux administrateurs de désactiver l'accès d'un utilisateur ou d'un groupe d'utilisateurs spécifique aux périphériques de communication.
HP Trust Circles	• Sécurise les fichiers et les documents. • Crypte les fichiers placés dans des dossiers dont l'utilisateur est spécifié et les protège dans un cercle de confiance. • Autorise l'utilisation et le partage de fichiers uniquement par des membres du cercle de confiance.
Theft Recovery (Computrace, vendu séparément)	• Activation nécessitant des abonnements séparés aux services de suivi et de traçage. • Permet le suivi des ressources en toute sécurité. • Surveille les activités de l'utilisateur, ainsi que les modifications apportées au matériel et aux logiciels. • Reste actif même si vous reformatez ou remplacez le disque dur.

Description et exemples d'utilisation courante des produits HP Client Security

La plupart des produits HP Client Security disposent à la fois d'un système d'authentification utilisateur (généralement par mot de passe) et d'un système de sauvegarde administrative permettant l'obtention d'accès en cas de perte, indisponibilité ou oubli de mot de passe et lorsque requis par le service de sécurité de l'entreprise.

REMARQUE : Certains produits HP Client Security sont conçus pour permettre la définition de restrictions d'accès aux données. Le cryptage des données est nécessaire lorsque leur importance est telle que leur perte par l'utilisateur est préférable à leur compromission. Il est recommandé de sauvegarder toutes les données dans un emplacement sécurisé.

Password Manager

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

- Enregistrer les noms et les mots de passe de connexion pour l'accès à Internet ou à la messagerie électronique.
- Connecter automatiquement l'utilisateur à un site Web ou à la messagerie électronique.

- Gérer et organiser des authentifications.
- Sélectionner une ressource Web ou réseau et accéder directement au lien.
- Afficher les noms et les mots de passe si nécessaire.
- Marquer un compte comme compromis, afin que vous puissiez être alerté pour d'autres compte(s) avec des informations d'identification similaires.
- Importer des données de connexion depuis un navigateur pris en charge.

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

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

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

HP Drive Encryption (certains modèles uniquement)

HP Drive Encryption permet de restreindre l'accès aux données ou à l'intégralité du disque dur principal ou d'un disque dur secondaire. Il permet également la gestion de disques durs à auto-chiffrement.

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

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

HP Device Access Manager (certains modèles uniquement)

HP Device Access Manager permet à un administrateur de restreindre et de gérer les accès aux périphériques. Il peut être utilisé pour bloquer les accès non autorisés à des clés USB afin d'éviter la copie de données. Il permet également de restreindre l'accès aux lecteurs CD/DVD, de contrôler les périphériques USB et les connexions réseau, etc. Par exemple, des fournisseurs externes peuvent avoir besoin d'accéder aux ordinateurs de votre entreprise, mais ne pas être autorisés à en copier les données sur une clé USB.

Exemple 1 : Le responsable d'une société de matériel médical travaille souvent avec des dossiers médicaux personnels parallèlement aux informations propriétaires de sa société. Les employés doivent pouvoir accéder à ces données, mais il est fondamental que celles-ci ne puissent pas être supprimées de l'ordinateur et copiées sur une clé USB ou tout autre support de stockage externe. Le réseau est sécurisé, mais les ordinateurs sont équipés de graveurs CD et de ports USB permettant la copie ou le vol de données. Le responsable utilise Device Access Manager pour désactiver les graveurs CD et les ports USB afin d'en empêcher l'utilisation. Même si les ports USB sont bloqués, les souris et claviers continuent à fonctionner.

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

Computrace (vendu séparément)

Computrace est un service permettant de localiser un ordinateur portable volé lorsque son utilisateur accède à Internet. Il facilite également la gestion et la localisation d'ordinateurs distants, ainsi que la surveillance de leur utilisation et de leurs applications.

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

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

Atteinte des principaux objectifs de sécurité

La collaboration entre les modules de HP Client Security permet d'apporter des solutions à divers problèmes de sécurité, notamment grâce à :

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

Protection contre le vol ciblé

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

- Une fois activée, la fonction d'authentification au préamorçage d'empêcher l'accès au système d'exploitation.
  - HP Client Security — Consultez HP Client Security à la page 14.
  - HP Drive Encryption — Reportez-vous à la section HP Drive Encryption (certains modèles uniquement) à la page 33.
- Encryption permet de garantir que les données ne sont pas accessibles même si le disque dur est retiré et installé dans un système non sécurisé.
- Computrace peut suivre l'emplacement de l'ordinateur volé.
  - Computrace — Reportez-vous à la section Récupération en cas de vol (certains modèles) à la page 58.

Limitation de l'accès aux données sensibles

Supposons qu'un auditeur de contrats travaille sur site et bénéficie d'un accès à des données financières confidentielles. Vous ne souhaitez pas qu'il puisse imprimer des fichiers ou les enregistrer sur un support inscriptible, par exemple un CD. Les fonctions suivantes vous permettent de restreindre l'accès aux données :

- HP Device Access Manager permet aux responsables informatiques de restreindre l'accès aux périphériques de communication pour empêcher la copie d'informations confidentielles depuis le disque dur. Reportez-vous à la section Vue système à la page 47.

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

L'accès non autorisé à un ordinateur professionnel non sécurisé représente un risque réel pour les ressources réseau de l'entreprise, notamment les informations provenant des services financiers, d'un cadre ou de l'équipe de Recherche et développement, et les informations privées telles que les dossiers de patient ou les dossiers financiers personnels. Les fonctions suivantes permettent d'empêcher tout accès non autorisé :

- Une fois activée, la fonction d'authentification au préamorçage d'empêcher l'accès au système d'exploitation. (reportez-vous à la section HP Drive Encryption (certains modèles uniquement) à la page 33.
- HP Client Security garantit qu'un utilisateur non autorisé ne peut pas obtenir de mots de passe ni accéder à des applications protégées par des mots de passe. Reportez-vous à la section HP Client Security à la page 14.
- Device Access Manager permet aux responsables informatiques de retreindre l'accès aux périphériques inscriptibles pour empêcher la copie d'informations confidentielles depuis le disque dur. Reportez-vous à la section HP Device Access Manager (certains modèles uniquement) à la page 46.

Création de règles de mot de passe fort

Si une politique d'entreprise exige que vous utilisiez un mot de passe fort pour une dizaine d'applications et de bases de données Web, Security Manager propose un référentiel sécurisé pour

simplifier les mots de passe et l'authentification unique. Reportez-vous à la section Gestionnaire de mots de passe à la page 20.

Éléments de sécurité supplémentaires

Attribution de rôles de sécurité

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

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

Les responsabilités et privilèges de sécurité peuvent être répartis entre les rôles suivants :

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

  REMARQUE : De nombreuses fonctions de HP Client Security peuvent être personnalisées par le responsable de la sécurité en coopération avec HP. Pour plus d'informations, reportez-vous à la section http://www.hp.com.

- Administrateur informatique — Il applique et gère les fonctions de sécurité définies par le responsable de la sécurité. Il peut également activer ou désactiver certaines fonctions. Par exemple, si le responsable de la sécurité a décidé de déployer des cartes à puce, l'administrateur informatique peut activer à la fois le mode mot de passe et le mode carte à puce.
- Utilisateur — Il utilise les fonctions de sécrurité. Par exemple, si le responsable de la sécurité et l'administrateur informatique ont activé les cartes à puce sur le système, l'utilisateur peut définir un code PIN de carte à puce et l'utiliser pour s'identifier.

ATTENTION : Les administrateurs sont encouragés à respecter les « meilleures pratiques » en matière de restriction des privilèges et accès des utilisateurs finaux.

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

Gestion des mots de passe dans HP Client Security

La majorité des fonctions de HP Client Security sont sécurisées par mot de passe. Le tableau suivant répertorie les mots de passe couramment utilisés, le module logiciel dans lequel ils sont utilisés et leurs fonctions.

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

Mot de passe de HP Client Security	Défini dans le module suivant	Fonction
Mot de passe d'ouverture de session Windows	Panneau de configuration Windows ou HP Client Security	Peut être utilisé pour la connexion et l'authentification manuelles afin d'accéder aux diverses fonctions de HP Client Security.

Mot de passe de HP Client Security	Défini dans le module suivant	Fonction
HP Client Security : mot de passe pour la sauvegarde et la restauration	HP Client Security, par utilisateur	Protège l'accès au fichier de sauvegarde et restauration de HP Client Security.
Code PIN de la carte Smart Card	Credential Manager	Peut être utilisé pour une authentification multifacteur. Peut être utilisé pour une authentification Windows. Authentifie les utilisateurs de Drive Encryption si la carte Smart Card est sélectionnée.

Création d’un mot de passe sécurisé

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

- Utilisez des mots de passe de plus de 6 caractères, et même de préférence de plus de 8 caractères.
- Mélangez les majuscules et les minuscules dans votre mot de passe.
- Si possible, mélangez les caractères alphanumériques et incluez des caractères spéciaux et des signes de ponctuation.
- Remplacez les lettres par des caractères spéciaux ou des nombres dans un mot clé. Par exemple, vous pouvez utiliser le chiffre 1 pour la lettre I ou L.
- Combinez des mots de 2 langues ou plus.
- Coupez un mot ou une expression contenant des chiffres ou des caractères spéciaux au milieu, par exemple « Mary2-2Cat45 ».
- N’utilisez pas un mot de passe qui figurerait dans un dictionnaire.
- N’utilisez pas votre nom comme mot de passe, ni aucune autre information personnelle, telle que votre date de naissance, des noms d'animaux de compagnie ou le nom de jeune fille de votre mère, même si vous le saisissez à l’envers.
- Modifiez les mots de passe régulièrement. Vous pouvez ne modifier que quelques caractères.
- Si vous notez votre mot de passe, ne le stockez pas à un endroit visible proche de l’ordinateur.
- N’enregistrez pas le mot de passe dans un fichier, tel qu’un message électronique, sur l’ordinateur.
- Ne partagez pas les comptes et ne communiquez votre mot de passe à personne.

Sauvegarde des informations et paramètres d'authentification

L'outil de sauvegarde et de restauration de HP Client Security fournit un emplacement central à partir duquel vous pouvez sauvegarder et restaurer les informations d'authentification sécurisée de certains des modules de HP Client Security installés.

2 Mise en route

Pour configurer HP Client Security de sorte à utiliser vos informations d'authentification, lancez HP Client Security selon l'une des méthodes suivantes : Une fois qu'un utilisateur a entièrement renseigné l'assistant, celui-ci ne pourra pas être relancé par cet utilisateur.

1. Dans l'Écran d'accueil ou des applications, cliquez ou tapez sur l'application **HP Client Security** (Windows 8).

   –ou–

   Sur le bureau Windows, cliquez ou tapez sur le gadget **HP Client Security** (Windows 7).

   –ou–

   Sur le bureau Windows, double-cliquez ou double-tapez sur l'icône **HP Client Security** dans la zone de notification, située tout à droite de la barre des tâches.

   –ou–

   Sur le bureau Windows, cliquez ou tapez sur l'icône **HP Client Security** dans la zone de notification, puis sélectionnez **Ouvrir HP Client Security**.

2. L'assistant de configuration de HP Client Security se lance en affichant la page d'accueil.

3. Lisez les informations de l'Écran d'accueil, vérifiez votre identité en tapant votre mot de passe Windows, puis cliquez ou tapez sur **Suivant**.

   Si vous n'avez pas encore créé de mot de passe Windows, vous serez invité à le faire. Un mot de passe Windows est nécessaire pour protéger l'accès à votre compte Windows vis-à-vis de personnes non autorisées et utiliser les fonctions de HP Client Security.

4. Sur la page HP SpareKey, sélectionnez trois questions de sécurité. Saisissez une réponse pour chaque question, puis cliquez sur **Suivant**. Les questions personnalisées sont autorisées. Pour plus d'informations, reportez-vous à la section HP SpareKey — Récupération de mot de passe à la page 16.

5. Sur la page Empreintes digitales, enregistrez au minimum le nombre d'empreintes digitales requises, puis cliquez ou tapez sur **Suivant**. Pour plus d'informations, reportez-vous à la section Empreintes digitales à la page 14.

6. Sur la page de Drive Encryption, activez le cryptage, sauvegardez la clé de cryptage, puis cliquez ou tapez sur **Suivant**. Pour plus d'informations, reportez-vous à l'aide logicielle de HP Drive Encryption.

REMARQUE : Ceci concerne le cas dans lequel l'utilisateur est un administrateur et l'assistant de configuration de HP Client Security n'a pas été configuré auparavant par un administrateur.

7. À la dernière page de l'assistant, cliquez ou tapez sur **Terminer**.

   Cette page indique l'état des fonctions et des informations d'authentification.

8. L'assistant de configuration de HP Client Security garantit la bonne activation de l'authentification Just In Time et des fonctions de File Sanitizer. Pour plus d'informations, consultez les aides logicielles de HP Device Access Manager et HP File Sanitizer.

REMARQUE : Ceci concerne le cas dans lequel l'utilisateur est un administrateur et l'assistant de configuration de HP Client Security n'a pas été configuré auparavant par un administrateur.

Ouverture de HP Client Security

Vous pouvez ouvrir l'application HP Client Security de l'une des façons suivantes :

REMARQUE : Il faut mener à bien l'assistant de configuration de HP Client Security pour que l'application HP Client Security HP puisse être lancée.

- Dans l'Écran d'accueil ou des applications, cliquez ou tapez sur l'application **HP Client Security**.

  –ou–

  Sur le bureau Windows, cliquez ou tapez sur le gadget **HP Client Security** (Windows 7).

  –ou–

  Sur le bureau Windows, double-cliquez ou double-tapez sur l'icône **HP Client Security** dans la zone de notification, située tout à droite de la barre des tâches.

  –ou–

  Sur le bureau Windows, cliquez ou tapez sur l'icône **HP Client Security** dans la zone de notification, puis sélectionnez **Ouvrir HP Client Security**.

3 Guide de configuration facile pour les petites entreprises

Cette section présente les principales étapes à suivre pour activer les options les plus courantes et les plus utiles de HP Client Security pour les PME. Le logiciel offre de nombreux outils et options vous permettant de définir vos préférences et vos paramètres de contrôle d'accès. Ce Guide de configuration rapide a pour but de vous aider à mettre en route chaque module le plus simplement et rapidement possible. Pour afficher des informations complémentaires, sélectionnez le module qui vous intéresse et cliquez sur le bouton **?** ou Aide situé dans l'angle supérieur droit de la fenêtre. Les rubriques d'aide correspondant à la fenêtre affichée s'afficheront automatiquement.

Mise en route

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

Pour faire en sorte que HP Client Security ne requière qu'une seule authentification au cours de la session Windows, reportez-vous à la section Fonctions de sécurité à la page 29.

Password Manager

Nous avons tous un certain nombre de mots de passe, en particulier en cas d'accès régulier à des sites Web ou d'utilisation courante d'applications nécessitant une authentification. L'utilisateur standard soit utilise le même mot de passe pour tous les sites Web et applications, soit fait preuve de créativité et oublie très vite quel mot de passe correspond à quelle application.

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

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

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

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

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

Affichage et gestion des authentifications enregistrées dans Password Manager

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

Pour ouvrir le Gestionnaire de mots de passe, utilisez la combinaison de touches Ctrl+touche Windows+h pour ouvrir le Gestionnaire de mots de passe, puis cliquez sur **Se connecter** pour lancer et authentifier le raccourci enregistré.

L'option **Modifier** du Gestionnaire de mots de passe vous permet d'afficher et de modifier le nom et le nom d'utilisateur, et même de visualiser les mots de passe.

HP Client Security pour les PME permet de sauvegarder et/ou de copier toutes les informations d'authentification sur un autre ordinateur.

HP Device Access Manager

Device Access Manager vous permet de restreindre l'utilisation de divers périphériques de stockage internes et externes afin que vos données restent sécurisées sur le disque dur et ne sortent pas de votre entreprise. Vous pouvez par exemple permettre à un utilisateur d'accéder à vos données mais l'empêcher de les copier sur un CD, un lecteur de musique personnel ou un périphérique mémoire USB.

1. Ouvrez **Device Access Manager** (reportez-vous à la section Ouverture de Device Access Manager à la page 47).

   L'accès pour l'utilisateur actuel est affiché.

2. Pour modifier l'accès des utilisateurs, des groupes ou des périphériques, cliquez ou tapez sur **Modifier**. Pour plus d'informations, reportez-vous à la section Vue système à la page 47.

HP Drive Encryption

HP Drive Encryption vous permet de protéger vos données en cryptant l'intégralité du disque dur. Les données présentes sur votre disque dur seront protégées en cas de vol de votre PC et/ou de retrait du disque dur de l'ordinateur d'origine pour l'installer sur un autre ordinateur.

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

Pour vous simplifier la tâche, plusieurs modules logiciels synchronisent automatiquement les mots de passe, y compris les comptes utilisateur Windows, les domaines d'authentification, HP Drive Encryption, le Gestionnaire de mots de passe et HP Client Security.

Pour configurer HP Drive Encryption lors de la configuration initiale avec l'assistant de configuration HP Client Security, reportez-vous à la section Mise en route à la page 9.

4 HP Client Security

La page d'accueil de HP Client Security est l'emplacement central qui permet d'accéder aisément aux fonctionnalités, applications et paramètres de HP Client Security. La page d'accueil est divisée en trois sections :

- **DONNÉES** — Permet d'accéder à des applications de gestion portant sur la sécurité des données.
- **PÉRIPHÉRIQUE** — Permet d'accéder à des applications de gestion portant sur la sécurité des périphériques.
- **IDENTITÉ** — Permet l'inscription et la gestion des informations d'authentification.

Déplacez le curseur sur la vignette d'une application pour afficher la description de cette application.

Il se peut que HP Client Security indique au bas d'une page des liens vers des paramètres d'utilisateur et d'administration. HP Client Security permet d'accéder aux fonctions et Paramètres avancés en tapant ou en cliquant sur l'icône d'**Engrenage** (paramètres).

Fonctions, applications et paramètres d'identité

Les fonctions, applications et paramètres d'identité fournis par HP Client Security vous aident à gérer divers aspects de votre identité numérique. Cliquez ou tapez sur l'une des vignettes suivantes sur la page d'accueil de HP Client Security, puis saisissez votre mot de passe Windows :

- **Empreintes digitales** — Inscrit et gère vos empreintes digitales à des fins d'authentification.
- **SpareKey** — Configure et gère vos informations d'authentification HP SpareKey, qui peuvent servir à vous connecter à votre ordinateur en cas de perte des autres informations d'authentification. Vous pouvez également réinitialiser votre mot de passe oublié.
- **Mot de passe Windows** — Permet de modifier facilement votre mot de passe Windows.
- **Périphériques Bluetooth** — Permet d'inscrire et gérer vos périphériques Bluetooth.
- **Cartes** — Permet d'inscrire et gérer vos cartes à puce, vos cartes sans contact et vos cartes de proximité.
- **PIN** — Permet d'inscrire et gérer vos codes PIN d'authentification.
- **RSA SecurID** — Permet d'inscrire et gérer vos informations d'authentification RSA SecurID (dans le cas d'une configuration appropriée).
- **Gestionnaire de mots de passe** — Permet de gérer les mots de passe pour vos comptes et applications en ligne.

Empreintes digitales

L'assistant de configuration de HP Client Security vous guide au cours de l'enregistrement, ou « inscription », de vos empreintes digitales.

Vous pouvez également inscrire ou effacer vos empreintes digitales sur la page Empreintes digitales, à laquelle vous pouvez accéder en cliquant ou en tapant sur l'icône **Empreintes digitales** dans la page d'accueil de HP Client Security.

1. Sur la page Empreintes digitales, faites glisser un de vos doigts jusqu'à ce qu'il soit enregistré avec succès.

   Le nombre de doigts à inscrire est indiqué sur la page. Enregistrez de préférence index et majeur.

2. Pour effacer des empreintes digitales déjà inscrites, cliquez ou tapez sur **Supprimer**.
3. Pour enregistrer d'autres doigts, cliquez ou tapez sur **Enroll an additional fingerprint** (Inscrire une autre empreinte digitale).
4. Cliquez ou tapez sur **Enregistrer** avant de quitter la page.

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

- ▲ Pour accéder aux paramètres d'administration des empreintes digitales, servant aux administrateurs à configurer la procédure d'inscription, sa précision et d'autres réglages, cliquez ou tapez sur **Administrative Settings** (Paramètres d'administration ; nécessite des privilèges d'administration).
- ▲ Pour accéder aux paramètres d'utilisateur des empreintes digitales, vous permettant de configurer l'apparence et le comportement de la reconnaissance d'empreintes digitales, cliquez ou tapez sur **Paramètres utilisateur**.

Paramètres d'administration des empreintes digitales

Les administrateurs peuvent configurer la procédure d'inscription, la précision et d'autres réglages d'un lecteur d'empreintes digitales. Des privilèges d'administration sont requis.

- ▲ Pour accéder aux paramètres d'administration de l'authentification par empreinte digitale, cliquez ou tapez sur **Administrative Settings** (Paramètres d'administration) dans la page Empreintes digitales.

- **Inscription d'utilisateur** — Choisissez les nombres minimum et maximum d'empreintes digitales qu'un utilisateur peut inscrire.
- **Reconnaissance** — Déplacez le curseur pour régler la sensibilité du lecteur d'empreintes digitales lorsque vous faites glisser vos doigts.

  Si votre empreinte digitale n'est pas reconnue à chaque passage, vous pouvez sélectionner une sensibilité inférieure. Une valeur plus élevée augmente la sensibilité aux variations lors des passages d'empreintes digitales et réduit par conséquent le risque d'une fausse acceptation. Le paramètre **Moyen-Élevé** offre un bon compromis entre sécurité et commodité.

Paramètres d'utilisateur des empreintes digitales

Sur la page Paramètres d'utilisateur des empreintes digitales, vous pouvez spécifier les paramètres qui régissent l'apparence et le comportement de la reconnaissance d'empreintes digitales.

▲ Pour accéder aux paramètres d'utilisateur de l'authentification par empreinte digitale, cliquez ou tapez sur **Paramètres utilisateur** dans la page Empreintes digitales.

- **Activer le retour audio** — Par défaut, HP Client Security vous donne un retour audio lorsqu'une empreinte digitale a été soumise, en jouant différents sons selon les évènements possibles. Vous pouvez attribuer de nouveaux sons à ces évènements à l'aide de l'onglet Sons de la section Paramètres audio du Panneau de configuration Windows, ou désactiver le retour audio en décochant cette case.
- **Afficher le retour qualité de la lecture** — Pour afficher tous les glissements, sans se soucier de leur qualité, cochez cette case. Pour n'afficher que des glissements de bonne qualité, décochez cette case.

HP SpareKey — Récupération de mot de passe

Une clé HP SpareKey vous permet d'accéder à votre ordinateur (sur les plates-formes prises en charge) en répondant à trois questions de sécurité.

HP Client Security vous invite à configurer votre clé HP SpareKey personnelle lors de la configuration initiale de l'Assistant de configuration de HP Client Security.

Pour configurer votre clé HP SpareKey :

1. Sur la page HP SpareKey de l'assistant, sélectionnez trois questions de sécurité, puis saisissez une réponse pour chacune d'elles.

   Vous pouvez choisir une question dans une liste prédéfinie ou rédiger votre propre question.

2. Cliquez ou tapez sur **Inscrire**.

Pour supprimer votre clé HP SpareKey :

▲ Cliquez ou tapez sur **Supprimer votre SpareKey**.

Une fois la SpareKey configurée, vous pouvez l'utiliser pour accéder à votre ordinateur depuis un écran d'authentification au démarrage ou l'Écran d'accueil de Windows.

Vous pouvez sélectionner des questions différentes ou changer vos réponses sur la page SpareKey, accessible à partir de la vignette de Récupération de mot de passe sur la page d'accueil de HP Client Security.

Pour accéder aux paramètres de HP SpareKey, qu'un administrateur peut utiliser pour configurer l'authentification par clé HP SpareKey, cliquez sur **Paramètres** (nécessite des privilèges d'administration).

Paramètre SpareKey HP

Sur la page Paramètres de HP SpareKey, vous pouvez spécifier les paramètres régissant le comportement et l'utilisation de l'authentification par clé HP SpareKey.

▲ Pour lancer la page Paramètres de HP SpareKey, cliquez ou tapez sur **Paramètres** sur la page HP SpareKey (nécessite des privilèges d'administration).

Les administrateurs peuvent configurer les paramètres suivants :

- Définir les questions présentées à chaque utilisateur lors de la configuration de HP SpareKey.
- Ajouter jusqu'à trois questions de sécurité personnalisées à la liste présentée aux utilisateurs.
- Choisir d'autoriser ou non les utilisateurs à rédiger leurs propres questions de sécurité.
- Préciser quels environnements d'authentification (Windows ou Authentification au démarrage) permettent l'utilisation de HP SpareKey pour la récupération de mot de passe.

Mot de passe Windows

Avec HP Client Security, changer votre mot de passe Windows est plus facile et plus rapide qu'avec le panneau de configuration Windows.

Pour changer votre mot de passe Windows :

1. Sur la page d'accueil de HP Client Security, cliquez ou tapez sur **Mot de passe Windows**.
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 saisissez-le à nouveau dans la zone de texte **Confirmer le nouveau mot de passe**.
4. Cliquez ou tapez sur **Modifier** pour remplacer immédiatement votre mot de passe actuel par celui que vous venez de saisir.

Périphériques Bluetooth

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

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

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

Pour accéder à la page Paramètres des périphériques Bluetooth à la page 17 dans laquelle un administrateur peut définir des paramètres pour les périphériques Bluetooth, cliquez sur **Paramètres** (nécessite des privilèges d'administration).

Paramètres des périphériques Bluetooth

Les administrateurs peuvent spécifier les paramètres suivants qui régissent le comportement et l'utilisation des informations d'authentification des périphériques Bluetooth :

Authentification silencieuse

- **Automatically use your connected enrolled Bluetooth Device during verification of your identity** (Utiliser automatiquement votre périphérique Bluetooth inscrit connecté lors de la vérification de votre identité) — Cochez cette case pour permettre aux utilisateurs d'utiliser les informations d'authentification Bluetooth pour s'identifier sans recourir à une quelconque action, ou bien décochez-la pour désactiver cette option.

Proximité Bluetooth

- **Verrouiller l'ordinateur lorsque votre périphérique Bluetooth inscrit devient hors de portée de votre ordinateur** : cochez cette case pour verrouiller l'ordinateur lorsqu'un périphérique Bluetooth connecté à l'ouverture de session devient hors de portée, ou bien décochez-la pour désactiver cette option.

REMARQUE : Le module Bluetooth de votre ordinateur doit prendre en charge cette fonctionnalité pour pouvoir en profiter.

Cartes

HP Client Security peut prendre en charge de nombreux types différents de cartes d'identification, c'est-à-dire des petites cartes en plastique contenant une puce informatique. Parmi celles-ci figurent des cartes à puce, des cartes sans contact et des cartes de proximité. Si l'une de ces cartes, ainsi que le lecteur de cartes adéquat, est connectée à l'ordinateur, et si l'administrateur a installé le pilote fourni par le fabricant et a autorisé la carte comme méthode d'authentification, vous pouvez utiliser cette carte pour vous identifier.

Dans le cas des cartes à puce, le fabricant doit fournir des outils pour installer un certificat de sécurité et gérer le code PIN que HP Client Security utilise dans son algorithme de sécurité. Le nombre et le type de caractères utilisés pour un code PIN peuvent varier. Un administrateur doit initialiser la carte à puce avant de pouvoir l'utiliser.

Voici les formats de cartes à puce pris en charge par HP Client Security :

- CSP
- PKCS11

Les types de cartes sans contact suivants sont pris en charge par HP Client Security :

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

Voici les types de cartes de proximité pris en charge par HP Client Security :

- cartes de proximité HID

Pour inscrire une carte à puce :

1. Insérez la carte dans un lecteur de carte à puce Smart Card connecté.
2. Une fois la carte reconnue, entrez son code PIN, puis cliquez ou tapez sur **Inscrire**.

Pour modifier le code PIN d'une carte à puce :

1. Insérez la carte dans un lecteur de carte à puce Smart Card connecté.
2. Une fois la carte reconnue, entrez son code PIN, puis cliquez ou tapez sur **Authentifier**.
3. Cliquez ou tapez sur **Changer le PIN**, puis entrez le nouveau code PIN.

Pour inscrire une carte sans contact ou de proximité :

1. Placez la carte sur ou très près du lecteur adéquat.
2. Une fois la carte reconnue, cliquez ou tapez sur **Inscrire**.

Pour supprimer une carte inscrite :

1. Rapprochez la carte du lecteur.
2. S'il s'agit d'une carte à puce, entrez son code PIN, puis cliquez ou tapez sur **Authentifier**.
3. Cliquez ou tapez sur **Supprimer**.

Une fois la carte enregistrée, des informations sur celle-ci sont affichées sous **Cartes inscrites**. Lorsqu'une carte est supprimée, elle est retirée de la liste.

Pour accéder aux paramètres des cartes à puce, de proximité et sans contact, que les administrateurs peuvent utiliser pour configurer les méthodes d'authentification par carte, cliquez ou tapez sur **Paramètres** (nécessite des privilèges d'administration).

Paramètres des cartes à puce, de proximité et sans contact

Pour accéder aux paramètres d'une carte, cliquez ou tapez sur celle-ci dans la liste, puis sur la flèche qui s'affiche.

Pour modifier le code PIN d'une carte à puce :

1. Rapprochez la carte du lecteur
2. Entrez le code PIN de la carte, puis cliquez ou tapez sur **Continuer**.
3. Entrez et confirmez le nouveau code PIN, puis cliquez ou tapez sur **Continuer**.

Pour initialiser le code PIN d'une carte à puce :

1. Rapprochez la carte du lecteur
2. Entrez le code PIN de la carte, puis cliquez ou tapez sur **Continuer**.
3. Entrez et confirmez le nouveau code PIN, puis cliquez ou tapez sur **Continuer**.
4. Cliquez ou tapez sur **Oui** pour confirmer l'initialisation.

Pour effacer les données d'une carte :

1. Rapprochez la carte du lecteur
2. Entrez le code PIN de la carte (uniquement pour les cartes à puce), puis cliquez ou tapez sur **Continuer**.
3. Cliquez ou tapez sur **Oui** pour confirmer la suppression.

PIN

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

Pour définir un nouveau code PIN :

- Entrez le code PIN, saisissez-le à nouveau pour le confirmer, puis cliquez ou tapez sur **Appliquer**.

Pour supprimer un code PIN :

- Cliquez ou tapez sur **Supprimer**, puis sur **Oui** pour confirmer.

Pour accéder aux paramètres PIN, que les administrateurs peuvent utiliser pour configurer les codes PIN servant à s'authentifier, cliquez ou tapez sur **Paramètres** (nécessite des privilèges d'administration).

Paramètres de PIN

Sur la page Paramètres PIN, vous pouvez spécifier les longueurs minimale et maximale autorisées pour un code PIN d'authentification.

RSA SecurID

Si l'administrateur a activé RSA en tant que méthode d'authentification, et que les conditions suivantes sont remplies, vous pouvez inscrire ou supprimer un authentifieur RSA SecurID.

REMARQUE : Une configuration appropriée est nécessaire.

- L'utilisateur doit avoir été créé sur un serveur RSA.
- Les authentifieurs RSA SecurID affectés à l'utilisateur et à l'ordinateur doivent avoir été joints au domaine du serveur RSA.
- Le logiciel SecurID est installé sur l'ordinateur.
- Une connexion au serveur RSA, correctement configuré, est disponible.

Pour inscrire un authentifieur RSA SecurID :

▲ Entrez votre nom d'utilisateur et votre mot de passe RSA SecurID (code de l'authentifieur RSA SecurID ou code PIN + code de l'authentifieur, selon votre environnement), puis cliquez ou tapez sur **Appliquer**.

Après une inscription réussie, un message de confirmation s'affiche et le bouton Supprimer devient actif.

Pour supprimer un authentifieur RSA SecurID :

▲ Cliquez sur **Supprimer**, puis sélectionnez **Oui** dans la boite de dialogue contextuelle demandant une confirmation de la suppression.

Gestionnaire de mots de passe

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

REMARQUE : En raison de la structure en constante évolution des écrans de connexion des sites Web, le Gestionnaire de mots de passe risque de ne pas pouvoir prendre en charge tous les sites à tout moment.

Le Gestionnaire de mots de passe offre les options suivantes :

Page du Gestionnaire de mots de passe

- Cliquez ou tapez sur un compte pour lancer automatiquement une page Web ou une application et vous connecter.
- Utilisez des catégories pour organiser vos comptes.

Sécurité du mot de passe

- Déterminer instantanément si certains de vos mots de passe présentent un risque de sécurité.
- Lorsque vous ajoutez des données de connexion, vérifiez la robustesse des différents mots de passe utilisés pour les sites web et les applications.
- La force des mots de passe est illustrée par des indicateurs d'état rouge, jaune et vert.

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

▲ Cliquez ou tapez sur l'icône du **Gestionnaire de mots de passe** pour afficher un menu contextuel proposant les options suivantes :

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

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

Les options suivantes s'affichent dans le menu contextuel :

- **Ajouter [undomaine.com] au Gestionnaire de mots de passe** : vous permet d'ajouter une connexion à l'écran de connexion actuel.
- **Ouvrir le Gestionnaire de mots de passe** : lance le Gestionnaire de mots de passe.
- **Paramètres de l'icône** — Permet d'indiquer les conditions d'affichage de l'icône du **Gestionnaire de mots de passe**.
- **Aide** — Affiche l'aide logicielle de HP Client Security.

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

Les options suivantes s'affichent dans le menu contextuel :

- **Remplir les données de connexion** — Affiche la page **Vérifiez votre identité**. Si l'authentification aboutit, vos données de connexion sont placées dans les champs de connexion, puis la page est envoyée (si l'envoi a été spécifié lors de la création de la connexion ou de sa dernière modification).
- **Modifier la connexion** — Permet de modifier vos données de connexion pour ce site Web.
- **Ajouter une connexion** — Vous permet d'ajouter un compte à Password Manager (Gestionnaire de mots de passe).
- **Ouvrir le Gestionnaire de mots de passe** — Lance le Gestionnaire de mots de passe.
- **Aide** — Affiche l'aide logicielle de HP Client Security.

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

Ajout de connexions

Vous pouvez ajouter aisément une connexion à un site Web ou un programme en saisissant une seule fois les informations de connexion. Par la suite, le Gestionnaire de mots de passe entre

automatiquement ces informations à votre place. Vous pouvez utiliser ces connexions après avoir navigué sur le site ou programme.

Pour ajouter une connexion :

1. Ouvrez l'écran de connexion d'un site Web ou d'un programme.
2. Cliquez ou tapez sur l'icône du **Gestionnaire de mots de passe**, puis sur l'une des options suivantes, en fonction de l'écran de connexion affiché (site Web ou programme) :
   - Dans le cas d'un site Web, cliquez ou tapez sur **Ajouter [nom de domaine] au Gestionnaire de mots de passe**.
   - Dans le cas d'un programme, cliquez ou tapez sur **Ajouter cet écran de connexion au Gestionnaire de mots de passe**.
3. Saisissez vos données de connexion. Les champs de connexion à l'écran et leurs champs correspondant dans la boite de dialogue, sont identifiés par un liseré orange en gras.
   a. Pour remplir un champ de connexion avec l'un des choix préformatés, cliquez ou tapez sur les flèches à droite du champ.
   b. Pour consulter le mot de passe de cette connexion, cliquez ou tapez sur **Afficher le mot de passe**.
   c. Pour que les données des champs de connexion soient fournies sans être envoyées, désactivez la case à cocher **Envoyer automatiquement les données de connexion**.
   d. Cliquez ou tapez sur **OK** pour sélectionner la méthode d'authentification à utiliser (empreintes digitales, carte à puce, carte de proximité, carte sans contact, téléphone Bluetooth, code PIN ou mot de passe), puis connectez-vous à l'aide de la méthode choisie.

      Le signe plus est retiré de l'icône **Gestionnaire de mots de passe** afin de vous indiquer que la connexion a été créée.
   e. Si le Gestionnaire de mots de passe ne détecte pas les champs de connexion, cliquez ou tapez sur **Plus de champs**.
      - Cochez la case de chaque champ requis pour la connexion ou effacez la case des champs qui ne sont pas requis pour la connexion.
      - Cliquez ou tapez sur **Fermer**.

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

Modification des connexions

Pour modifier une connexion :

1. Ouvrez l'écran de connexion d'un site Web ou d'un programme.
2. Pour afficher une boite de dialogue dans laquelle vous pouvez modifier vos informations de connexion, cliquez ou tapez sur l'icône du **Gestionnaire de mots de passe**, puis sur **Modifier une connexion**.

   Les champs de connexion à l'écran et leurs champs correspondant dans la boite de dialogue, sont identifiés par un liseré orange en gras.

   Vous pouvez également modifier les informations du compte depuis la page du Gestionnaire de mots de passe, en cliquant ou tapant sur la connexion pour afficher les options de modification, puis en sélectionnant **Modifier**.
3. Modifier vos informations de connexion.
   - Pour changer le **Nom du compte**, saisissez un nouveau nom dans le champ correspondant.
   - Pour ajouter ou modifier le nom d'une **Catégorie**, saisissez un nouveau nom dans le champ **Catégorie**.
   - Pour sélectionner un champ **Nom d'utilisateur** avec l'un des choix préformatés, cliquez ou tapez sur la flèche descendante à droite du champ.

     Les choix préformatés ne sont disponibles que lorsque vous modifiez la connexion à partir de la commande Modifier située dans le menu contextuel de l'icône du Gestionnaire de mots de passe.
   - Pour sélectionner un champ **Mot de passe** avec l'un des choix préformatés, cliquez ou tapez sur la flèche descendante à droite du champ.

     Les choix préformatés ne sont disponibles que lorsque vous modifiez la connexion à partir de la commande Modifier située dans le menu contextuel de l'icône du Gestionnaire de mots de passe.
   - Pour ajouter d'autres champs de l'écran à votre connexion, cliquez ou tapez sur **Plus de champs**.
   - Pour consulter le mot de passe de cette connexion, cliquez ou tapez sur l'icône **Afficher le mot de passe**.
   - Pour que les données des champs de connexion soient fournies sans être envoyées, désactivez la case à cocher **Envoyer automatiquement les données de connexion**.
   - Pour signaler que cette connexion possède un mot de passe compromis, cochez la case **This password is compromised** (Ce mot de passe est compromis).

     Une fois les modifications enregistrées, toutes les autres connexions partageant le même mot de passe seront également marquées comme compromises. Vous pouvez ensuite consulter chaque compte touché et changer les mots de passe à votre convenance.
4. Cliquez ou tapez sur **OK**.

Utilisation du menu Liens rapides du Gestionnaire de mots de passe

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 ou double-tapez sur une connexion à un programme ou site Web dans le menu **Liens rapides du Gestionnaire de mots de**

passe, ou depuis la page du Gestionnaire de mots de passe dans HP Client Security, pour ouvrir l'écran d'ouverture de session, puis renseignez vos données de connexion.

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

Pour afficher le menu **Liens rapides** :

- ▲ Appuyez sur la combinaison de touches d'activation du **Gestionnaire de mots de passe** (Ctrl +touche Windows+h est le paramètre défini en usine). Pour modifier cette combinaison de touches, cliquez ou tapez sur **Gestionnaire de mots de passe** dans la page d'accueil de HP Client Security, puis sur **Paramètres**.

Organisation des connexions en catégories

Créez une ou plusieurs catégories afin d'organiser vos connexions.

Pour affecter une connexion à une catégorie :

1. Sur la page d'accueil de HP Client Security, cliquez ou tapez sur **Gestionnaire de mots de passe**.
2. Cliquez ou tapez sur un compte, puis sur **Modifier**.
3. Dans le champ **Catégorie**, entrez un nom de catégorie.
4. Cliquez ou tapez sur **Enregistrer**.

Pour supprimer un compte d'une catégorie :

1. Sur la page d'accueil de HP Client Security, cliquez ou tapez sur **Gestionnaire de mots de passe**.
2. Cliquez ou tapez sur un compte, puis sur **Modifier**.
3. Dans le champ **Catégorie**, effacez un nom de catégorie.
4. Cliquez ou tapez sur **Enregistrer**.

Pour renommer une catégorie :

1. Sur la page d'accueil de HP Client Security, cliquez ou tapez sur **Gestionnaire de mots de passe**.
2. Cliquez ou tapez sur un compte, puis sur **Modifier**.
3. Dans le champ **Catégorie**, modifiez le nom de catégorie.
4. Cliquez ou tapez sur **Enregistrer**.

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 sur la page du Gestionnaire de mots de passe.

Pour gérer vos connexions :

1. Sur la page d'accueil de HP Client Security, cliquez ou tapez sur **Gestionnaire de mots de passe**.
2. Cliquez ou tapez sur une connexion existante, sélectionnez l'une des options suivantes, puis suivez les instructions à l'écran :
   - **Modifier** : permet de modifier une connexion. Pour plus d'informations, reportez-vous à la section Modification des connexions à la page 23.
   - **Se connecter** — Connectez-vous au compte sélectionné.
   - **Supprimer** — Supprimer la connexion pour le compte sélectionné.

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

1. Ouvrez l'écran d'ouverture de session du site Web ou du programme.
2. Cliquez ou tapez sur l'icône du **Gestionnaire de mots de passe** pour afficher son menu contextuel.
3. Cliquez ou tapez sur **Ajouter une connexion**, puis suivez les instructions à l'écran.

Évaluation de la force de votre mot de passe

L'utilisation de mots de passe robustes 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 robustesse de chaque mot de passe utilisé pour vous connecter à des sites Web ou programmes.

Au moment de saisir un mot de passe lors de la création pour un compte d'une connexion du Gestionnaire de mots de passe, une barre de couleur s'affiche sous le mot de passe pour indiquer sa robustesse. Les couleurs correspondent aux valeurs suivantes :

- **Rouge** — Faible
- **Jaune** — Suffisant
- **Vert** — Robuste

Paramètres de l'icône du Gestionnaire de mots de passe

Le Gestionnaire de mots de passe tente d'identifier les écrans d'ouverture de session des sites Web et des 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 un signe plus dans l'icône **Gestionnaire de mots de passe**.

1. Cliquez ou tapez sur l'icône, puis sur **Paramètres de l'icône** pour personnaliser la manière dont le Gestionnaire de mots de passe va traiter les sites pour lesquels une connexion est possible.
   - **Inviter à ajouter des connexions aux écrans de connexion** : Cliquez ou tapez sur cette option pour que le Gestionnaire de mots de passe vous invite à ajouter une connexion lorsqu'un écran de connexion qui n'a pas encore été configuré est affiché.
   - **Exclure cet écran** : sélectionnez la case à cocher afin que le Gestionnaire de mots de passe ne vous invite plus à ajouter une connexion à cet écran de connexion.
   - **Ne pas inviter à ajouter des connexions pour les écrans de connexion** : sélectionnez cette case d'option.
2. Pour ajouter une connexion à un écran qui a été précédemment exclu :
   a. Connectez-vous au site Web précédemment exclu.
   b. Pour que le Gestionnaire de mots de passe conserve le mot de passe de ce site, cliquez ou tapez sur **Se rappeler** dans la boîte de dialogue contextuelle afin d'enregistrer le mot de passe et créer une connexion pour cet écran.
3. Pour accéder à d'autres paramètres du Gestionnaire de mots de passe, cliquez ou tapez sur l'icône du Gestionnaire de mots de passe, puis sur **Ouvrir le Gestionnaire de mots de passe**, et enfin sur **Paramètres** dans la page du Gestionnaire de mots de passe.

Importation et exportation de connexions

Sur la page Importer et exporter du Gestionnaire de mots de passe de HP, vous pouvez importer des connexions enregistrées par des navigateurs Web sur votre ordinateur. Vous pouvez également importer des données depuis un fichier de sauvegarde de HP Client Security et exporter des données vers un fichier de sauvegarde de HP Client Security.

▲ Pour ouvrir la page Importer et exporter, cliquez ou tapez sur **Importer et exporter** dans la page du Gestionnaire de mots de passe.

Pour importer des mots de passe depuis un navigateur :

1. Cliquez ou tapez sur le navigateur à partir duquel vous souhaitez importer des mots de passe (seuls les navigateurs installés sont affichés).
2. Décochez les cases des comptes pour lesquels vous ne souhaitez pas importer de mots de passe.
3. Cliquez ou tapez sur **Importer**.

L'importation ou l'exportation de données depuis/vers un fichier de sauvegarde de HP Client Security peut être réalisée en suivant les liens associés (sous **Autres Options**) dans la page Importer et exporter.

REMARQUE : Cette fonctionnalité ne permet d'importer ou exporter que les données du Gestionnaire de mots de passe. Pour en savoir plus sur la sauvegarde et la restauration des autres données de HP Client Security, reportez-vous à la section Sauvegarde et restauration de vos données à la page 31.

Pour importer des données depuis un fichier de sauvegarde de HP Client Security :

1. Sur la page Importer et exporter du Gestionnaire de mots de passe, cliquez ou tapez sur **Import data from an HP Client Security backup file** (Importer des données à partir d'un fichier de sauvegarde de HP Client Security).
2. Vérifiez votre identité.
3. Sélectionnez le fichier de sauvegarde créé précédemment ou saisissez le chemin d'accès dans le champ prévu à cet effet, puis cliquez ou tapez sur **Parcourir**.
4. Entrez le mot de passe protégeant le fichier, puis cliquez ou tapez sur **Suivant**.
5. Cliquez ou tapez sur **Restaurer**.

Pour exporter des données vers un fichier de sauvegarde de HP Client Security :

1. Sur la page Importer et exporter du Gestionnaire de mots de passe, cliquez ou tapez sur **Export data to an HP Client Security backup file** (Exporter des données vers un fichier de sauvegarde de HP Client Security).
2. Vérifiez votre identité, puis cliquez ou tapez sur **Suivant**.
3. Donnez un nom au fichier de sauvegarde. Par défaut, le fichier est enregistré dans le dossier Documents. Pour spécifier un emplacement différent, cliquez ou tapez sur **Parcourir**.
4. Entrez un mot de passe pour protéger le fichier et confirmez-le, puis cliquez ou tapez sur **Sauvegarder**.

Paramètres

Vous pouvez définir des paramètres permettant de personnaliser le Gestionnaire de mots de passe :

- **Inviter à ajouter des connexions aux écrans de connexion** — Un signe plus apparait sur l'icône du **Gestionnaire de mots de passe** dès qu'un écran de connexion à un site Web ou à un programme est détecté. Cela indique que vous pouvez ajouter une connexion pour cet écran au menu **Connexions**.

  Pour désactiver cette fonction, décochez la case **Inviter à ajouter des connexions aux écrans de connexion**.

- **Ouvrir le Gestionnaire de mots de passe avec Ctrl+Win+h** : la combinaison de touches d'activation par défaut qui ouvre le menu **Liens rapides du Gestionnaire de mots de passe** est Ctrl+touche Windows+h.

  Pour changer cette combinaison, cliquez ou tapez 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.

  Les combinaisons réservées à Windows ou à ses applications ne peuvent pas être employées.

- Pour rétablir les paramètres à leurs valeurs par défaut, cliquez ou tapez sur **Restaurer les valeurs par défaut**.

Paramètres avancés

Les administrateurs peuvent accéder aux options suivantes en sélectionnant l'icône d'**Engrenage** (paramètres) située dans la page d'accueil de HP Client Security.

- **Administrator Policies** (Règles d'administrateur) — Permet de configurer les règles de session et de connexion des administrateurs.
- **Standard User Policies** (Règles d'utilisateur standard) — Permet de configurer les règles de session et de connexion des utilisateurs standards.
- **Fonctions de sécurité** — Permet d'accroitre la sécurité de votre ordinateur en protégeant votre compte Windows à l'aide d'une authentification forte et/ou en activant l'authentification avant le démarrage de Windows.
- **Utilisateurs** — Permet de gérer les utilisateurs et leurs informations d'authentification.
- **Mes règles** — Permet de consulter vos règles d'authentification et l'état de votre inscription.
- **Sauvegarder et restaurer** — Permet de sauvegarder ou de restaurer des données de HP Client Security.
- **À propos de HP Client Security** — Affiche des informations sur la version de HP Client Security.

Règles d'administrateur

Vous pouvez configurer les règles de connexion et d'ouverture de session pour les administrateurs de cet ordinateur. Les règles de connexion définies ici régissent les informations d'identification qu'un administrateur local doit fournir pour se connecter à Windows. Les règles de session définies ici régissent les informations d'identification qu'un administrateur local doit fournir pour vérifier son identité au cours d'une session Windows.

Par défaut, toutes les règles nouvellement créées ou modifiées sont immédiatement mises en application après avoir tapé ou cliqué sur **Appliquer**.

Pour ajouter une nouvelle règle :

1. Sur la page d'accueil de HP Client Security, cliquez ou tapez sur l'icône d'**Engrenage**.
2. Sur la page Paramètres avancés, cliquez ou tapez sur **Administrator Policies** (Règles d'administrateur).
3. Cliquez ou tapez sur **Ajouter une nouvelle règle**.
4. Cliquez sur les flèches descendantes pour sélectionner les informations d'authentification principales et secondaires (facultatives) pour la nouvelle règle, puis cliquez ou tapez sur **Ajouter**.
5. Cliquez sur **Appliquer**.

Pour retarder l'application d'une règle nouvellement créée ou modifiée :

1. Cliquez ou tapez sur **Enforce this policy immediately** (Appliquer immédiatement cette règle).
2. Sélectionnez **Enforce this policy on the specific date** (Appliquer cette règle à la date indiquée).
3. Entrez une date ou servez-vous du calendrier contextuel pour sélectionner une date de mise en application pour cette règle.

4. Si vous le souhaitez, vous pouvez choisir quand envoyer aux utilisateurs un rappel au sujet de la nouvelle règle.
5. Cliquez sur **Appliquer**.

Règles d'utilisateur standard

Vous pouvez configurer les règles de connexion et d'ouverture de session pour les utilisateurs standards de cet ordinateur. Les règles de connexion définies ici régissent les informations d'identification qu'un utilisateur standard doit fournir pour se connecter à Windows. Les règles de session définies ici régissent les informations d'identification qu'un utilisateur standard doit fournir pour vérifier son identité au cours d'une session Windows.

Par défaut, toutes les règles nouvellement créées ou modifiées sont immédiatement mises en application après avoir tapé ou cliqué sur **Appliquer**.

Pour ajouter une nouvelle règle :

1. Sur la page d'accueil de HP Client Security, cliquez ou tapez sur l'icône d'**Engrenage**.
2. Sur la page Paramètres avancés, cliquez ou tapez sur **Standard user Policies** (Règles d'utilisateur standard).
3. Cliquez ou tapez sur **Ajouter une nouvelle règle**.
4. Cliquez sur les flèches descendantes pour sélectionner les informations d'authentification principales et secondaires (facultatives) pour la nouvelle règle, puis cliquez ou tapez sur **Ajouter**.
5. Cliquez sur **Appliquer**.

Pour retarder l'application d'une règle nouvellement créée ou modifiée :

1. Cliquez ou tapez sur **Enforce this policy immediately** (Appliquer immédiatement cette règle).
2. Sélectionnez **Enforce this policy on the specific date** (Appliquer cette règle à la date indiquée).
3. Entrez une date ou servez-vous du calendrier contextuel pour sélectionner une date de mise en application pour cette règle.
4. Si vous le souhaitez, vous pouvez choisir quand envoyer aux utilisateurs un rappel au sujet de la nouvelle règle.
5. Cliquez sur **Appliquer**.

Fonctions de sécurité

Vous pouvez activer les fonctions de sécurité de HP Client Security conçues pour empêcher tout accès non autorisé à l'ordinateur.

Pour configurer les fonctions de sécurité :

1. Sur la page d'accueil de HP Client Security, cliquez ou tapez sur l'icône d'**Engrenage**.
2. Sur la page Paramètres avancés, cliquez ou tapez sur **Fonctions de sécurité**.

3. Activez les fonctions de sécurité en sélectionnant les cases à cocher adéquates, puis cliquez ou tapez sur **Appliquer**. Plus vous sélectionnez de fonctions, plus votre ordinateur sera sécurisé.

   Ces paramètres s'appliquent à tous les utilisateurs.

   - **Sécurité de la connexion Windows** — Protège vos comptes Windows en rendant obligatoire la saisie des informations d'authentification de HP Client Security avant d'autoriser l'accès.
   - **Sécurité de préamorçage (authentification à la mise sous tension)** — Protège votre ordinateur avant le démarrage de Windows. Cette option n'est pas disponible si le BIOS ne la prend pas en charge.
   - **Autoriser la connexion directe** — Ce paramètre permet de sauter l'étape de connexion à Windows si l'authentification a déjà été effectuée au niveau de Drive Encryption ou de l'Authentification à la mise sous tension.

4. Cliquez ou tapez sur **Utilisateurs**, puis sur la vignette de l'utilisateur.

Utilisateurs

Vous pouvez contrôler et gérer les utilisateurs de HP Client Security de cet ordinateur.

Pour ajouter un autre utilisateur Windows à HP Client Security :

1. Sur la page d'accueil de HP Client Security, cliquez ou tapez sur l'icône d'**Engrenage**.
2. Sur la page Paramètres avancés, cliquez ou tapez sur **Utilisateurs**.
3. Cliquez ou tapez sur **Add another Windows user to HP Client Security** (Ajouter un autre utilisateur Windows à HP Client Security).
4. Entrez le nom de l'utilisateur que vous souhaitez ajouter, puis cliquez ou tapez sur **OK**.
5. Entrez le mot de passe Windows de l'utilisateur.

   Une vignette correspondant à l'utilisateur ajouté s'affiche sur la page Utilisateur.

Pour supprimer un utilisateur Windows de HP Client Security :

1. Sur la page d'accueil de HP Client Security, cliquez ou tapez sur l'icône d'**Engrenage**.
2. Sur la page Paramètres avancés, cliquez ou tapez sur **Utilisateurs**.
3. Cliquez ou tapez sur le nom de l'utilisateur que vous souhaitez supprimer.
4. Cliquez ou tapez sur **Supprimer l'utilisateur**, puis sur **Oui** pour confirmer.

Pour afficher un récapitulatif des règles de session et de connexion en application pour un utilisateur :

▲ Cliquez ou tapez sur **Utilisateurs**, puis sur la vignette de l'utilisateur.

Mes règles

Vous pouvez afficher vos règles d'authentification et le statut de votre inscription. La page Mes règles contient également des liens vers les pages Règles d'administrateur et Règles d'utilisateur standard.

1. Sur la page d'accueil de HP Client Security, cliquez ou tapez sur l'icône d'**Engrenage**.
2. Sur la page Paramètres avancés, cliquez ou tapez sur **Mes règles**.

   Les règles de session et de connexion qui s'appliquent à l'utilisateur actuellement connecté s'affichent alors.

La page Mes règles contient également des liens vers les sections Règles d'administrateur à la page 28 et Règles d'utilisateur standard à la page 29.

Sauvegarde et restauration de vos données

Il est recommandé de sauvegarder régulièrement vos données de HP Client Security. 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 : Cette fonctionnalité concerne uniquement le Gestionnaire de mots de passe. Drive Encryption possède une méthode de sauvegarde indépendante. Les informations d'authentification par empreinte digitale et à Device Access Manager ne sont pas sauvegardées.

HP Client Security 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 vos données :

1. Sur la page d'accueil de HP Client Security, cliquez ou tapez sur l'icône d'**Engrenage**.
2. Sur la page Paramètres avancés, cliquez ou tapez sur **Administrator Policies** (Règles d'administrateur).
3. Cliquez ou tapez sur **Sauvegarder et restaurer**.
4. Cliquez ou tapez sur **Sauvegarder**, puis vérifiez votre identité.
5. Sélectionnez le module que vous souhaitez inclure dans la sauvegarde, puis cliquez ou tapez sur **Suivant**.
6. Entrez le nom du fichier de stockage. Par défaut, le fichier est enregistré dans le dossier Documents. Pour spécifier un emplacement différent, cliquez ou tapez sur **Parcourir**.
7. Entrez un mot de passe afin de protéger le fichier, puis confirmez-le.
8. Cliquez ou tapez sur **Enregistrer**.

Pour restaurer les données :

1. Sur la page d'accueil de HP Client Security, cliquez ou tapez sur l'icône d'**Engrenage**.
2. Sur la page Paramètres avancés, cliquez ou tapez sur **Administrator Policies** (Règles d'administrateur).
3. Cliquez ou tapez sur **Sauvegarder et restaurer**.
4. Sélectionnez **Restaurer**, puis vérifiez votre identité.
5. Sélectionnez le fichier de stockage créé. Saisissez le chemin d'accès dans le champ prévu à cet effet. Pour spécifier un emplacement différent, cliquez ou tapez sur **Parcourir**.
6. Entrez le mot de passe protégeant le fichier, puis cliquez ou tapez sur **Suivant**.

7. Sélectionnez les modules pour lesquels vous souhaitez restaurer les données.
8. Cliquez ou tapez sur **Restaurer**.

5 HP Drive Encryption (certains modèles uniquement)

Drive Encryption offre une protection complète des données sur votre ordinateur en les cryptant. Lorsque vous activez Drive Encryption, vous devez vous connecter depuis l'écran de connexion de Drive Encryption, qui s'affiche avant le démarrage du système d'exploitation Windows®.

L'écran d'accueil de HP Client Security permet aux administrateurs Windows d'activer Drive Encryption, de sauvegarder la clé de cryptage et de sélectionner ou désélectionner une ou plusieurs unités ou partitions en vue du cryptage. Pour plus d'informations, reportez-vous à l'aide du logiciel HP Client Security.

Les tâches suivantes peuvent être effectuées avec Drive Encryption :

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

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

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

Ouverture de Drive Encryption

Les administrateurs peuvent accéder à Drive Encryption en ouvrant HP Client Security :

1. Dans le menu Démarrer, cliquez ou toquez sur l'application **HP Client Security** (Windows 8).

   - ou -

   Sur le bureau Windows, double-cliquez ou double-tapez sur l'icône **HP Client Security** dans la zone de notification, située tout à droite de la barre des tâches.

2. Cliquez ou tapez sur l'icône de **Drive Encryption**.

Tâches générales

Activation de Drive Encryption pour les disques durs standard

Les disques durs standard sont cryptés à l'aide du cryptage logiciel. Suivez ces étapes pour crypter un disque ou une partition de disque :

1. Lancez **Drive Encryption**. Pour plus d'informations, reportez-vous à la section Ouverture de Drive Encryption à la page 33.
2. Cochez la case correspondant à l'unité ou partition que vous souhaitez crypter, puis cliquez ou tapez sur **Clé de sauvegarde**.

REMARQUE : Pour une sécurité renforcée, cochez la case **Désactiver le mode Veille pour une sécurité accrue**. Lorsque vous désactivez le mode veille, il n'y a absolument aucun risque que les informations d'authentification utilisées pour déverrouiller le disque soient stockées en mémoire.

3. Sélectionnez une ou plusieurs des options de sauvegarde, puis cliquez ou tapez sur **Sauvegarder**. Pour plus d'informations, reportez-vous à la section Sauvegarde des clés de cryptage à la page 37.
4. Vous pouvez continuer à travailler pendant la sauvegarde de la clé de cryptage. Ne redémarrez pas votre ordinateur.

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

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

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

Activation de Drive Encryption pour les unités auto-cryptées

Les unités à cryptage automatique conformes aux spécifications OPAL du Trusted Computing Group relatives à la gestion des unités à cryptage automatique peuvent être cryptées à l'aide d'un cryptage logiciel ou matériel. Le cryptage matériel est beaucoup plus rapide que le cryptage logiciel. Cependant, vous ne pouvez pas choisir parmi les partitions à crypter. Le disque entier, incluant toutes les partitions du disque, est crypté.

Pour crypter certaines partitions en particulier, vous devez utiliser le cryptage logiciel. Veillez alors à décocher la case **Autoriser uniquement le cryptage matériel pour les unités autocryptées (SED)**.

Procédez comme suit afin d'activer Drive Encryption pour les unités à cryptage automatique :

1. Lancez **Drive Encryption**. Pour plus d'informations, reportez-vous à la section Ouverture de Drive Encryption à la page 33.
2. Cochez la case correspondant à l'unité que vous souhaitez crypter, puis cliquez ou tapez sur **Clé de sauvegarde**.

REMARQUE : Pour une sécurité renforcée, cochez la case **Désactiver le mode Veille pour une sécurité accrue**. Lorsque vous désactivez le mode veille, il n'y a absolument aucun risque que les informations d'authentification utilisées pour déverrouiller le disque soient stockées en mémoire.

3. Sélectionnez une ou plusieurs des options de sauvegarde, puis cliquez ou tapez sur **Sauvegarder**. Pour plus d'informations, reportez-vous à la section Sauvegarde des clés de cryptage à la page 37.
4. Vous pouvez continuer à travailler pendant la sauvegarde de la clé de cryptage. Ne redémarrez pas votre ordinateur.

REMARQUE : Dans le cas d'unités autocryptées, vous êtes invité-e à arrêter l'ordinateur.

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

Désactivation de Drive Encryption

1. Lancez **Drive Encryption**. Pour plus d'informations, reportez-vous à la section Ouverture de Drive Encryption à la page 33.
2. Décochez les cases de chaque unité cryptée, puis cliquez ou tapez sur **Appliquer**.

   La désactivation de Drive Encryption commence.

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

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

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

Connexion après l'activation de Drive Encryption

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

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

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

Connexion d'utilisateur unique :

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

Connexion d'utilisateurs multiples :

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

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

Cartes Smart card prises en charge

- Gemalto Cyberflex Access 64k V2c

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

Cryptage de disques durs supplémentaires

Il est fortement conseillé d'utiliser HP Drive Encryption pour protéger vos données en cryptant votre disque dur. Une fois l'activation effectuée, tous les disques durs ou partitions supplémentaires créés peuvent être cryptés en procédant comme suit :

1. Lancez **Drive Encryption**. Pour plus d'informations, reportez-vous à la section Ouverture de Drive Encryption à la page 33.
2. Pour les unités cryptées par cryptage logiciel, sélectionnez les partitions à crypter.

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

- ou -

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

Tâches avancées

Gestion de Drive Encryption (administrateur uniquement)

Les administrateurs peuvent utiliser Drive Encryption pour consulter et modifier l'état de cryptage (Crypté ou Non crypté) de tous les disques durs de l'ordinateur.

- Si l'état est Activé, Drive Encryption a été activé et configuré. L'unité se trouve dans l'un des états suivants :

Cryptage logiciel

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

Cryptage matériel

- Cryptée
- Non crypté (dans le cas d'unités supplémentaires)

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

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

1. Lancez **Drive Encryption**. Pour plus d'informations, reportez-vous à la section Ouverture de Drive Encryption à la page 33.
2. Sous **État d'unité**, cochez ou décochez la case en regard de chaque partition de disque dur à crypter ou à décrypter, puis cliquez ou tapez sur **Appliquer**.

REMARQUE : Lorsqu'une partition est en cours de cryptage ou de décryptage, une barre de progression affiche le pourcentage de partition cryptée.

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

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

Gestion des disques

- **Pseudo** — Vous pouvez nommer vos unités ou partitions pour en faciliter l'identification.
- **Unités déconnectées** — Drive Encryption permet de suivre les disques qui sont retirés de l'ordinateur. Un disque retiré de l'ordinateur est automatiquement transféré vers la liste des unités déconnectées. Si un disque est réintégré au système, il apparaitra à nouveau dans la liste des unités connectées.
- Si vous ne souhaitez plus suivre ou gérer une unité déconnectée, vous pouvez la supprimer de la liste des unités déconnectées.
- Drive Encryption reste activé tant que toutes les cases correspondant aux unités connectées ne sont pas décochées et que la liste des unités déconnectées n'est pas vide.

Sauvegarde et restauration (tâche administrateur)

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

Sauvegarde des clés de cryptage

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

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

1. Lancez **Drive Encryption**. Pour plus d'informations, reportez-vous à la section Ouverture de Drive Encryption à la page 33.
2. Sélectionnez une unité en cochant la case correspondante, puis cliquez ou tapez sur **Clé de sauvegarde**.

3. Sous **Créer une clé de récupération HP Drive Encryption**, sélectionnez une ou plusieurs des options suivantes :

   - **Stockage amovible** — Cochez la case puis sélectionnez le périphérique de stockage sur lequel la clé de cryptage sera sauvegardée.
   - **SkyDrive** — Sélectionnez la case à cocher. Vous devez être connecté-e à Internet. Connectez-vous à Microsoft SkyDrive, puis cliquez ou tapez sur **Oui**.

   REMARQUE : Pour utiliser la clé de sauvegarde HP Drive Encryption stockée sur SkyDrive, vous devez la télécharger depuis SkyDrive sur un périphérique de stockage amovible, puis insérer celui-ci dans cet ordinateur.

   - **TPM** (certains modèles uniquement) — Permet de récupérer vos données à l'aide de votre mot de passe TPM.

   ATTENTION : Si le TPM est effacé ou bien si l'ordinateur est endommagé, vous perdrez l'accès à la sauvegarde. Dans le cas où cette méthode serait retenue, vous devriez également sélectionner une autre méthode de sauvegarde.

4. Cliquez ou tapez sur **Sauvegarder**.

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

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

Les administrateurs peuvent effectuer une récupération à l’aide de la clé Drive Encryption sauvegardée sur un périphérique de stockage amovible lors de l’activation ou en sélectionnant l’option **Clé de sauvegarde** dans Drive Encryption.

1. Insérez le périphérique de stockage amovible contenant la clé de sauvegarde.
2. Mettez l'ordinateur sous tension.
3. Lorsque la boite de dialogue d'ouverture de session de HP Drive Encryption s'affiche, cliquez ou tapez sur **Récupération**.
4. Entrez le nom ou le chemin d’accès du fichier contenant votre clé de sauvegarde, puis cliquez ou tapez sur **Récupération**.
5. Lorsque la boite de dialogue de confirmation s'affiche, cliquez ou tapez sur **OK**.

   L'écran de connexion Windows s'affiche.

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

Récupération de HP SpareKey

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

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

1. Mettez l’ordinateur sous tension.
2. Lorsque la page HP Drive Encryption s’affiche, accédez à la page de connexion d’utilisateur.

3. Cliquez sur **SpareKey**.

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

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

   L'écran de connexion Windows s'affiche.

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

6 Assainisseur de fichiers HP (certains modèles uniquement)

File Sanitizer permet de détruire des ressources en toute sécurité (par exemple : informations ou fichiers personnels, données d'historique ou de site Web ou autres éléments de données) stockées sur le disque dur interne de votre ordinateur et de nettoyer ce dernier de manière périodique.

File Sanitizer ne peut pas être utilisé pour assainir ou nettoyer les types de disques durs suivants :

- Disque SSD, y compris les volumes RAID qui incluent un périphérique SSD.
- Disques externes connectés par USB, Firewire ou interface eSATA.

Si une opération de destruction ou de nettoyage est tentée sur un disque SSD, un message d'avertissement s'affiche et l'opération est annulée.

Destruction

Une destruction diffère d'une suppression Windows® standard. Lorsque vous détruisez une ressource à l'aide de File Sanitizer, les fichiers sont remplacés par des données sans importance, ce qui rend toute récupération des ressources d'origine impossible. Une suppression simple de Windows peut laisser le fichier (ou la ressource) intact sur le disque dur ou dans un état dans lequel des méthodes policières pourraient être utilisées pour le récupérer.

Vous pouvez programmer une destruction à l'avance ou en activer une manuellement en sélectionnant l'icône **File Sanitizer** dans l'écran d'accueil de HP Client Security ou à l'aide de l'icône **File Sanitizer** située sur le bureau Windows. Pour plus d'informations, reportez-vous à la section Définition d'une programmation de destruction à la page 42, Destruction par bouton droit à la page 44 ou Lancement manuel d'une opération de destruction à la page 44.

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

Nettoyage de l'espace libre

Lorsque vous supprimez un élément sous Windows, son contenu n'est pas totalement supprimé du disque dur. Windows supprime uniquement la référence de l'élément ou son emplacement sur le disque dur. Le contenu demeure sur le disque dur jusqu'à ce qu'un autre élément écrase cette même zone et y inscrive de nouvelles données.

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 ne fournit aucune sécurité supplémentaire aux ressources détruites.

Vous pouvez programmer un nettoyage de l'espace libre à l'avance ou en activer un manuellement en sélectionnant l'icône **File Sanitizer** dans l'écran d'accueil de HP Client Security ou à l'aide de l'icône **File Sanitizer** située sur le bureau Windows. Pour plus d'informations, reportez-vous à la section Définition d'une programmation de nettoyage de l'espace libre à la page 43, Lancement

manuel du nettoyage de l'espace libre à la page 45 ou Utilisation de l'icône File Sanitizer à la page 44.

Ouverture de l'Assainisseur de fichiers

1. Dans le menu Démarrer, cliquez ou toquez sur l'application **HP Client Security** (Windows 8).

   - ou -

   Sur le bureau Windows, double-cliquez ou double-tapez sur l'icône **HP Client Security** dans la zone de notification, située tout à droite de la barre des tâches.

2. Sous **Données**, cliquez ou tapez sur **File Sanitizer**.

- ou -

▲ Double-cliquez ou double-tapez sur l'icône **File Sanitizer** située sur le bureau Windows.

–ou–

▲ Faites un clic droit ou maintenez votre doigt appuyé sur l'icône **File Sanitizer** située sur le bureau Windows, puis sélectionnez **Ouvrir File Sanitizer**.

Procédures de configuration

Destruction : File Sanitizer supprime ou détruit de manière sécurisée les catégories de ressources sélectionnées.

1. Sous **Destruction**, cochez chacune des cases correspondant aux types de fichiers à détruire, ou décochez celles des fichiers que vous ne voulez pas éliminer.

   - **Corbeille** : détruit tous les éléments se trouvant dans la corbeille.
   - **Fichiers système temporaires** : détruit tous les fichiers se trouvant dans le dossier des fichiers système temporaires. Les variables d'environnement suivantes sont recherchées dans l'ordre suivant et le premier chemin découvert est considéré comme le dossier système :
     - TMP
     - TEMP
   - **Fichiers Internet temporaires** : détruit les copies de pages Web, les images, et les supports enregistrés par les navigateurs Web pour permettre un affichage plus rapide.
   - **Cookies** : détruit tous les fichiers stockés sur l'ordinateur par des sites Web permettant d'enregistrer des préférences, telles que des informations de connexion.

2. Pour lancer la destruction, cliquez ou tapez sur **Détruire**.

Nettoyage : écrit des données aléatoires sur l'espace libre et empêche la récupération des éléments supprimés.

▲ Pour lancer le nettoyage, cliquez ou tapez sur **Nettoyer**.

Options de File Sanitizer : cochez les cases appropriées pour activer les options suivantes ou décochez celles correspondant aux options que vous souhaitez désactiver :

- **Activer l'icône du bureau** — Affiche l'icône File Sanitizer sur le bureau Windows.
- **Activer le clic droit** — Vous permet, en faisant un clic droit ou en maintenant le doigt appuyé sur une ressource, de sélectionner **HP File Sanitizer – Détruire**.

- **Demander le mot de passe Windows avant une destruction manuelle** — Exige une authentification par mot de passe Windows avant de détruire manuellement un élément.
- **Détruire les cookies et les fichiers Internet temporaires à la fermeture du navigateur** — Détruit toutes les ressources Web sélectionnées, telles que l'historique des URL du navigateur, lorsque vous fermez un navigateur Web.

Définition d'une programmation de destruction

Vous pouvez programmer une destruction automatique à un horaire spécifique, ou également détruire manuellement des ressources à tout moment. Pour plus d'informations, reportez-vous à la section Procédures de configuration à la page 41.

1. Ouvrez File Sanitizer, puis cliquez ou tapez sur **Paramètres**.
2. Pour planifier la destruction de ressources sélectionnées à une date ultérieure, sélectionnez, sous **Programme de destruction**, **Jamais**, **Une fois**, **Tous les jours**, **Toutes les semaines** ou **Tous les mois**, puis choisissez le jour et l'horaire :
   a. Cliquez ou tapez sur le champ heure, minute ou AM/PM.
   b. Faites défiler jusqu'à ce que la valeur désirée s'affiche au même niveau que les autres champs.
   c. Cliquez ou tapez sur l'espace vierge entourant les champs de réglage de l'horaire.
   d. Répétez l'opération pour chaque champ jusqu'à ce que l'horaire adéquat soit sélectionné.
3. Voici les quatre types de ressources répertoriées :
   - **Corbeille** : détruit tous les éléments se trouvant dans la corbeille.
   - **Fichiers système temporaires** : détruit tous les fichiers se trouvant dans le dossier des fichiers système temporaires. Les variables d'environnement suivantes sont recherchées dans l'ordre suivant et le premier chemin découvert est considéré comme le dossier système :
     - TMP
     - TEMP
   - **Fichiers Internet temporaires** : détruit les copies de pages Web, les images, et les supports enregistrés par les navigateurs Web pour permettre un affichage plus rapide.
   - **Cookies** : détruit tous les fichiers stockés sur l'ordinateur par des sites Web permettant d'enregistrer des préférences, telles que des informations de connexion.

   Si ces ressources font partie de la sélection, elles seront détruites à l'horaire programmé.
4. Pour sélectionner d'autres ressources personnalisées à détruire :
   a. Sous **Liste des éléments à destruction programmée**, cliquez ou tapez sur **Ajouter un dossier**, puis accédez au fichier ou au dossier voulu.
   b. Cliquez ou tapez sur **Ouvrir**, puis sur **OK**.

   Pour retirer une ressource de la Liste des éléments à destruction programmée, décochez la case correspondante.

Définition d'une programmation de nettoyage de l'espace libre

Le nettoyage de l'espace libre ne fournit aucune sécurité supplémentaire aux ressources détruites.

1. Ouvrez File Sanitizer, puis cliquez ou tapez sur **Paramètres**.
2. Pour planifier le nettoyage de votre disque dur à une date ultérieure, sélectionnez, sous **Programme de nettoyage**, **Jamais**, **Une fois**, **Tous les jours**, **Toutes les semaines** ou **Tous les mois**, puis choisissez le jour et l'horaire :
   a. Cliquez ou tapez sur le champ heure, minute ou AM/PM.
   b. Faites défiler jusqu'à ce que l'horaire désiré s'affiche au même niveau que les autres champs.
   c. Cliquez ou tapez sur l'espace vierge entourant les champs de réglage de l'horaire.
   d. Répétez l'opération jusqu'à ce que l'horaire adéquat soit sélectionné.

REMARQUE : L'opération de nettoyage de l'espace libre peut prendre beaucoup de temps. Vérifiez que votre ordinateur est connecté à l'alimentation secteur. Bien qu'elle soit effectuée en tâche de fond, l'utilisation accrue du processeur peut affecter les performances de l'ordinateur. Le nettoyage de l'espace libre peut être effectué après les heures de travail ou lorsque l'ordinateur est inutilisé.

Protéger des fichiers d'une destruction

Pour protéger des fichiers ou dossiers d'une destruction :

1. Ouvrez File Sanitizer, puis cliquez ou tapez sur **Paramètres**.
2. Sous **Liste des éléments à ne jamais détruire**, cliquez ou tapez sur **Ajouter un dossier**, puis accédez au fichier ou au dossier voulu.
3. Cliquez ou tapez sur **Ouvrir**, puis sur **OK**.

REMARQUE : Les fichiers de cette liste sont protégés tant qu'ils y restent répertoriés.

Pour retirer une ressource de la liste d'exclusion, décochez la case correspondante.

Tâches générales

Utilisez l'Assainisseur de fichiers pour effectuer les tâches suivantes :

- **Utiliser l'icône File Sanitizer pour démarrer la destruction** : permet de faire glisser des fichiers dans l'icône **File Sanitizer** sur le Bureau Windows. Pour plus d'informations, reportez-vous à la section Utilisation de l'icône File Sanitizer à la page 44.
- **Détruire manuellement une ressource spécifique ou toutes les ressources sélectionnées** : permet de détruire des éléments à tout moment sans attendre l'heure planifiée de la destruction normale. Pour plus d'informations, reportez-vous à la section Destruction par bouton droit à la page 44 ou Lancement manuel d'une opération de destruction à la page 44.
- **Activer manuellement le nettoyage de l'espace libre** : permet d'activer le nettoyage de l'espace libre à tout moment. Pour plus d'informations, reportez-vous à la section Lancement manuel du nettoyage de l'espace libre à la page 45.
- **Afficher les fichiers journaux** : permet d'afficher les fichiers journaux de destruction et de nettoyage de l'espace libre, qui contiennent les erreurs ou défaillances survenues lors de la dernière opération de destruction ou de nettoyage de l'espace libre. Pour plus d'informations, reportez-vous à la section Affichage des fichiers journaux à la page 45.

REMARQUE : Une opération de destruction ou de nettoyage de l'espace libre peut être relativement longue. Bien que la destruction ou le nettoyage de l'espace libre s'exécute en arrière-plan, une utilisation accrue du processeur peut affecter les performances de votre ordinateur.

Utilisation de l'icône File Sanitizer

ATTENTION : Les ressources détruites ne peuvent être récupérées. Examinez attentivement les éléments sélectionnés lors d'une destruction manuelle.

Lorsque vous lancez une opération manuelle de destruction, les ressources de la liste standard d'éléments à détruire affichée dans la vue de File Sanitizer sont détruites (reportez-vous à Procédures de configuration à la page 41).

Vous pouvez démarrer manuellement une opération de destruction de l'une des façons suivantes :

1. Ouvrez File Sanitizer (reportez-vous à la section Ouverture de l'Assainisseur de fichiers à la page 41), puis cliquez ou tapez sur **Détruire**.
2. Lorsque la boite de dialogue de confirmation s'ouvre, assurez-vous que les ressources que vous voulez détruire sont cochées, puis cliquez ou tapez sur **OK**.

–ou–

1. Faites un clic droit ou maintenez votre doigt appuyé sur l'icône **File Sanitizer** située sur le bureau Windows, puis cliquez ou tapez sur **Détruire maintenant**.
2. Lorsque la boite de dialogue de confirmation s'affiche, assurez-vous que les ressources que vous voulez détruire sont cochées, puis cliquez ou tapez sur **Détruire**.

Destruction par bouton droit

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

Si l'option **Activer la destruction par bouton droit** a été sélectionnée dans la vue de File Sanitizer, vous pouvez détruire une ressource de la manière suivante :

1. Accédez au document ou dossier que vous souhaitez détruire.
2. Faites un clic droit ou maintenez votre doigt appuyé sur le fichier/dossier, puis sélectionnez **HP File Sanitizer – Détruire**.

Lancement manuel d'une opération de destruction

ATTENTION : Les ressources détruites ne peuvent être récupérées. Examinez attentivement les éléments sélectionnés lors d'une destruction manuelle.

Lorsque vous lancez une opération manuelle de destruction, les ressources de la liste standard d'éléments à détruire affichée dans la vue de File Sanitizer sont détruites (reportez-vous à Procédures de configuration à la page 41).

Vous pouvez démarrer manuellement une opération de destruction de l'une des façons suivantes :

1. Ouvrez File Sanitizer (reportez-vous à la section Ouverture de l'Assainisseur de fichiers à la page 41), puis cliquez ou tapez sur **Détruire**.
2. Lorsque la boite de dialogue de confirmation s'ouvre, assurez-vous que les ressources que vous voulez détruire sont cochées, puis cliquez ou tapez sur **OK**.

–ou–

1. Faites un clic droit ou maintenez votre doigt appuyé sur l'icône **File Sanitizer** située sur le bureau Windows, puis cliquez ou tapez sur **Détruire maintenant**.
2. Lorsque la boite de dialogue de confirmation s'affiche, assurez-vous que les ressources que vous voulez détruire sont cochées, puis cliquez ou tapez sur **Détruire**.

Lancement manuel du nettoyage de l'espace libre

Lorsque vous lancez une opération manuelle de nettoyage, les ressources de la liste standard d'éléments à détruire affichée dans la vue de File Sanitizer sont détruites (reportez-vous à Procédures de configuration à la page 41).

Vous pouvez démarrer manuellement une opération de nettoyage de l'une des façons suivantes :

1. Ouvrez File Sanitizer (reportez-vous à la section Ouverture de l'Assainisseur de fichiers à la page 41), puis cliquez ou tapez sur **Nettoyer**.
2. Lorsque la boite de dialogue de confirmation s'affiche, cliquez ou tapez sur **OK**.

– ou –

1. Faites un clic droit ou maintenez votre doigt appuyé sur l'icône **File Sanitizer** située sur le bureau Windows, puis cliquez ou tapez sur **Nettoyer maintenant**.
2. Lorsque la boite de dialogue de confirmation s'affiche, cliquez ou tapez sur **Nettoyer**.

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 supprimés ou nettoyés n'apparaissent pas dans les fichiers journaux.

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

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

Pour les systèmes 64 bits, les fichiers journaux se trouvent sur le disque dur dans les dossiers suivants :

- C:\Program Files (x86)\Hewlett-Packard\File Sanitizer*[NomUtilisateur]*_ShredderLog.txt
- C:\Program Files (x86)\Hewlett-Packard\File Sanitizer*[NomUtilisateur]*_DiskBleachLog.txt

7 HP Device Access Manager (certains modèles uniquement)

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

REMARQUE : Certains périphériques de saisie ou d'interface utilisateur comme une souris, un clavier, un pavé tactile ou un lecteur d'empreintes digitales, ne sont pas contrôlés par Device Access Manager. Pour plus d'informations, reportez-vous à la section Classes de périphériques non gérées à la page 50.

Les administrateurs du système d'exploitation Windows® ont recours à HP Device Access Manager pour contrôler l'accès aux périphériques d'un système et 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 ou non autorisés à accéder.
- L'authentification Just In Time permet à des utilisateurs prédéfinis de s'authentifier en vue d'accéder aux périphériques auxquels ils se verraient autrement refuser l'accès.
- Les restrictions d'accès aux périphériques imposées par Device Access Manager peuvent être levées pour les administrateurs et les utilisateurs de confiance en les ajoutant au groupe des Administrateurs de périphériques. L'appartenance à ce groupe est définie dans les Paramètres avancés.
- L'accès aux périphériques peut être octroyé ou refusé sur la base de l'appartenance à un groupe ou sur une base individuelle.
- Pour les classes de périphériques telles que les lecteurs CD-ROM et DVD, l'accès en lecture et en écriture peut être autorisé ou refusé séparément.

HP Device Access Manager est automatiquement configuré avec les paramètres suivants au cours de l'exécution de l'assistant de configuration de HP Client Security :

- Les supports amovibles d'authentification Just-In-Time (JITA) sont activés pour les administrateurs et les utilisateurs.
- La politique relative aux périphériques permet un accès complet à d'autres périphériques.

Ouverture de Device Access Manager

1. Dans le menu Démarrer, cliquez ou toquez sur l'application **HP Client Security** (Windows 8).

   - ou -

   Sur le bureau Windows, double-cliquez ou double-tapez sur l'icône **HP Client Security** dans la zone de notification, située tout à droite de la barre des tâches.

2. Sous **Device** (Périphérique), cliquez ou tapez sur **Device Permissions** (Autorisations d'accès aux périphériques).

   - Les utilisateurs standards peuvent consulter leur accès actuel aux périphériques (reportez-vous à la section Vue utilisateur à la page 47).
   - Les administrateurs peuvent consulter et modifier la configuration actuelle de l'accès aux périphériques sur l'ordinateur en cliquant ou en tapant sur **Modifier**, puis en saisissant le mot de passe administrateur (reportez-vous à Vue système à la page 47).

Vue utilisateur

Lorsque l'option **Device Permissions** (Autorisations d'accès aux périphériques) est sélectionnée, la vue utilisateur s'affiche. Selon la politique, les administrateurs et les utilisateurs standards peuvent consulter leur propre accès à des classes de périphériques ou à des périphériques particuliers sur cet ordinateur.

- **Utilisateur actuel** — Le nom de l'utilisateur actuellement connecté est affiché.
- **Classe de périphérique** — Les types de périphériques sont affichés.
- **Accès** — La configuration actuelle de votre accès à des types de périphériques ou à des périphériques spécifiques est affichée.
- **Durée** — Le délai imparti pour votre accès aux lecteurs de CD/DVD-ROM ou aux lecteurs de disque amovibles est affiché.
- **Paramètres** — Les administrateurs peuvent choisir quels sont les lecteurs dont l'accès doit être contrôlé par Device Access Manager.

Vue système

Dans la vue Système, les administrateurs peuvent autoriser ou refuser l'accès à des périphériques sur cet ordinateur pour le groupe d'utilisateurs ou le groupe d'administrateurs.

▲ Les administrateurs peuvent accéder à la vue système en cliquant ou en tapant sur **Modifier**, en saisissant un mot de passe administrateur, puis en sélectionnant parmi les options suivantes :

- **Device Access Manager** — Pour activer ou désactiver HP Device Access Manager avec l'authentification Just-In-Time, cliquez ou tapez sur **On** (Activé) ou **Off** (Désactivé).
- **Utilisateurs et groupes sur ce PC** — Affiche le groupe d'utilisateurs ou le groupe d'administrateurs auxquels l'accès est autorisé ou refusé pour les classes de périphériques sélectionnées.
- **Classe de périphérique** — Affiche les classes de périphériques et les périphériques installés sur le système ou pouvant l'avoir été auparavant. Pour développer la liste, cliquez sur l'icône **+**. Tous les périphériques connectés à l'ordinateur sont affichés, et les groupes d'administrateurs et

d'utilisateurs sont développés de sorte à en afficher les membres. Pour actualiser la liste des périphériques, cliquez sur l'icône de flèche ronde (actualisation).

- La protection s'applique généralement à une classe de périphérique. Si l'accès est défini sur **Autoriser**, l'utilisateur ou le groupe sélectionné sera en mesure d'accéder à tous les périphériques de la classe.
- La protection peut également être appliquée à des périphériques spécifiques.
- Configurez l'authentification Just-in-time (JITA), qui permet aux utilisateurs sélectionnés d'accéder aux lecteurs de DVD/CD-ROM ou à des lecteurs de disque amovibles en s'authentifiant eux-mêmes. Pour plus d'informations, reportez-vous à la section Configuration JITA à la page 49.
- Autorisez ou refusez l'accès à d'autres classes de périphériques, telles que les supports amovibles (comme les clés USB), les ports série et parallèle, les périphériques Bluetooth®, les modems, les périphériques PCMCIA/ExpressCard, les périphériques 1394, les lecteurs d'empreintes digitales ou les lecteurs de carte à puce. Si l'accès aux lecteurs d'empreintes digitales et aux lecteurs de carte à puce est refusé, ceux-ci peuvent servir à s'authentifier, mais ils ne peuvent pas être utilisés pour les règles de session.

REMARQUE : si des périphériques Bluetooth sont utilisés à des fins d'authentification, l'accès aux périphériques Bluetooth ne doit pas avoir été restreint au sein de la politique de Device Access Manager.

- Lorsque vous sélectionnez un paramètre au niveau du groupe ou de la classe de périphérique, il vous est demandé s'il faut appliquer le paramètre aux objets fils :

  Oui — Le paramètre se propagera.

  Non — Le paramètre ne se propagera pas.
- Certaines classes de périphériques, telles que les DVD et les CD-ROM, peuvent être contrôlées de manière plus poussée en autorisant ou en refusant l'accès séparément pour les opérations de lecture et d'écriture.

REMARQUE : Le groupe Administrateurs ne peut pas être ajouté à la liste des utilisateurs.

- **Accès** — Cliquez ou tapez sur la flèche descendante, puis sélectionnez l'un des types d'accès suivants pour autoriser ou refuser l'accès :
  - **Autoriser – Accès maximal**
  - **Autoriser – Lecture seule**
  - **Autoriser – JITA requis** — Pour plus d'informations, reportez-vous à la section Configuration JITA à la page 49

    Si ce type d'accès est sélectionné, sous **Durée**, cliquez ou tapez sur la flèche descendante pour sélectionner un délai maximal.
  - **Refuser**
- **Durée** — Cliquez ou tapez sur la flèche descendante afin de sélectionner un délai maximal pour accéder aux lecteurs de CD/DVD-ROM ou aux lecteurs de disque amovibles (reportez-vous à Configuration JITA à la page 49).

Configuration JITA

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

Les utilisateurs pour lesquels l'authentification JITA est activée seront en mesure d'accéder à certains périphériques pour lesquels des politiques créées dans la vue **Configuration de classes de périphérique** ont été restreintes.

La période JITA peut être autorisée pour un nombre donné de minutes ou peut être illimitée. Les utilisateurs pour lesquels la période est illimitée auront accès au périphérique depuis leur authentification jusqu'à leur déconnexion du système.

Si une période JITA limitée est attribuée à un utilisateur, celui-ci est invité une minute avant l'expiration de la période JITA à prolonger son accès. Dès que l'utilisateur se déconnecte du système ou qu'un autre utilisateur se connecte, la période JITA expire. La prochaine fois que l'utilisateur se connecte et tente d'accéder à un périphérique ayant l'authentification JITA activée, une invite de saisie des informations d'authentification s'affiche.

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

- Lecteurs de DVD/CD-ROM
- Lecteurs de disque amovibles

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

Les administrateurs peuvent permettre à des utilisateurs ou à des groupes d'accéder à des périphériques à l'aide de l'authentification Just-In-Time (JITA).

1. Lancez **Device Access Manager**, puis cliquez ou tapez sur **Modifier**.
2. Sélectionnez l'utilisateur ou le groupe désiré, puis cliquez ou tapez sur la flèche descendante sous **Accès** pour les **Lecteurs de disque amovibles** ou les **Lecteurs de CD-ROM/DVD-ROM**, et ensuite sur **Autoriser – JITA requis**.
3. Sous **Durée**, cliquez ou tapez sur la flèche descendante afin de sélectionner une période pour l'accès JITA.

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

Désactivation d'une politique JITA pour un utilisateur ou un groupe

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

1. Lancez **Device Access Manager**, puis cliquez ou tapez sur **Modifier**.
2. Sélectionnez l'utilisateur ou le groupe désiré, puis cliquez ou tapez sur la flèche descendante sous **Accès** pour les **Lecteurs de disque amovibles** ou les **Lecteurs de CD-ROM/DVD-ROM**, et ensuite sur **Refuser**.

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

Paramètres

La vue **Paramètres** permet aux administrateurs de consulter et de choisir quels sont les lecteurs dont l'accès doit être contrôlé par Device Access Manager.

REMARQUE : Device Access Manager doit être activé lorsque la liste des lettres d'unités est configurée (reportez-vous à la section Vue système à la page 47).

Classes de périphériques non gérées

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

- Périphériques d'entrée/de sortie
  - CD-ROM
  - Unité de disque
  - Contrôleur de disquette (FDC)
  - Contrôleur de disque dur (HDC)
  - Classe de périphérique d'interface utilisateur infrarouge (HID)
  - Périphériques d'interface utilisateur infrarouge
  - Souris
  - Série multi-port
  - Clavier
  - Imprimantes Plug and play (PnP)
  - Imprimante
  - Mise à niveau d'imprimante
- Alimentation
  - Support de gestion de l'alimentation avancé (APM)
  - Batterie
- Divers
  - Ordinateur
  - Décodeur
  - Affichage
  - Pilote d'affichage unifié Intel®
  - Legacard
  - Pilote multimédia
  - Changeur de média
  - Technologie de mémoire
  - Moniteur
  - Multifonction
  - Client Net
  - Service Net
  - Net trans

- Processeur
- Adaptateur SCSI
- Accélérateur de sécurité
- Périphériques de sécurité
- Système
- Inconnu
- Volume
- Volume instantané

8 HP Trust Circles

HP Trust Circles est une application de sécurité pour fichiers et documents, qui combine le cryptage de fichier/dossier avec une modalité pratique de partage fondées sur des cercles de confiance. L'application crypte les fichiers placés dans des dossiers spécifiés par l'utilisateur, en les protégeant au sein d'un cercle de confiance. Une fois protégés, les fichiers ne peuvent être utilisés et partagés que par les membres du cercle de confiance. Si un non-membre reçoit un fichier protégé, celui-ci reste crypté et le non-membre ne peut pas accéder à son contenu.

Ouverture de Trust Circles

1. Dans l'Écran d'accueil, cliquez ou tapez sur l'application **HP Client Security**.

   –ou–

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

2. Sous **Données**, cliquez ou tapez sur **Trust Circles**.

Mise en route

Il existe deux façons d'envoyer des invitations par courriel et d'y répondre :

- **À l'aide de Microsoft® Outlook** — Utiliser Trust Circles avec Microsoft Outlook permet d'automatiser le traitement de toutes les invitations et réponses Trust Circles venant d'autres utilisateurs.
- **À l'aide de Gmail, Yahoo, Outlook.com ou d'autres services de messagerie (SMTP)** — En renseignant votre nom, votre adresse e-mail et votre mot de passe, Trust Circles utilise votre service de messagerie pour envoyer des invitations électroniques aux membres choisis afin qu'ils rejoignent votre cercle de confiance.

Pour configurer votre profil de base :

1. Entrez votre nom et votre adresse électronique, puis cliquez ou tapez sur **Suivant**.

   Votre nom sera visible à tous les membres qui sont invités à rejoindre votre cercle de confiance. L'adresse électronique sert à envoyer, recevoir ou répondre à des invitations.

2. Entrez le mot de passe de votre messagerie électronique, puis cliquez ou tapez sur **Suivant**.

   Un courriel de test est envoyé pour s'assurer que les paramètres de courrier électronique sont exacts.

   REMARQUE : L'ordinateur doit être connecté à un réseau.

3. Dans le champ **Nom du cercle de confiance**, donnez un nom au cercle de confiance, puis cliquez ou tapez sur **Suivant**.

4. Ajouter des membres et des dossiers, puis cliquez ou tapez sur **Suivant**. Le cercle de confiance est créé avec tous les dossiers sélectionnés et des invitations électroniques sont envoyées à tous les membres choisis. Si, pour une raison quelconque, une invitation ne peut pas être envoyée, une notification s'affiche. Il est possible de réinviter des membres à tout moment

depuis la vue Trust Circle en cliquant sur **Vos cercles de confiance**, puis en double-cliquant ou double-tapant sur le cercle de confiance concerné. Pour plus d'informations, reportez-vous à la section Trust Circles à la page 53.

Trust Circles

Vous pouvez créer un cercle de confiance lors de la configuration initiale après avoir entré votre adresse électronique, ou depuis la vue Trust Circle :

▲ Dans la vue Trust Circle, cliquez ou tapez sur **Créer un cercle de confiance**, puis nommez le cercle de confiance.

- Pour ajouter des membres au cercle de confiance, cliquez ou tapez sur l'icône **M+** située à côté de **Membres**, puis suivez les instructions à l'écran.
- Pour ajouter des dossiers au cercle de confiance, cliquez ou tapez sur l'icône **+** située à côté de **Dossiers**, puis suivez les instructions à l'écran.

Ajout de dossiers à un cercle de confiance

Ajout de dossiers à un nouveau cercle de confiance :

- Lors de la création d'un cercle de confiance, vous pouvez ajouter des dossiers en cliquant ou en tapant sur l'icône **+** située à côté de **Dossiers**, puis en suivant les instructions à l'écran.

  –ou–

- Dans l'Explorateur Windows, faites un clic droit ou maintenez votre doigt appuyé sur un dossier n'appartenant pas à un cercle de confiance, et sélectionnez **Trust Circle** (Cercle de confiance), puis **Create Trust Circle from Folder** (Créer un cercle de confiance à partir du dossier).

ASTUCE : Vous pouvez sélectionner un ou plusieurs dossiers.

Ajout de dossiers à un cercle de confiance existant :

- Dans la vue Trust Circle, cliquez sur **Vos cercles de confiance**, double-cliquez ou double-tapez sur le cercle de confiance existant pour en afficher les dossiers, puis cliquez ou tapez sur l'icône **+** située à côté de **Dossiers**, et enfin suivez les instructions à l'écran.

  –ou–

- Dans l'Explorateur Windows, faites un clic droit ou maintenez votre doigt appuyé sur un dossier n'appartenant pas à un cercle de confiance, et sélectionnez **Trust Circle** (Cercle de confiance), puis **Add to existing Trust Circle from Folder** (Ajouter le dossier à un cercle de confiance existant).

ASTUCE : Vous pouvez sélectionner un ou plusieurs dossiers.

Une fois qu'un dossier a été ajouté à un cercle de confiance, Trust Circles le crypte automatiquement, lui et son contenu. Une fois tous les fichiers cryptés, une notification s'affiche. De plus, un cadenas vert s'affiche alors sur toutes les icônes des dossiers et fichiers cryptés dans ces dossiers, indiquant ainsi qu'ils sont entièrement protégés.

Ajout de membres à un cercle de confiance

Trois étapes sont nécessaires pour ajouter des membres à un cercle de confiance :

1. **Invitation** — Tout d'abord, le propriétaire du cercle de confiance invite un ou plusieurs membres. Le courriel d'invitation peut être envoyé à plusieurs utilisateurs ou à des groupes/listes de diffusion.
2. **Acceptation** — La personne invitée reçoit l'invitation et choisit de l'accepter ou la refuser. Si l'invité accepte l'invitation, un courriel de réponse est envoyé à l'invitant. Si l'invitation a été envoyée à un groupe, chaque membre reçoit une invitation et décide de l'accepter ou la refuser.
3. **Inscription** — L'invitant peut alors confirmer ou non sa décision d'ajouter le membre au cercle de confiance. S'il décide d'inscrire le membre, un courriel est envoyé à l'invité pour lui faire part de la réponse. L'invitant et l'invité peuvent éventuellement vérifier la sécurité de la procédure d'invitation. Un code de vérification s'affiche alors pour l'invité, qu'il doit lire à l'invitant par téléphone. Une fois le code vérifié, l'invitant peut envoyer le courriel final d'inscription.

Ajout de membres à un nouveau cercle de confiance :

▲ Lors de la création d'un cercle de confiance, vous pouvez ajouter des membres en cliquant ou en tapant sur l'icône **M+** située à côté de **Membres**, puis en suivant les instructions à l'écran.

- Si vous utilisez Outlook, sélectionnez les contacts du carnet d'adresses Outlook, puis cliquez sur **OK**
- Si vous utilisez un autre service de messagerie, vous pouvez soit ajouter manuellement de nouvelles adresses électroniques à Trust Circle, ou les récupérer à partir de l'adresse électronique enregistrée sur Trust Circle.

Ajout de membres à un cercle de confiance existant :

▲ Dans la vue Trust Circle, cliquez sur **Vos cercles de confiance**, double-cliquez ou double-tapez sur le cercle de confiance existant pour en afficher les membres actuels, puis cliquez ou tapez sur l'icône **M+** située à côté de **Membres**, et enfin suivez les instructions à l'écran.

- Si vous utilisez Outlook, sélectionnez les contacts du carnet d'adresses Outlook, puis cliquez sur **OK**.
- Si vous utilisez un autre service de messagerie, vous pouvez soit ajouter manuellement de nouvelles adresses électroniques à Trust Circle, ou les récupérer à partir de l'adresse électronique enregistrée sur Trust Circle.

Ajout de fichiers à un cercle de confiance

Vous pouvez ajouter des fichiers à un cercle de confiance de l'une des façons suivantes :

- Copiez ou déplacez le fichier vers un dossier d'un cercle de confiance existant.

  –ou–

- Dans l'Explorateur Windows, faites un clic droit ou maintenez votre doigt appuyé sur un fichier n'étant pas crypté, et sélectionnez **Trust Circle**, puis **Crypter**. Vous serez invité-e à sélectionner le cercle de confiance auquel le fichier doit être ajouté.

ASTUCE : Vous pouvez sélectionner un ou plusieurs fichiers.

Dossiers cryptés

Tout membre d'un cercle de confiance peut consulter et éditer les fichiers qui appartiennent à ce cercle de confiance.

REMARQUE : Trust Circle Manager/Reader ne synchronise pas les fichiers entre les membres.

Les fichiers doivent être partagés au moyen d'outils existants tels que le courrier électronique, le transfert FTP ou le stockage en nuage. Les fichiers copiés, déplacés ou créés dans un dossier de cercle de confiance sont immédiatement protégés.

Suppression de dossiers placés dans un cercle de confiance

Supprimer un dossier d'un cercle de confiance décrypte le dossier et l'ensemble de son contenu, et retire également sa protection.

- Dans la vue Trust Circle, cliquez sur **Vos cercles de confiance**, double-cliquez ou double-tapez sur le cercle de confiance existant pour en afficher les dossiers, puis cliquez ou tapez sur l'icône de **poubelle** située à côté de ce dossier.

  –ou–

- Dans l'Explorateur Windows, faites un clic droit ou maintenez votre doigt appuyé sur un dossier appartenant à un cercle de confiance, et sélectionnez **Trust Circle** (Cercle de confiance), puis **Remove from trust circle** (Supprimer du cercle de confiance).

ASTUCE : Vous pouvez sélectionner un ou plusieurs dossiers.

Suppression d'un fichier placé dans un cercle de confiance

Pour supprimer un fichier d'un cercle de confiance, dans l'Explorateur Windows, faites un clic droit ou maintenez votre doigt appuyé sur un fichier n'étant pas crypté, et sélectionnez **Trust Circle** (Cercle de confiance), puis **Decrypt File** (Décrypter le fichier).

Retrait de membres d'un cercle de confiance

Un membre dont l'inscription s'est entièrement déroulée ne peut pas être retiré d'un cercle de confiance. Une solution possible consiste à créer un nouveau cercle de confiance comportant tous les autres membres, puis déplacer tous les fichiers et dossiers vers le nouveau cercle de confiance, et enfin supprimer l'ancien cercle de confiance. Ceci garantira que le membre de l'ancien cercle n'aura pas accès aux nouveaux fichiers. Toutefois, tout ce qui a été partagé auparavant lui restera accessible.

Si l'inscription d'un membre n'est pas complète (parce que son invitation est en attente ou qu'il a refusé de rejoindre le cercle de confiance), vous pouvez retirer le membre du cercle de confiance de l'une des façons suivantes :

- Dans la vue Trust Circle, cliquez ou tapez sur **Vos cercles de confiance**, puis double-cliquez ou double-tapez sur le cercle de confiance pour en afficher la liste des membres actuels. Cliquez ou tapez sur l'icône de **poubelle** située à côté du nom du membre à retirer.
- Dans la vue Trust Circle, cliquez ou tapez sur **Membres**, puis double-cliquez ou double-tapez sur le membre pour afficher les cercles de confiance auxquels il appartient. Cliquez ou tapez sur l'icône de **poubelle** située à côté d'un cercle de confiance pour en retirer le membre.

Suppression d'un cercle de confiance

Pour supprimer un cercle de confiance, il faut en être propriétaire.

▲ Dans la vue Trust Circle, cliquez ou tapez sur **Vos cercles de confiance**, puis sur l'icône de **poubelle** située à côté du cercle de confiance à supprimer.

Cette opération supprime le cercle de confiance de la page et envoie des courriels à tous ses membres pour les informer de sa suppression. Tous les fichiers ou dossiers ayant été inclus dans ce cercle de confiance sont alors décryptés.

Configuration des préférences

Dans la vue Trust Circle, cliquez ou tapez sur **Préférences**. Trois volets s'affichent :

- **Paramètres de courrier électronique**

Option	Description
Nom d'utilisateur	Le nom d'utilisateur actuellement utilisé est affiché. Pour le modifier, entrez un nouveau nom d'utilisateur dans la zone de texte. Les modifications sont enregistrées automatiquement.
Adresse électronique	Le compte de messagerie actuellement utilisé est affiché. Pour le changer, cliquez ou tapez sur **Modifier les paramètres de courrier électronique** et suivez les instructions à l'écran.
Confirmation des nouveaux membres	Sélectionnez parmi les options suivantes : ◦ **Confirmer automatiquement** — Après avoir reçu l'acceptation d'un invité, celui-ci est inscrit dans le cercle de confiance sans besoin d'aucune opération manuelle, et un courriel de confirmation lui est envoyé. ◦ **Confirmer manuellement** — Après avoir reçu l'acceptation d'un invité, une intervention manuelle est nécessaire pour inscrire le nouveau membre dans le cercle de confiance, puis un courriel de confirmation lui est envoyé. ◦ **Vérification requise** — Après avoir reçu l'acceptation d'un invité, un code de vérification est nécessaire pour pouvoir finaliser son inscription. Le propriétaire du cercle de confiance doit contacter l'invité et lui demander le code de vérification. Une fois le code correct saisi, un courriel de confirmation est envoyé.
Authentification périodique	L'authentification périodique oblige l'utilisateur à saisir le mot de passe Windows après un délai spécifié (en minutes) ainsi que lors de l'exécution d'opérations sensibles. Ce paramètre permet aux utilisateurs d'activer ou de désactiver cette authentification.
Délai d'authentification	Indiquez le délai d'attente (en minutes) avant qu'une authentification soit requise.
Ne pas afficher de message de confirmation	Cochez cette case pour désactiver les messages de confirmation, ou décochez-la pour en activer l'affichage.
Je voudrais contribuer à améliorer HP Trust Circle grâce au suivi d'utilisation anonyme	Cochez cette case pour participer au programme, ou décochez-la si vous ne souhaitez pas y participer.

- **Sauvegarde/Restauration**

Option	Description
Sauvegarde	Copie vos données d'application (les paramètres et cercles de confiance) de Trust Circle Manager/Reader dans un fichier de sauvegarde. En cas de défaillance ou panne du système, vous pouvez utiliser ce fichier pour restaurer votre nouvelle installation de Trust Circles à l'état sauvegardé dans le fichier. **REMARQUE :** Seules vos données d'application pour Trust Circle sont sauvegardées (les cercles de confiance, paramètres et membres). Les fichiers se trouvant dans les dossiers des cercles de confiance ne sont pas sauvegardés. Ces fichiers doivent être sauvegardés séparément. Pour sauvegarder les données utilisateur et les paramètres de Trust Circle : **1.** Cliquez ou tapez sur **Sauvegarder**. **2.** Choisissez un nom de fichier et un répertoire pour le fichier de sauvegarde, puis cliquez ou tapez sur **Enregistrer**. **3.** Entrez un mot de passe, confirmez-le, puis cliquez ou tapez sur **OK**. Ce mot de passe sera nécessaire pour restaurer ce fichier.
Restauration	Restaure les paramètres et les cercles de confiance à partir d'un fichier de sauvegarde, généralement à la suite d'une panne du système ou d'une migration vers un autre ordinateur. Pour restaurer les paramètres et les données utilisateur de Trust Circle Manager : **1.** Cliquez ou tapez sur **Restaurer**. **2.** Accédez au répertoire du fichier de sauvegarde et sélectionnez celui-ci, puis cliquez ou tapez sur **Ouvrir**. **3.** Entrez le mot de passe défini lors de la sauvegarde.

- **À propos de** — La version du logiciel Trust Circle Manager/Reader est affichée. Des liens s'affichent pour vous permettre de mettre à niveau Trust Circle Manager à la version Pro ou consulter la déclaration de confidentialité de HP.

9 Récupération en cas de vol (certains modèles)

Computrace (vendu séparément) vous permet de contrôler, de gérer et de localiser votre ordinateur à distance.

Une fois activé, Computrace peut être configuré depuis le Centre clientèle d'Absolute Software. Depuis le Centre clientèle, l'administrateur peut configurer le contrôle et la gestion de l'ordinateur par Computrace. En cas de perte ou de vol de l'ordinateur, le Centre clientèle peut aider les autorités locales à le localiser et à le retrouver. Une fois configuré, Computrace continue à fonctionner même en cas d'effacement ou de remplacement du disque dur.

Pour activer Computrace :

1. Connectez-vous à l'Internet.
2. Ouvrir HP Client Security Pour plus d'informations, reportez-vous à la section Ouverture de HP Client Security à la page 10.
3. Cliquez sur **Récupération en cas de vol**.
4. Pour lancer l'Assistant d'activation Computrace, cliquez sur le bouton **Mise en route**.
5. Saisissez vos informations de contact, ainsi que les informations de paiement de votre carte de crédit ou saisissez une clé de produit achetée au préalable.

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

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

Pour vous connecter au Centre de clientèle :

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

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

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

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

10 Exceptions de mot de passe localisé

Aux niveaux de l'Authentification à la mise sous tension et de HP Drive Encryption, la prise en charge de la localisation des mots de passe est limitée. Pour plus d'informations, reportez-vous à la section Les IME Windows ne sont pas pris en charge au niveau de l'Authentification à la mise sous tension ou de Drive Encryption à la page 59.

Que faire lorsqu'un mot de passe est rejeté

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

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

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

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

  1. Modifiez le mot de passe de Windows de manière à n'utiliser que des caractères pris en charge. Pour en savoir plus sur les caractères non pris en charge, reportez-vous à la section Gestion des touches spéciales à la page 60.
  2. Lancez HP Client Security, puis entrez le mot de passe Windows.

Les IME Windows ne sont pas pris en charge au niveau de l'Authentification à la mise sous tension ou de Drive Encryption

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

Les IME ne sont pas pris en charge au niveau de l'Authentification à la mise sous tension ou de Drive Encryption. Un mot de passe Windows ne peut pas être saisi par le biais d'un IME dans l'écran d'identification de l'Authentification à la mise sous tension ou de HP Drive Encryption. Procéder de la sorte peut provoquer un blocage. Dans certains cas, Microsoft®Windows n'affiche pas l'IME lorsque l'utilisateur saisit le mot de passe.

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

- Microsoft IME pour le japonais
- La disposition de clavier japonais
- Office 2007 IME pour le japonais : si Microsoft ou une tierce partie utilise le terme IME ou éditeur de méthode d'entrée, la méthode d'entrée peut ne pas être réellement un IME. Cela peut être source de confusion, mais le logiciel lit la représentation du code hexadécimal. Par conséquent,

si un IME établit une correspondance avec une disposition de clavier prise en charge, HP Client Security peut alors prendre en charge la configuration.

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

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

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

REMARQUE : Les administrateurs peuvent résoudre ce problème en utilisant la page Utilisateurs de HP Client Security (accessible à partir de l'icône d'**Engrenage** de la page d'accueil) pour supprimer l'utilisateur de HP Client Security, puis en sélectionnant la disposition de clavier souhaitée dans le système d'exploitation, et enfin en exécutant à nouveau l'Assistant de configuration de HP Client Security pour cet utilisateur. Le BIOS sauvegarde la disposition de clavier désirée, permettant aux mots de passe pouvant être saisis à l'aide de cette disposition de clavier d'être proprement définis dans le BIOS.

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

Gestion des touches spéciales

- Chinois, slovaque, français canadien et tchèque.

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

- Coréen

  Lorsqu'un utilisateur sélectionne une disposition de clavier coréen prise en charge, puis saisit un mot de passe, le même mot de passe doit être saisi tout en appuyant sur la touche alt de droite pour les minuscules et les touches alt et maj. de droite pour les majuscules dans l'authentification à la mise sous tension et HP Drive Encryption.

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

Language (Langue)	Windows	BIOS	Drive Encryption
Arabe	Les touches ﻻ ,ﻷ, et ﻹ génèrent deux caractères.	Les touches ﻻ ,ﻷ, et ﻹ génèrent un seul caractère.	Les touches ﻻ ,ﻷ, et ﻹ génèrent un seul caractère.

Language (Langue)	Windows	BIOS	Drive Encryption
Français canadien	ç, è, à et é deviennent Ç, È, À, et É lors de l'utilisation de maj. dans Windows.	ç, è, à, et é avec verr maj sont ç, è, à, et é dans l'authentification à la mise sous tension.	ç, è, à et é deviennent ç, è, à et é lors de l'utilisation de maj. dans HP Drive Encryption.
Espagnol	40a n'est pas pris en charge. Néanmoins, cela fonctionne parce que le logiciel le convertit en c0a. Cependant, en raison de différences légères entre les dispositions de clavier, il est recommandé aux utilisateurs de langue espagnole de modifier la disposition de leur clavier sous Windows afin d'utiliser 1040a (variation espagnole) ou 080a (Amérique latine).	n/a	n/a
US international	◦ Les touches ¡, ¤, ‘, ’, ¥ et ×, situées sur la ligne du haut, sont rejetées. ◦ Les touches å, ®, et Þ, situées sur la deuxième ligne, sont rejetées. ◦ Les touches á, ð, et ø, situées sur la troisième ligne, sont rejetées. ◦ La touche æ, située sur la ligne du bas, est rejetée.	n/a	n/a
Czech	◦ La touche ğ est rejetée. ◦ La touche į est rejetée. ◦ La touche ų est rejetée. ◦ Les touches ė, ı, et ż sont rejetées. ◦ Les touches ģ, ķ, ļ, ņ, et ţ keys sont rejetées.	n/a	n/a
Slovaque	La touche ż est rejetée.	◦ Les touches š, ś, et ş sont rejetées lors de la saisie, mais acceptées si saisies à l'aide du clavier virtuel. ◦ La touche ţ génère deux caractères.	n/a
Hungarian	La touche ż est rejetée.	La touche ţ génère deux caractères.	n/a

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

Glossaire

activation
Tâche devant être effectuée avant de pouvoir accéder à l'une des fonctions de Drive Encryption. Les administrateurs peuvent activer Drive Encryption via l'Assistant de configuration de HP Client Security ou HP Client Security. Le processus d'activation consiste à activer le logiciel, à crypter l'unité et à créer la clé de cryptage de sauvegarde initiale sur un périphérique de stockage amovible.

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

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

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

authentification
Processus de vérification de votre identité à l’aide d’informations d’authentification telles que votre mot de passe Windows, vos empreintes digitales, une carte Smart Card, une carte sans contact ou une carte de proximité.

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

Authentification au préamorçage de Drive Encryption.
Ecran de connexion affiché avant le démarrage de Windows. Les utilisateurs doivent entrer leur nom d'utilisateur Windows, ainsi que le mot de passe ou le code PIN de la carte Smart Card, ou bien passer leur doigt si leur empreinte est enregistrée. Si la connexion directe est sélectionnée, la saisie des informations correctes sur l'écran de connexion de Drive Encryption permet d'accéder directement à Windows sans avoir à se reconnecter sur l'écran de connexion Windows.

Authentification Just In Time
Reportez-vous à l'aide logicielle de HP Device Access Manager.

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

Bluetooth
Technologie utilisant les transmissions radio pour activer les ordinateurs, les imprimantes, les souris, les téléphones mobiles et les autres périphériques compatibles Bluetooth pour la communication sans fil sur une courte distance.

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

carte de proximité
Carte en plastique avec puce informatique intégrée qui peut être utilisée à des fins d’authentification en conjonction avec d’autres informations d’authentification pour plus de sécurité.

carte sans contact

Carte en plastique avec puce informatique intégrée pouvant être utilisée pour l’authentification.

Cercle de confiance
Fournit un confinement des données en liant celles-ci à un groupe défini d'utilisateurs approuvés. Ceci empêche que les données tombent entre de mauvaises mains, que ce soit de manière accidentelle ou intentionnelle. Sécurisées au moyen de la technologie Zero Overhead Key Management de CryptoMill, les données sont liées cryptographiquement à un cercle de confiance. Cela empêche le décryptage de documents ou d'autres informations sensibles hors du cercle de confiance.

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

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

compte utilisateur Windows
Utilisateur autorisé à se connecter à un réseau ou à un ordinateur individuel.

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

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

cryptage logiciel
Utilisation du logiciel pour crypter le disque dur secteur par secteur. Ce processus est plus lent que le cryptage matériel.

cryptage matériel
Utilisation d'unités auto cryptées conformes aux spécifications OPAL du Trusted Computing Group relatives à la gestion des unités auto cryptées pour l'exécution d'un cryptage simultané. Le cryptage matériel est instantané et peut prendre seulement quelques minutes, tandis que le cryptage logiciel peut prendre plusieurs heures.

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

destruction
Exécution d'un algorithme remplaçant les données contenues dans une ressource par des données sans importance.

destruction automatique
Destruction que vous planifiez dans File Sanitizer.

destruction manuelle
La destruction d'une ressource ou des ressources sélectionnées, qui ignore une destruction planifiée.

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

Dossier de cercle de confiance
Tout dossier protégé par un cercle de confiance.

Drive Encryption

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

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

écran de connexion de Drive Encryption
Voir authentification au préamorçage de Drive Encryption.

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

empreinte digitale
Extraction numérique de l'image de votre empreinte digitale. L'image réelle de votre empreinte digitale n'est jamais stockée par HP Client Security.

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

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

information d'identification
Information ou périphérique matériel spécifique utilisé pour authentifier un utilisateur individuel.

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

nettoyage de l'espace libre
Le remplacement de ressources supprimées et d'espace inutilisé par des données aléatoires. Ce processus réduit l'existence de la ressource supprimée rendant encore plus difficile toute récupération de la ressource d'origine.

Page d'accueil
Emplacement central qui vous permet d'accéder aux fonctions et paramètres de HP Client Security et de les gérer.

périphérique connecté
Périphérique matériel connecté à un port de l'ordinateur.

PIN
Un numéro d'identification personnel pour un utilisateur inscrit utilisé pour l'authentification.

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

Puce de sécurité intégrée TPM (Trusted Platform Module)
Un TPM authentifie un ordinateur, plutôt qu'un utilisateur, en enregistrant les informations propres au système hôte, telles que les clés de chiffrement, les certificats numériques et les mots de passe. Il minimise le risque de compromission des informations présentes sur l'ordinateur en cas de vol ou de piratage.

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

redémarrage
Processus de redémarrage de l'ordinateur.

ressource

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

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

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

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

Smart Card
Périphérique matériel pouvant être utilisé pour s'authentifier à l'aide d'un code PIN.

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

Trust Circle Manager/Reader
Trust Circle Reader permet uniquement d'accepter des invitations envoyées par des utilisateurs de Trust Circle Manager. Trust Circle Manager, quant à lui, peut servir à créer des cercles de confiance. Cette application permet également d'inviter quelqu'un par courriel dans un cercle de confiance et d'accepter des invitations à des cercles de confiance venant d'autres personnes. Une fois qu'un cercle de confiance est établi entre des individus, les fichiers protégés par ce cercle de confiance peuvent être partagés en toute sécurité.

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

Index

A

accès
  contrôle 46
  empêcher l'accès non autorisé 6
activation
  Drive Encryption pour les disques durs standard 34
  Drive Encryption pour les unités auto-cryptées 34
affichage des fichiers journaux 45
ajout de dossiers 53
ajout de fichiers 54
ajout de membres 54
Assainisseur de disque 43
  ouverture 41
  procédures de configuration 41
Assainisseur de fichiers HP 40
Assistant de configuration de HP Client Security 9

C

cartes 18
changements de mot de passe à l'aide de différentes dispositions de clavier 60
classes de périphériques, non gérées 50
classes de périphériques non gérées 50
clé de cryptage
  sauvegarde 37
Computrace 58
configuration
  classe de périphérique 47
Configuration de l'authentification Just-In-Time 49
Configuration JITA 49
connexion à l'ordinateur 35
connexions
  catégories 24
  gestion 24
  importation et exportation 26
  modification 23
contrôle de l'accès aux périphériques 46
cryptage
  lecteurs 33
  logiciel 34, 35, 37
  matériel 34, 35
cryptage de disque dur 36
cryptage de partitions de disque dur 37
cryptage logiciel 34, 35, 37
cryptage matériel 34, 35

D

décryptage
  lecteurs 33
décryptage de partitions de disque dur 37
définition
  programmation de destruction 42
  programmation de nettoyage 43
désactivation de Drive Encryption 35
destruction
  clic droit 44
  manuelle 44
destruction par bouton droit 44
données
  limitation de l'accès 6
dossiers cryptés 55

E

empreintes digitales
  paramètres d'administration 15
  paramètres d'utilisateur 16
empreintes digitales, inscription 14
exceptions de mot de passe 59

F

fichiers journaux, affichage 45
fonctions, HP Client Security 1
Fonctions de HP Client Security 1
Fonctions de sécurité 29

G

gestion
  cryptage ou décryptage de partitions d'unités 37
  mots de passe 20, 21
gestion des disques 37
gestion des touches spéciales 60
Gestionnaire de mots de passe 20, 21
Guide de configuration facile pour les petites entreprises 11

H

HP Client Security 14
  Mot de passe de sauvegarde et restauration 8
HP Client Security, ouverture 10
HP Device Access Manager 46
  configuration rapide 13
  ouverture 47
HP Drive Encryption 33, 36
  activation 34
  configuration rapide 13
  connexion après activation de Drive Encryption 34
  cryptage de lecteurs individuels 36
  décryptage de lecteurs individuels 36
  désactivation 34
  gestion de Drive Encryption 36
  sauvegarde et restauration 37
HP SpareKey 16
HP Trust Circles 52

I

icône, utilisation 44
informations de connexion
  ajout 21

inscription
empreintes digitales 14

L
lancement du nettoyage de l'espace libre 45
lancement manuel d'une opération de destruction 44
Liens rapides
Menu 23
limitation
accès aux données sensibles 6

M
Mes règles 30
mise en route 11, 52
mot de passe
directives 8
gestion 7
HP Client Security 7
règles 6
sécurisé 8
mot de passe d'ouverture de session Windows 7
mot de passe rejeté 59
mot de passe Windows, changement 17

N
nettoyage
démarrage 45
manuel 45
programmation 43
nettoyage de l'espace libre 43
non autorisé, empêcher l'accès 6

O
objectifs de sécurité 5
ouverture
Assainisseur de disque 41
HP Device Access Manager 47
ouverture de Drive Encryption 33
ouverture de Trust Circle 52

P
paramètres 16
Gestionnaire de mots de passe 27
HP SpareKey 16
icône 25
Périphériques Bluetooth 17
PIN 20
paramètres, cartes à puce, de proximité et sans contact 19
Paramètres avancés 49
paramètres avancés de HP Client Security 28
paramètres d'administration
empreintes digitales 15, 16
Password Manager
affichage et gestion des authentifications enregistrées 12
configuration facile 11
Périphériques Bluetooth 17
PIN 19
Politique JITA
création pour un utilisateur ou un groupe 49
désactivation pour un utilisateur ou un groupe 49
préférences 56
principaux objectifs de sécurité 5
profil de destruction 42
programmation de destruction, définition 42
protéger des ressources d'une destruction 43

R
récupération de HP SpareKey 38
récupération de mot de passe 16
récupération en cas de Vol 58
règle
administrateur 28
utilisateur standard 29
restauration
Informations d'authentification de HP Client Security 8
restauration de l'accès activé à l'aide des clés de sauvegarde 38
restriction
accès aux périphériques 46
retrait de membres 55
RSA SecurID 20

S
sauvegarde
Informations d'authentification de HP Client Security 8
sauvegarde de la clé de cryptage 37
sécurité 7
principaux objectifs 5
rôles 7
sécurité du mot de passe 25
Smart Card
code PIN 8
suppression de cercles de confiance 56
suppression de dossiers 55
suppression de fichiers 55

T
Trust Circles
ouverture 52

V
vol, protection 6
vue système 47
vue utilisateur 47