

HP ProtectTools

Mise en route

© Copyright 2011 Hewlett-Packard
Development Company, L.P.

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

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

Première édition : janvier 2011

Référence du document : 638391-051

Sommaire

1 Introduction à la sécurité	1
Fonctions HP ProtectTools	2
Description des produits de sécurité HP ProtectTools et exemples d'utilisation courante	4
Credential Manager for HP ProtectTools	4
Drive Encryption for HP ProtectTools	4
File Sanitizer for HP ProtectTools	5
Device Access Manager for HP ProtectTools	5
Privacy Manager for HP ProtectTools	6
Computrace for HP ProtectTools (anciennement LoJack Pro)	6
Embedded Security for HP ProtectTools (certains modèles uniquement)	7
Objectifs de sécurité fondamentaux	8
Protection contre le vol ciblé	8
Limitation de l'accès aux données confidentielles	8
Protection contre des accès non autorisés depuis des sites internes ou externes	8
Création de stratégies de mots de passe complexes	9
Éléments de sécurité supplémentaires	10
Attribution des rôles de sécurité	10
Gestion de mots de passe HP ProtectTools	10
Création d'un mot de passe sécurisé	12
Sauvegarde et restauration des informations d'authentification de HP ProtectTools	12
2 Mise en route avec l'Assistant de configuration	13
3 Console d'administration de HP ProtectTools Security Manager	16
Ouverture de la console d'administration de HP ProtectTools	17
Utilisation de la console d'administration	18
Configuration de votre système	19
Configuration de l'authentification pour votre ordinateur	19
Règles de connexion	19
Règles de session	20
Paramètres	20

Gestion des utilisateurs	20
Informations d'authentification	21
SpareKey	21
Empreintes digitales	22
Smart Card	22
Visage	23
Configuration de vos applications	24
onglet Général	24
Onglet Applications	24
Gestion centrale	25

4 HP ProtectTools Security Manager 26

Ouverture de Security Manager	27
Utilisation du tableau de bord de Security Manager	28
Etat des applications de sécurité	29
My Logons (Mes connexions)	30
Gestionnaire de mots de passe	30
Si aucune connexion n'a été créée pour les pages Web ou les programmes . .	30
Si une connexion a déjà été créée pour les pages Web ou les programmes ...	31
Ajout de connexions	31
Modification des connexions	32
Utilisation du menu des connexions	33
Organisation des connexions en catégories	33
Gestion de vos connexions	34
Evaluation de la force de votre mot de passe	34
Paramètres de l'icône du Gestionnaire de mots de passe	35
VeriSign Identity Protection (VIP)	35
Paramètres	37
Credential Manager	37
Changement de votre mot de passe Windows	37
Configuration d'une SpareKey	38
Inscription des empreintes digitales	38
Configuration d'une Smart Card	38
Initialisation de la Smart Card	39
Enregistrement de la Smart Card	39
Configuration de la Smart Card	40
Inscription de scènes pour la connexion par reconnaissance faciale	40
Paramètres utilisateur avancés	42
Votre carte d'identité personnelle	44
Définition de vos préférences	44
Sauvegarde et restauration de vos données	45

5 Drive Encryption for HP ProtectTools (certains modèles uniquement)	47
Ouverture de Drive Encryption	48
Tâches générales	49
Activation de Drive Encryption pour les disques durs standard	49
Activation de Drive Encryption pour les unités autocryptées	50
Désactivation de Drive Encryption	51
Connexion après l'activation de Drive Encryption	52
Protection de vos données via le cryptage de votre disque dur	53
Affichage de l'état de cryptage	53
Tâches avancées	55
Gestion de Drive Encryption (administrateur uniquement)	55
Cryptage ou décryptage d'unités individuelles (cryptage logiciel uniquement) .	55
Sauvegarde et restauration (tâche de l'administrateur)	56
Sauvegarde des clés de cryptage	56
Récupération des clés de cryptage	56
6 Privacy Manager pour HP ProtectTools (certains modèles)	58
Ouverture de Privacy Manager	59
Procédures de configuration	60
Gestion des certificats Privacy Manager	60
Demande d'un certificat Privacy Manager	60
Obtention d'un certificat Privacy Manager d'entreprise préattribué	61
Configuration d'un certificat Privacy Manager	61
Importation d'un certificat tiers	61
Affichage des détails du certificat Privacy Manager	62
Renouvellement d'un certificat Privacy Manager	62
Configuration d'un certificat Privacy Manager par défaut	62
Suppression d'un certificat Privacy Manager	63
Restauration d'un certificat Privacy Manager	63
Révocation d'un certificat Privacy Manager	63
Gestion des contacts authentifiés	64
Ajout de contacts authentifiés	64
Ajout d'un contact authentifié	65
Ajout de contacts authentifiés à l'aide des contacts Microsoft Outlook	65
Affichage des détails d'un contact authentifié	66
Suppression d'un contact authentifié	66
Vérification de l'état de révocation d'un contact authentifié	66
Tâches générales	68
Utilisation de Privacy Manager dans Microsoft Outlook	68
Configuration de Privacy Manager pour Microsoft Outlook	68

Signature et envoi d'un message électronique	69
Scellage et envoi d'un message électronique	69
Affichage d'un message électronique crypté	69
Utilisation de Privacy Manager dans un document Microsoft Office 2007	69
Configuration de Privacy Manager pour Microsoft Office	70
Signature d'un document Microsoft Office	70
Ajout d'une ligne de signature lors de la signature d'un document Microsoft Word ou Microsoft Excel	70
Ajout de signataires suggérés à un document Microsoft Word ou Microsoft Excel	71
Ajout d'une ligne de signature pour un signataire suggéré	71
Cryptage d'un document Microsoft Office	71
Suppression du cryptage d'un document Microsoft Office	72
Envoi d'un document Microsoft Office crypté	72
Affichage d'un document Microsoft Office signé	73
Affichage d'un document Microsoft Office crypté	73
Tâches avancées	73
Migration de certificats Privacy Manager et de contacts authentifiés vers un autre ordinateur	73
Sauvegarde de certificats Privacy Manager et de contacts authentifiés	73
Restauration de certificats Privacy Manager et de contacts authentifiés	74
Administration centrale de Privacy Manager	74
7 File Sanitizer pour HP ProtectTools	75
Destruction	76
Nettoyage de l'espace libre	77
Ouverture de File Sanitizer	78
Procédures de configuration	79
Définition d'une programmation de destruction	79
Définition d'une programmation de nettoyage de l'espace libre	79
Sélection ou création d'un profil de destruction	80
Sélection d'un profil de destruction prédéfini	80
Personnalisation d'un profil de destruction	81
Personnalisation d'un profil de suppression simple	82
Tâches générales	83
Utilisation d'une séquence de touches pour démarrer la destruction	83
Utilisation de l'icône File Sanitizer	84
Destruction manuelle d'une ressource	84
Destruction manuelle de tous les éléments sélectionnés	85
Activation manuelle du nettoyage de l'espace libre	85
Abandon d'une opération de destruction ou de nettoyage de l'espace libre	85

Affichage des fichiers journaux	85
8 Device Access Manager pour HP ProtectTools (certains modèles)	87
Ouverture de Device Access Manager	88
Procédures de configuration	89
Configuration de l'accès aux périphériques	89
Configuration simple	89
Démarrage du service d'arrière-plan	90
Configuration de classe de périphérique	90
Interdiction d'accès à un utilisateur ou à un groupe	92
Autorisation d'accès pour un utilisateur ou un groupe	93
Autorisation de l'accès à une classe de périphérique pour un seul utilisateur d'un groupe	93
Autorisation de l'accès à un périphérique spécifique pour un seul utilisateur d'un groupe	94
Suppression des paramètres pour un utilisateur ou un groupe	94
Réinitialisation de la configuration	94
Configuration JITA	95
Création d'une JITA pour un utilisateur ou un groupe	96
Création d'une JITA extensible pour un utilisateur ou un groupe	96
Désactivation d'une JITA pour un utilisateur ou un groupe	96
Paramètres avancés	98
Groupe Administrateurs de périphériques	98
Assistance eSATA	99
Classes de périphériques non gérées	99
9 Récupération en cas de Vol	101
10 Embedded Security for HP ProtectTools (sur certains modèles uniquement)	103
Procédures de configuration	104
Activation de la puce de sécurité intégrée dans Computer Setup	104
Initialisation de la puce de sécurité intégrée	105
Configuration du compte utilisateur de base	106
Tâches générales	107
Utilisation du lecteur sécurisé personnel	107
Cryptage de fichiers et dossiers	107
Envoi et réception de courrier électronique crypté	107
Modification du mot de passe de la clé utilisateur de base	108
Tâches avancées	109
Sauvegarde et restauration	109
Création d'un fichier de sauvegarde	109

Restauration des données de certification à partir du fichier de sauvegarde .	109
Modification du mot de passe propriétaire	110
Réinitialisation d'un mot de passe utilisateur	110
Migration de clés avec l'Assistant de migration	111
11 Exceptions de mot de passe localisé	112
Les IME Windows ne sont pas pris en charge aux niveaux de la sécurité de préamorçage et de HP Drive Encryption.	113
Changements de mot de passe à l'aide d'une disposition de clavier également prise en charge ...	114
Gestion des touches spéciales	115
Que faire lorsqu'un mot de passe est rejeté	118
Glossaire	119
Index	125

1 Introduction à la sécurité

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

Application	Fonctions
Console d'administration de HP ProtectTools (pour les administrateurs)	<ul style="list-style-type: none">• Accès nécessitant des droits d'administrateur Microsoft Windows.• Offre un accès aux modules configurés par un administrateur et non disponibles pour les utilisateurs.• Permet la configuration initiale de la sécurité et configure des options et des exigences pour l'ensemble des utilisateurs.
HP ProtectTools Security Manager (pour les utilisateurs)	<ul style="list-style-type: none">• Permet aux utilisateurs de configurer les options fournies par un administrateur.• Permet aux administrateurs d'offrir aux utilisateurs un contrôle limité sur certains modules HP ProtectTools.

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

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

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

Fonctions HP ProtectTools

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

Module	Principales fonctions
Console d'administration de HP ProtectTools (pour les administrateurs)	<ul style="list-style-type: none">• Définir et configurer des niveaux de sécurité et des méthodes de connexion sécurisées à l'aide de l'assistant de configuration de Security Manager.• Permet de configurer les options masquées, non accessibles aux utilisateurs.• Configurer Device Access Manager et l'accès des utilisateurs.• Ajouter et supprimer des utilisateurs ProtectTools, ainsi qu'afficher l'état des utilisateurs à l'aide des outils d'administration.
HP ProtectTools Security Manager (pour les utilisateurs)	<ul style="list-style-type: none">• Permet d'organiser, de configurer et de changer de mot de passe.• Permet de configurer et de modifier des informations d'authentification de l'utilisateur, telles qu'un mot de passe Windows, une empreinte digitale et une carte Smart Card.• Permet de configurer et de modifier les paramètres de destruction et de nettoyage et d'autres de File Sanitizer.• Afficher les paramètres de Device Access Manager.• Permet de configurer Computrace for HP ProtectTools.• Permet de configurer des préférences et des options de sauvegarde et de restauration.
Credential Manager for HP ProtectTools (Gestionnaire de mots de passe)	<ul style="list-style-type: none">• Permet d'enregistrer, d'organiser et de protéger les noms d'utilisateur et les mots de passe.• Configurer les écrans de connexion des sites Web et programmes pour un accès rapide et sécurisé.• Enregistrez les noms d'utilisateur et mots de passes des sites Web en les entrant dans le Gestionnaire de mots de passe. Lors de la prochaine visite du site, le Gestionnaire de mots de passe renseignera et enverra automatiquement ces données.• Permet de créer des mots de passe plus forts afin de renforcer la sécurité du compte. Password Manager insère et envoie automatiquement les informations.
Drive Encryption for HP ProtectTools (certains modèles)	<ul style="list-style-type: none">• 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.
File Sanitizer for HP ProtectTools	<ul style="list-style-type: none">• Permet de détruire les ressources numériques (informations sensibles : fichiers d'application, contenu de l'historique ou contenu Web, autres données confidentielles) de l'ordinateur et de nettoyer régulièrement le disque dur.

Module	Principales fonctions
Device Access Manager for HP ProtectTools (sur certains modèles uniquement)	<ul style="list-style-type: none"> • 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 inscriptibles.
Privacy Manager pour HP ProtectTools (certains modèles)	<ul style="list-style-type: none"> • Permet d'acquérir des certificats d'autorité, qui vérifient la source, l'intégrité et la sécurité de la communication lors de l'utilisation de la messagerie Microsoft et des documents Microsoft Office.
Computrace for HP ProtectTools (acheté séparément)	<ul style="list-style-type: none"> • 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. • Activation nécessitant des abonnements séparés aux services de suivi et de traçage.
Embedded Security for HP ProtectTools (certains modèles uniquement)	<ul style="list-style-type: none"> • Utilise une puce de sécurité intégrée TPM (Trusted Platform Module) pour assurer la protection contre les accès non autorisés aux données utilisateur et aux informations d'authentification stockées sur un ordinateur. • Permet la création d'un lecteur sécurisé personnel (PSD), qui s'avère utile pour la protection des informations sur le fichier et le dossier de l'utilisateur. • Prend en charge des applications tierces (Microsoft Outlook et Internet Explorer, p. ex) pour assurer la protection des opérations de certificat numérique.

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

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



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

Credential Manager for HP ProtectTools

Credential Manager (composante de Security 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 le courrier électronique.
- Connecter automatiquement l'utilisateur à un site Web ou programme de messagerie.
- Gérer et organiser des authentifications.
- Sélectionner une ressource Web ou réseau et accéder directement au lien.
- Afficher les noms et les mots de passe si nécessaire.

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

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

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

Drive Encryption for HP ProtectTools

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

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

Embedded Security for HP ProtectTools et Drive Encryption for HP ProtectTools ne permettent pas l'accès aux données cryptées même lorsque vous retirez le disque dur. En effet, ils sont intégrés à la carte mère d'origine.

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

File Sanitizer for HP ProtectTools

File Sanitizer for HP ProtectTools permet de supprimer définitivement des données, notamment l'activité du navigateur Internet, les fichiers temporaires, les données précédemment supprimées ou bien d'autres informations. Il est possible de configurer File Sanitizer pour l'exécuter manuellement ou automatiquement en fonction du programme défini par l'utilisateur.

Exemple 1 : Un avocat doit souvent gérer les données sensibles des clients et souhaite s'assurer que les données des fichiers supprimés ne peuvent pas être récupérées. Il utilise File Sanitizer pour "détruire" les fichiers supprimés. De cette façon, il est presque impossible de les récupérer.

En général, lorsque vous supprimez des données sous Windows, ces dernières ne sont pas supprimées du disque dur. Les secteurs du disque dur sont plutôt marqués comme étant disponibles pour une utilisation ultérieure. Tant que les données ne sont remplacées, vous pouvez facilement les récupérer à l'aide des outils courants disponibles sur Internet. File Sanitizer remplace les secteurs par des données aléatoires (à plusieurs reprises si nécessaire), pour que les données supprimées deviennent illisibles et irrécupérables.

Exemple 2 : Un chercheur souhaite détruire automatiquement les données supprimées, les fichiers temporaires, l'activité du navigateur, etc. à la fin de la session. Elle se sert de File Sanitizer pour programmer la "destruction". De cette façon, elle peut sélectionner les fichiers communs ou les fichiers personnalisés à supprimer définitivement et automatiquement.

Device Access Manager for HP ProtectTools

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

Exemple 1 : Un directeur d'une société spécialisée dans la fourniture d'équipement médical utilise souvent des dossiers médicaux personnels avec les données de son entreprise. Les employés doivent accéder à ces données. Cependant, ils doivent veiller à ne pas supprimer les données de l'ordinateur en les transférant sur un lecteur USB ou sur tout autre support de stockage externe. Le réseau est sécurisé, mais les ordinateurs sont équipés de graveurs de CD et de ports USB qui

peuvent permettre aux employés de copier ou de voler des données. Le directeur utilise Device Access Manager pour désactiver les ports USB et les graveurs de CD. De cette façon, il est impossible de les utiliser. Même si les ports USB sont bloqués, la souris et les claviers restent fonctionnels.

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

Privacy Manager for HP ProtectTools

Utilisez Privacy Manager for HP ProtectTools lorsque vous devez sécuriser les communications par messagerie Internet. L'utilisateur peut créer et envoyer un message électronique que seul un destinataire authentifié peut ouvrir. Grâce à Privacy Manager, les informations ne peuvent être ni détournées ni interceptées par un imposteur.

Exemple 1 : Un courtier souhaite s'assurer que ses messages électroniques sont uniquement envoyés à des clients spécifiques et que personne ne peut ni falsifier le compte de messagerie ni l'intercepter. Il s'inscrit à Privacy Manager en plus d'inscrire ses clients. Privacy Manager émet un certificat d'authentification (CA) pour chaque utilisateur. Grâce à cet outil, le courtier et ses clients doivent s'authentifier avant de pouvoir échanger les messages électroniques.

Avec Privacy Manager for HP ProtectTools, vous pouvez facilement envoyer et recevoir des messages électroniques dans la mesure où le destinataire a été vérifié et authentifié. Vous pouvez également crypter le service de messagerie. Le processus de cryptage est identique à celui utilisé pendant les achats courants par carte de crédit sur Internet.

Exemple 2 : Un PDG souhaite s'assurer que seuls les membres du conseil d'administration peuvent consulter les informations envoyées par courrier électronique. Le PDG choisit de crypter les messages électroniques reçus et envoyés par les membres du conseil d'administration. Grâce à un certificat d'authentification Privacy Manager, le PDG et les membres du conseil d'administration peuvent avoir une copie de la clé de cryptage. De cette façon, ils sont les seuls habilités à décrypter le message électronique confidentiel.

Computrace for HP ProtectTools (anciennement LoJack Pro)

Computrace for HP ProtectTools (acheté séparément) est un service capable de suivre l'emplacement d'un ordinateur volé chaque fois que l'utilisateur accède à Internet.

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.

Computrace for HP ProtectTools permet également de gérer et de localiser des ordinateurs à distance. Par ailleurs, il permet de surveiller l'utilisation des ordinateurs et les applications informatiques.

Exemple 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.

Embedded Security for HP ProtectTools (certains modèles uniquement)

Embedded Security for HP ProtectTools permet de créer un lecteur sécurisé personnel. Cette fonction permet à l'utilisateur de créer une partition de disque virtuelle sur l'ordinateur. Cette dernière est entièrement masquée jusqu'à ce que l'utilisateur y accède. Vous pouvez utiliser Embedded Security à chaque fois que vous devez protéger des données de façon discrète, lorsque le reste des données n'est pas crypté.

Exemple 1 : De nombreux employés accèdent, de façon intermittente, à l'ordinateur d'un directeur d'entrepôt à tout moment de la journée. Le directeur souhaite crypter et masquer les données d'entrepôt confidentielles de l'ordinateur. Il souhaite que les données soient tellement protégées que même si quelqu'un vole le disque dur, il ne peut ni décrypter les données ni les lire. Le directeur d'entrepôt décide d'activer Embedded Security et transfère les données confidentielles sur le lecteur sécurisé personnel. Il peut entrer un mot de passe et accéder aux données confidentielles à l'instar d'un autre disque dur. Lorsqu'il se déconnecte ou redémarre le lecteur sécurisé personnel, il doit entrer le mot de passe approprié pour pouvoir afficher ou ouvrir ce dernier. Les employés ne voient jamais les données confidentielles lorsqu'ils accèdent à l'ordinateur.

Embedded Security protège les clés de cryptage d'une puce TPM (Trusted Computing Module) matérielle se trouvant sur la carte mère. Il s'agit du seul outil de cryptage qui réponde aux conditions minimales requises pour résister aux attaques de mot de passe, où un utilisateur tente de deviner le mot de passe de décryptage. Embedded Security permet également de crypter l'intégralité du disque et du courrier électronique.

Exemple 2 : Un courtier souhaite transférer des données extrêmement sensibles sur un autre ordinateur à l'aide d'un lecteur portable. Elle souhaite s'assurer que seuls ces deux ordinateurs peuvent ouvrir le lecteur, même si le mot de passe est compromis. Le courtier a recours à la migration TPM Embedded Security pour autoriser un deuxième ordinateur à accéder aux clés de cryptage nécessaires au décryptage des données. Durant le processus de transfert, même avec le mot de passe, seuls les deux ordinateurs physiques peuvent décrypter les données.

Objectifs de sécurité fondamentaux

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

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

Protection contre le vol ciblé

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

- Une fois activée, la fonction d'authentification au préamorçage d'empêcher l'accès au système d'exploitation. Reportez-vous aux chapitres suivants :
 - Security Manager for HP ProtectTools
 - Embedded Security for HP ProtectTools
 - Drive Encryption for HP ProtectTools
- La fonction Lecteur sécurisé personnel, fournie par le module Embedded Security for HP ProtectTools, permet de crypter des données sensibles afin de garantir qu'elles ne sont pas accessibles sans authentification. Reportez-vous au chapitre suivant :
 - Embedded Security for HP ProtectTools
- Computrace peut suivre l'emplacement de l'ordinateur volé. Reportez-vous au chapitre suivant :
 - Computrace for HP ProtectTools

Limitation de l'accès aux données confidentielles

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

- Device Access Manager for HP ProtectTools permet aux responsables informatiques de limiter l'accès aux périphériques inscriptibles. Il est donc impossible d'imprimer ou de copier les informations sensibles du disque dur sur un support amovible.

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

L'accès non autorisé à un ordinateur professionnel non sécurisé représente un 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 aux chapitres suivants :
 - Password Manager for HP ProtectTools
 - Embedded Security for HP ProtectTools
 - Drive Encryption for HP ProtectTools
- Le Gestionnaire de mots de passe veille à ce que les utilisateurs non-autorisés ne puissent pas obtenir les mots de passe ou accéder aux applications protégées par mot de passe.
- Device Access Manager for HP ProtectTools permet aux responsables informatiques de limiter l'accès aux périphériques inscriptibles de façon à ce que les informations sensibles ne puissent pas être imprimées ou copiées depuis le disque dur.
- File Sanitizer permet de supprimer les données en toute sécurité en détruisant des fichiers et des dossiers critiques ou en nettoyant le disque dur (remplacement des données supprimées qui sont toujours récupérables).
- Grâce à Privacy Manager, vous pouvez acquérir des certificats d'autorité lorsque vous utilisez un programme de messagerie Microsoft ou des documents Microsoft Office. Vous pouvez ainsi envoyer et enregistrer les informations importantes en toute sécurité.

Création de stratégies de mots de passe complexes

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.

Éléments de sécurité supplémentaires

Attribution des rôles de sécurité

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

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

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

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

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

- Administrateur informatique : applique et gère les fonctions de sécurité définies par l'agent de sécurité. Peut également activer et désactiver certaines fonctions. Ainsi, si l'agent de sécurité a décidé de déployer des cartes Smart Card, l'administrateur informatique peut activer à la fois le mot de passe et le mode Smart Card.
- Utilisateur : utilise les fonctions de sécurité. Ainsi, si l'agent de sécurité et l'administrateur informatique ont activé les cartes Smart Card du système, l'utilisateur peut définir le code PIN de la carte Smart Card et utiliser cette dernière pour l'authentification.

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

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

Gestion de mots de passe HP ProtectTools

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

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

Mot de passe HP ProtectTools	Définition dans le module	Fonction
Mot de passe de connexion Windows	Panneau de configuration Windows® ou HP ProtectTools Security Manager	Peut être utilisé pour la connexion et l'authentification manuelles afin d'accéder aux diverses fonctions de Security Manager.
Security Manager : mot de passe pour la sauvegarde et la restauration	Security Manager, par l'utilisateur individuel	Protège l'accès au fichier de sauvegarde et restauration de Security Manager.

Mot de passe HP ProtectTools	Définition dans le module	Fonction
code PIN de la carte Smart Card	Credential Manager	<p>Peut être utilisé pour une authentification multifacteur.</p> <p>Peut être utilisé pour une authentification Windows.</p> <p>Authentifie les utilisateurs de Drive Encryption, si le jeton de la carte Smart Card est sélectionné.</p>
Mot de passe du jeton Emergency Recovery	Embedded Security, par l'administrateur informatique	Protège l'accès au jeton Emergency Recovery Token, qui est un fichier de sauvegarde de la puce de sécurité intégrée.
Mot de passe propriétaire	Embedded Security, par l'administrateur informatique	Protège le système et la puce TPM contre tout accès non autorisé à toutes les fonctions propriétaires d'Embedded Security.
Mot de passe administrateur BIOS	Computer Setup, par l'administrateur informatique	Protège l'accès à l'utilitaire Computer Setup.

Création d'un mot de passe sécurisé

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

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

Sauvegarde et restauration des informations d'authentification de HP ProtectTools

Vous pouvez utiliser la fonction de sauvegarde et de restauration de HP ProtectTools pour sélectionner et sauvegarder les données et paramètres des informations d'authentification de HP ProtectTools.

2 Mise en route avec l'Assistant de configuration

L'assistant de configuration de Security Manager vous guide lors de l'activation des fonctions de sécurité disponibles qui s'appliquent à tous les utilisateurs de cet ordinateur. Vous pouvez également gérer ces fonctions sur la page Fonctions de sécurité de la console d'administration.

Pour configurer les fonctions de sécurité via l'assistant de configuration de Security Manager :

1. Ouvrez HP ProtectTools Security Manager depuis l'icône du gadget de bureau de HP ProtectTools dans la barre latérale Windows ou l'icône de la barre des tâches dans la zone de notification, à l'extrémité droite de la barre des tâches.



La couleur de la bannière située sur l'icône du gadget de bureau HP ProtectTools indique l'une des conditions suivantes :

- Rouge : HP ProtectTools n'a pas été configuré ou une erreur s'est produite avec l'un des modules de ProtectTools.
- Jaune : Consultez la page Applications Status (État des applications) dans Security Manager pour connaître les modifications à apporter aux paramètres.
- Bleu : HP ProtectTools a été configuré et fonctionne correctement.

Un message s'affiche en bas de l'icône du gadget pour indiquer l'une des conditions suivantes :

- **Configurer maintenant** : l'administrateur doit cliquer sur l'icône du gadget pour exécuter l'assistant d'installation de Security Manager afin de configurer les informations d'authentification de l'ordinateur.

Il s'agit d'une application indépendante.

- **Inscrire maintenant** : un utilisateur doit cliquer sur l'icône du gadget pour exécuter l'assistant de mise en route de Security Manager afin d'inscrire les informations d'authentification.

L'assistant de mise en route s'affiche dans le tableau de bord de Security Manager.

- **Vérifier maintenant** : cliquez sur l'icône du gadget pour afficher des informations supplémentaires sur la page Etat des applications de sécurité.



REMARQUE : L'icône du gadget de bureau de HP ProtectTools n'est pas disponible dans Windows XP.

—ou—

Cliquez sur **Démarrer, Tous les programmes, HP**, puis sur **Console d'administration de HP ProtectTools**. Dans le volet gauche, cliquez sur **Assistant de configuration**.

2. Lisez l'écran de bienvenue, puis cliquez sur **Suivant**.
3. Vérifiez votre identité en tapant votre mot de passe de Windows, puis cliquez sur **Suivant**.

Si vous n'avez pas encore créé de mot de passe Windows, vous êtes invité à le faire. Un mot de passe Windows est nécessaire pour protéger votre compte Windows contre un accès par des utilisateurs non autorisés ; il permet également d'utiliser les fonctions de HP ProtectTools Security Manager.

4. Sur la page SpareKey, sélectionnez trois questions de sécurité, saisissez une réponse pour chaque question, puis cliquez sur **Suivant**.

Vous pouvez sélectionner des questions différentes ou modifier vos réponses sur la page SpareKey, sous **Credential Manager** dans le tableau de bord de Security Manager.



REMARQUE : Cette configuration SpareKey s'applique uniquement à l'utilisateur administrateur.

5. Activez les fonctions de sécurité en sélectionnant les cases à cocher correspondantes, puis cliquez sur **Suivant**.

Plus vous sélectionnez de fonctions, plus votre ordinateur est sécurisé.

 **REMARQUE :** Ces paramètres s'appliquent à tous les utilisateurs. Si certaines cases à cocher ne sont pas sélectionnées, l'assistant de configuration n'invitera pas les utilisateurs à enregistrer ces informations d'authentification.

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

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

6. L'assistant de configuration vous invite à vous inscrire ou à « enregistrer » vos informations d'authentification.

Si ni le lecteur d'empreintes digitales, ni une Smart Card, ni une webcam ne sont disponibles, vous êtes invité à saisir votre mot de passe Windows. Après l'inscription, vous devrez utiliser des informations d'authentification enregistrées pour vérifier votre identité à chaque fois qu'une authentification sera requise.

 **REMARQUE :** L'enregistrement de ces informations d'authentification s'applique uniquement à l'utilisateur administrateur.

7. Sur la dernière page de l'assistant, cliquez sur **Terminer**.

La page d'accueil du tableau de bord de Security Manager s'affiche.

3 Console d'administration de HP ProtectTools Security Manager

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

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

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

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

Ouverture de la console d'administration de HP ProtectTools

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

- ▲ Cliquez successivement sur **Démarrer**, **Tous les programmes**, **HP** et **Console d'administration de HP ProtectTools**.

– ou –

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

Utilisation de la console d'administration

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

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

- ou -

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

La console se compose des éléments suivants :

- **Accueil** : vous permet de configurer les options de sécurité suivantes :
 - **Accroître la sécurité du système**
 - **Exiger une authentification forte**
 - **Gérer les utilisateurs HP ProtectTools**
 - **Voyez comment vous pouvez gérer HP ProtectTools de manière centralisée**
 - **Système** : permet de configurer les fonctions de sécurité suivantes et l'authentification pour les utilisateurs et les périphériques :
 - **Sécurité**
 - **Utilisateurs**
 - **Informations d'authentification**
 - **Applications** : vous permet de configurer les paramètres de HP ProtectTools Security Manager et des applications de Security Manager.
 - **Données** : propose un menu expansible de liens vers les applications de Security Manager qui protègent vos données.
 - **Gestion centrale** : affiche des onglets pour accéder à des solutions, des mises à jour du produit et des messages supplémentaires.
 - **Assistant de configuration** : vous guide au cours des étapes de configuration de HP ProtectTools Security Manager.
 - **A propos de** : affiche des informations sur HP ProtectTools Security Manager, telles que le numéro de version et les informations sur les droits d'auteur.
 - **Zone principale** : affiche les écrans spécifiques aux applications.
- ? : affiche l'aide logicielle de la console d'administration. Cette icône se trouve dans la partie supérieure droite du cadre de la fenêtre, à côté des icônes d'agrandissement et de réduction.

Configuration de votre système

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

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

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

Configuration de l'authentification pour votre ordinateur

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

Pour configurer l'authentification sur votre ordinateur :

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

Règles de connexion

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

1. Dans le panneau gauche de la console d'administration, cliquez sur **Sécurité**, puis sur **Authentification**.
2. Dans l'onglet **Règles de connexion**, cliquez sur la flèche vers le bas, puis sélectionnez une catégorie d'utilisateur :
 - **Pour les administrateurs de cet ordinateur**
 - **Pour les utilisateurs autres que les administrateurs**
3. Spécifiez les informations d'authentification requises pour la catégorie d'utilisateur sélectionnée.
4. Indiquez si UNE des informations d'authentification spécifiées est requise ou si TOUTES sont requises afin d'authentifier un utilisateur.
5. Cliquez sur **Appliquer**.

Règles de session

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

1. Dans le panneau gauche de la console d'administration, cliquez sur **Sécurité**, puis sur **Authentification**.
2. Dans l'onglet **Règles de session**, cliquez sur la flèche vers le bas, puis sélectionnez une catégorie d'utilisateur :
 - **Pour les administrateurs de cet ordinateur**
 - **Pour les utilisateurs autres que les administrateurs**
3. Cliquez sur la flèche vers le bas, puis sélectionnez les informations d'authentification requises pour la catégorie d'utilisateur sélectionnée :
 - **Exige l'une des informations d'authentification spécifiées**
 **REMARQUE :** Décochez les cases à cocher, car toutes les informations d'authentification ont le même effet que la sélection de l'option **Ne demande pas d'authentification**.
 - **Exige toutes les informations d'authentification spécifiées**
 - **N'exige pas d'authentification** : en sélectionnant cette option, vous effacez toutes les informations d'authentification de la fenêtre.
4. Cliquez sur **Appliquer**.

Paramètres

1. Sélectionnez la case à cocher pour activer le paramètre suivant, ou désélectionnez-la pour le désactiver :

Autoriser la connexion directe : permet aux utilisateurs de cet ordinateur d'ignorer la connexion Windows si l'authentification a été effectuée au niveau du BIOS ou du disque crypté.
2. Cliquez sur **Appliquer**.

Gestion des utilisateurs

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

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

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

- Pour ajouter des utilisateurs supplémentaires, cliquez sur **Ajouter**.
- Pour supprimer un utilisateur, cliquez sur celui-ci, puis sur **Supprimer**.

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

Informations d'authentification

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

SpareKey

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

1. Sélectionnez la case à cocher pour activer ou désélectionnez-la pour désactiver l'utilisation de l'authentification SpareKey pour la connexion Windows.
2. Sélectionnez les questions de sécurité qui seront posées aux utilisateurs lors de leur inscription à SpareKey. Vous pouvez définir jusqu'à trois questions personnalisées ou vous pouvez permettre aux utilisateurs de saisir leur propre phrase de passe.
3. Cliquez sur **Appliquer**.

Empreintes digitales

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

- **Inscription** : choisissez le nombre minimum et maximum d'empreintes digitales qu'un utilisateur est autorisé à enregistrer.

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

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

- **Sensibilité** : Déplacez le glisseur pour ajuster la sensibilité utilisée par le lecteur d'empreinte digitale lorsqu'il passe vos empreintes digitales.

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

- **Avancé** : sélectionnez une des options suivantes pour configurer le lecteur d'empreintes digitales afin qu'il économise de l'énergie et améliore le retour visuel :
 - **Optimisé** : le lecteur d'empreintes digitales est activé lorsque cela s'avère nécessaire. Vous pourrez constater un court délai lorsque le lecteur est utilisé pour la première fois.
 - **Economie d'énergie** : le lecteur d'empreintes digitales est plus lent à répondre, mais le paramètre nécessite moins d'énergie.
 - **Mode normal** : le lecteur d'empreintes digitales est toujours prêt à être utilisé, mais ce paramètre utilise un maximum d'énergie.

Smart Card

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

- **Paramètres** : configurez l'ordinateur pour qu'il se verrouille automatiquement lorsqu'une Smart Card est retirée.

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

- **Administration** : sélectionnez parmi les options suivantes :
 - **Initialiser la Smart Card** : prépare une Smart Card pour une utilisation avec HP ProtectTools. Si une Smart Card a été précédemment initialisée en dehors de HP ProtectTools (avec une paire de clés asymétriques et un certificat associé), elle n'a pas besoin d'être initialisée à nouveau, sauf si une initialisation avec un certificat spécifique est nécessaire.
 - **Modifier le code PIN de la Smart Card** : vous permet de modifier le code PIN utilisé avec la Smart Card.

- **Effacer uniquement les données HP ProtectTools** : efface uniquement le certificat HP ProtectTools créé lors de l'initialisation de la carte. Aucune autre donnée ne sera effacée de la carte.
- **Effacer toutes les données de la Smart Card** : efface toutes les données de la Smart Card spécifiée. Vous ne pourrez plus utiliser la carte avec HP ProtectTools ou toute autre application.



REMARQUE : Les fonctions qui ne sont pas prises en charge par votre Smart Card ne sont pas disponibles.

- ▲ Cliquez sur **Appliquer**.

Visage

Si une webcam est installée ou connectée à l'ordinateur, et si le programme Face Recognition est installé, vous pouvez définir le niveau de sécurité de Face Recognition pour rechercher un équilibre entre convivialité et sécurité de l'ordinateur.

1. Cliquez sur **Démarrer, Tous les programmes, HP**, puis sur **Console d'administration de HP ProtectTools**.
2. Cliquez sur **Informations d'authentification**, puis sur **Visage**.
3. Pour plus de convivialité, cliquez sur le curseur pour le déplacer vers la gauche, ou pour plus de précision, cliquez sur le curseur pour le déplacer vers la droite.
 - **Convivialité** : pour faciliter l'accès aux utilisateurs inscrits dans des situations marginales, cliquez sur la barre du curseur pour le déplacer vers la position **Convivialité**.
 - **Equilibre** : pour assurer un bon compromis entre sécurité et convivialité, ou si vous disposez d'informations sensibles ou que votre ordinateur est située dans une zone où des accès non autorisés peuvent avoir lieu, cliquez sur la barre du curseur pour le déplacer vers la position **Equilibre**.
 - **Précision** : pour rendre plus difficile l'accès aux utilisateurs si les scènes enregistrées ou les conditions d'éclairage en cours se situent à un niveau inférieur à la normale et qu'il est peu probable qu'une acceptation erronée ne se produise, cliquez sur la barre du curseur pour le déplacer vers la position **Précision**.
4. Cliquez sur **Avancé**, puis configurez une sécurité supplémentaire. Pour plus d'informations, reportez-vous à la section [Paramètres utilisateur avancés à la page 42](#).
5. Cliquez sur **Appliquer**.

Configuration de vos applications

Vous pouvez utiliser l'option Paramètres pour personnaliser le comportement des applications de HP ProtectTools Security Manager actuellement installées.

Pour modifier vos paramètres d'application :

1. Dans le panneau gauche de la console d'administration, sous **Applications**, cliquez sur **Paramètres**.
2. Sélectionnez la case à cocher en regard d'un paramètre spécifique pour l'activer ou désélectionnez-la pour le désactiver.
3. Cliquez sur **Appliquer**.

onglet Général

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

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

Onglet Applications

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

- **Etat des applications** : permet d'afficher l'état de toutes les applications.
- **Gestionnaire de mots de passe** : active le Gestionnaire de mots de passe pour tous les utilisateurs de l'ordinateur.
- **Privacy Manager** : active Privacy Manager pour tous les utilisateurs de l'ordinateur.
- **Activer le lien Gestion centrale** : permet à tous les utilisateurs de cet ordinateur d'ajouter des applications à HP ProtectTools Security Manager en cliquant sur le bouton **Gestion centrale**.

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

Gestion centrale

Des applications supplémentaires peuvent être disponibles pour l'ajout de nouveaux outils de gestion à Security Manager. L'administrateur de cet ordinateur peut désactiver cette fonction sur la page Paramètres. La page Gestion centrale comporte deux onglets :

- **Solutions pour les professionnels** : si vous disposez d'une connexion Internet, vous pouvez accéder au site Web de DigitalPersona (<http://www.digitalpersona.com/>) pour y rechercher de nouvelles applications.
- **Mises à jour et messages**
 - Pour demander des informations sur des nouvelles applications et des mises à jour, cochez la case **Me tenir informé des nouvelles applications et des mises à jour**.
 - Pour planifier des mises à jour automatiques, sélectionnez le nombre de jours.
 - Pour vérifier l'existence de mises à jour, cliquez sur **Vérifier maintenant**.

4 HP ProtectTools Security Manager

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

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

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

Ouverture de Security Manager

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

- Cliquez successivement sur **Démarrer, Tous les programmes, HP**, puis sur **HP ProtectTools Security Manager**.
- Double-cliquez sur l'icône **HP ProtectTools** dans la zone de notification, à l'extrémité droite de la barre des tâches.
- Cliquez avec le bouton droit de la souris sur l'icône **HP ProtectTools**, puis sur **Ouvrir HP ProtectTools Security Manager**.
- Cliquez sur l'icône du gadget de bureau **HP ProtectTools**.
- Appuyez sur la combinaison de touches d'activation **ctrl** + touche logo Windows + **h** pour ouvrir le menu **Liens rapides de Security Manager**.

Pour plus d'informations sur la modification de la combinaison de touches d'activation, reportez-vous à la section [Paramètres à la page 37](#).

Utilisation du tableau de bord de Security Manager

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

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

Le tableau de bord affiche les éléments suivants :

- **Carte d'identité** : affiche le nom d'utilisateur Windows et une image sélectionnée identifiant le compte utilisateur connecté.
- **Applications de sécurité** : affiche un menu expansible des liens de configuration des catégories de sécurité suivantes :
 - **Accueil** : permet de gérer les mots de passe, de configurer les informations d'authentification ou de vérifier l'état des applications de sécurité.
 - **Etat** : permet de vérifier l'état des applications de sécurité HP ProtectTools.



REMARQUE : Les applications qui ne sont pas installées sur l'ordinateur ne sont pas affichées dans la liste suivante.

- **My Logons** (Mes connexions) : permet de gérer les informations d'authentification avec le Gestionnaire de mots de passe, Credential Manager, Mot de passe, SpareKey, Smart Card, Visage et Empreinte.
- **Mes données** : permet de gérer la sécurité des données avec Drive Encryption et File Sanitizer.
- **Poste de travail** : permet de gérer la sécurité de l'ordinateur avec Device Access Manager.
- **Mes communications** : permet de gérer la sécurité des communications avec Privacy Manager.
- **Administration** : permet aux administrateurs d'accéder aux options suivantes :
 - **Console d'administration** : permet aux administrateurs de gérer la sécurité et les utilisateurs.
 - **Central Management** (Gestion centrale) : permet aux administrateurs d'accéder à des solutions, des mises à jour du produit et des messages supplémentaires.
- **Avancé** : affiche les commandes permettant d'accéder à des fonctions supplémentaires, notamment :
 - **Préférences** : vous permet de personnaliser les paramètres de Security Manager.
 - **Sauvegarder et restaurer** : vous permet de sauvegarder ou de restaurer les données.
 - **A propos de** : affiche des informations sur HP ProtectTools Security Manager, telles que le numéro de version et les informations sur les droits d'auteur.
- **Zone principale** : affiche les écrans spécifiques aux applications.
- **?** : affiche l'aide logicielle de Security Manager. Cette icône se trouve en haut à droite de la fenêtre, en regard des icônes d'agrandissement et de réduction.

Etat des applications de sécurité

Vous pouvez afficher l'état des applications de sécurité installées à deux emplacements :

- **Le gadget de bureau HP ProtectTools**

La couleur de la bannière située en haut de l'icône du gadget HP ProtectTools change en fonction de l'état de sécurité global des applications de sécurité installées.

- **Rouge** : avertissement
- **Jaune** : attention, non configuré
- **Bleu** : ok

Un message s'affiche en bas de l'icône du gadget pour indiquer l'une des conditions suivantes :

- **Configurer maintenant** : l'administrateur doit cliquer sur l'icône du gadget pour exécuter l'assistant d'installation de Security Manager afin de configurer les informations d'authentification de l'ordinateur.

Il s'agit d'une application indépendante.
 - **Inscrire maintenant** : un utilisateur doit cliquer sur l'icône du gadget pour exécuter l'assistant de mise en route de Security Manager afin d'inscrire les informations d'authentification.

L'assistant de mise en route s'affiche dans le tableau de bord de Security Manager.
 - **Vérifier maintenant** : cliquez sur l'icône du gadget pour afficher des informations supplémentaires sur la page Etat des applications de sécurité.
- **Page Etat des applications de sécurité** : cliquez sur **Etat** dans le tableau de bord de Security Manager pour afficher l'état global des applications de sécurité installées, ainsi que l'état spécifique de chaque application.

My Logons (Mes connexions)

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

- **Gestionnaire de mots de passe** : crée et gère les liens rapides, ce qui vous permet de lancer et de vous connecter à des sites Web et des programmes en vous authentifiant avec votre mot de passe Windows, votre empreinte digitale ou une Smart Card.
- **Credential Manager** : fournit un moyen de changer aisément votre mot de passe Windows, d'inscrire vos empreintes digitales ou de configurer une Smart Card.

Les administrateurs peuvent ajouter davantage d'applications en cliquant sur **Administration**, puis sur **Central Management** (Gestion centrale) dans le coin inférieur gauche du tableau de bord.

Gestionnaire de mots de passe

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

Le Gestionnaire de mots de passe offre les options suivantes :

- Ajout, modification ou suppression des connexions de l'onglet **Gérer**.
- Utiliser des liens rapides afin de lancer le navigateur par défaut et de vous connecter à tout site Web ou programme après sa configuration.
- Glisser-déposer pour organiser vos liens rapides en catégories.
- Voir d'un seul coup d'œil si certains de vos mots de passe présentent un risque de sécurité et générer automatiquement un mot de passe fort complexe à utiliser pour de nouveaux sites.

L'icône **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. Lorsqu'aucune connexion n'a été créée pour ce site Web ou cette application, un signe plus s'affiche sur l'icône.

- ▲ Cliquez sur l'icône **Gestionnaire de mots de passe** pour afficher un menu contextuel dans lequel vous pouvez choisir parmi les options suivantes.

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

Les options suivantes s'affichent dans le menu contextuel :

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

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

Les options suivantes s'affichent dans le menu contextuel :

- **Remplir les données de connexion** : place vos données de connexion dans les champs de connexion, puis soumet la page (si la soumission a été spécifiée lors de la création de la connexion ou de sa dernière modification).
- **Modifier la connexion** : vous permet de modifier les données de connexion pour ce site Web.
- **Ajouter une connexion** : permet d'ajouter un compte à une connexion.
- **Ouvrir le Gestionnaire de mots de passe** : lance le Gestionnaire de mots de passe.
- **Aide** : affiche l'aide logicielle de Security Manager.



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

Ajout de connexions

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

Pour ajouter une connexion :

1. Ouvrez l'écran de connexion d'un site Web ou d'un programme.
2. Cliquez sur la flèche située sur l'icône **Gestionnaire de mots de passe**, puis cliquez sur l'une des options suivantes en fonction de l'écran de connexion affiché (site Web ou programme) :
 - Pour un site Web, cliquez sur **Ajouter [nom de domaine] au Gestionnaire de mots de passe**.
 - Pour un programme, cliquez sur **Ajouter cet écran de connexion au Gestionnaire de mots de passe**.
3. Saisissez vos données de connexion. Les champs de connexion à l'écran, et leurs champs correspondant dans la boîte de dialogue, sont identifiés par un liseré orange en gras. Vous pouvez aussi afficher cette boîte de dialogue en cliquant sur **Ajouter connexion** à partir de l'onglet **Gérer le gestionnaire de Mot de passe**. Certaines options dépendent des appareils de sécurité connectés à l'ordinateur (par exemple, au moyen de la touche d'activation **ctrl**+ touche logo Windows **+h**, faire glisser votre empreinte digitale ou insérer une carte à puce).
 - a. Pour remplir un champ de connexion avec l'un des choix préformatés, cliquez sur les flèches à droite du champ.
 - b. Pour consulter le mot de passe de cette connexion, cliquez sur **Afficher le mot de passe**.
 - c. Pour que les données des champs de connexion soient fournies sans être envoyées, désactivez la case à cocher **Envoyer automatiquement les données de connexion**.
 - d. Pour activer la sécurité VeriSign VIP, sélectionnez la case à cocher **I want VIP security on this site** (Je veux une sécurité VIP sur ce site).

Cette option apparaît uniquement pour les sites pour lesquels VeriSign Identity Protection (VIP) est disponible. Lorsque cette option est prise en charge par le site, vous pouvez également choisir de saisir automatiquement votre code de sécurité VIP, en plus de votre méthode d'authentification habituelle.

- e. Cliquez sur **OK**, sur la méthode d'authentification à utiliser (empreintes, mot de passe ou visage), 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.

- f. Si le Gestionnaire de mots de passe ne détecte aucun champ de connexion, cliquez sur **Plus de champs**.
 - Cochez la case de chaque champ obligatoire pour la connexion ou décochez la case des champs qui ne sont pas obligatoires pour effectuer l'opération.
 - Si le Gestionnaire de mots de passe détecte tous les champs de connexion, un message vous demande si vous souhaitez continuer. Cliquez sur **Oui**.
 - Une boîte de dialogue s'ouvre avec les champs de connexion remplis. Cliquez sur l'icône de chaque champ et faites-la glisser vers le champ de connexion approprié. Cliquez ensuite sur le bouton pour accéder au site Web.

 **REMARQUE :** Une fois que vous utilisez le mode manuel pour la saisie des données de connexion à un site, vous devez continuer à utiliser cette méthode pour accéder à nouveau à ce site.

REMARQUE : Le mode manuel n'est disponible qu'avec Internet Explorer 8.

- Cliquez sur **Fermer**.

A chaque fois que vous accédez à ce site Web ou ouvrez ce programme, l'icône **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 les informations d'authentification enregistrées pour vous connecter.

Modification des connexions

Pour modifier une connexion, procédez comme suit :

1. Ouvrez l'écran de connexion d'un site Web ou d'un programme.
2. Pour afficher une boîte de dialogue dans laquelle vous pouvez modifier vos informations de connexion, cliquez sur la flèche située sur l'icône **Gestionnaire de mots de passe**, puis cliquez sur **Modifier la connexion**. A l'écran, les champs de connexion et les champs correspondants de la boîte de dialogue sont identifiés par une bordure orange en gras.

Vous pouvez également afficher la boîte de dialogue en cliquant sur **Modifier pour obtenir la connexion souhaitée** dans l'onglet **Gestion par le Gestionnaire de mots de passe**.

3. Modifiez vos informations de connexion.
 - Pour sélectionner un champ de connexion **Nom d'utilisateur** avec l'un des choix préformatés, cliquez sur la flèche vers le bas à droite du champ.
 - Pour sélectionner un champ de connexion **Mot de passe** avec l'un des choix préformatés, cliquez sur la flèche vers le bas à droite du champ.

- Pour activer la sécurité VeriSign VIP, sélectionnez la case à cocher **I want VIP security on this site** (Je veux une sécurité VIP sur ce site).

Cette option apparaît uniquement pour les sites pour lesquels la sécurité VeriSign VIP est disponible. Lorsque cette option est prise en charge par le site, vous pouvez également choisir de saisir automatiquement votre code de sécurité VIP, en plus de votre méthode d'authentification habituelle.

- Pour ajouter des champs de connexion dans l'écran, cliquez sur **Plus de champs**.
- Pour consulter le mot de passe de cette connexion, cliquez sur **Afficher le mot de passe**.
- Pour que les données des champs de connexion soient fournies sans être envoyées, désactivez la case à cocher **Envoyer automatiquement les données de connexion**.

4. Cliquez sur **OK**.

Utilisation du menu des connexions

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

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

Pour afficher le menu **Connexions** :

1. Appuyez sur la combinaison de touches d'activation du **Gestionnaire de mots de passe** (**ctrl** + touche logo Windows + **h** est le paramètre défini en usine). Pour modifier la combinaison de touches d'activation, cliquez sur **Gestionnaire de mots de passe**, puis sur **Paramètres** dans le tableau de bord de Security Manager.
2. Faites glisser votre empreinte digitale (sur ordinateurs avec un lecteur d'empreinte digitale incorporé ou connecté), ou saisissez votre mot de passe Windows.

Organisation des connexions en catégories

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

Pour ajouter une catégorie :

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

Pour ajouter une connexion à une catégorie :

1. Placez le pointeur de la souris au-dessus de la connexion concernée.
2. Appuyez sur le bouton gauche de la souris et maintenez-le enfoncé.

3. Faites glisser la connexion dans la liste des catégories. Les catégories sont mises en surbrillance à mesure que vous déplacez le pointeur de la souris dessus.
4. Relâchez le bouton de la souris une fois la catégorie qui vous intéresse sélectionnée.

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

Gestion de vos connexions

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.

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

Pour gérer vos connexions :

- ▲ Dans le tableau de bord de Security Manager, cliquez sur **Gestionnaire de mots de passe**, puis sur l'onglet **Gérer**.
 - **Pour ajouter une connexion** : cliquez sur **Ajouter une connexion** et suivez les instructions à l'écran.
 - **Vos connexions** : cliquez sur une connexion existante, sélectionnez l'une des options suivantes, puis suivez les instructions à l'écran :
 - **Ouvrir** : permet d'ouvrir un site Web ou un programme pour lequel il existe une connexion.
 - **Ajouter** : permet d'ajouter une connexion. Pour plus d'informations, reportez-vous à la section [Ajout de connexions à la page 31](#).
 - **Modifier** : permet de modifier une connexion. Pour plus d'informations, reportez-vous à la section [Modification des connexions à la page 32](#).
 - **Supprimer** : permet de supprimer un site Web ou un programme pour lequel il existe une connexion.
 - **Ajouter une catégorie** : cliquez sur **Ajouter une catégorie**, puis suivez les instructions à l'écran. Pour plus d'informations, reportez-vous à la section [Organisation des connexions en catégories à la page 33](#).

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

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

Evaluation de la force de votre mot de passe

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

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

Paramètres de l'icône du Gestionnaire de mots de passe

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

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

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

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

- Lorsque la connexion au site Web ou la page du programme précédemment exclu s'affiche, ouvrez le tableau de bord de Security Manager, puis cliquez sur **Gestionnaire de mots de passe**.

- Cliquez sur **Ajouter une connexion**.

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

- Cliquez sur **Continuer**.

L'écran Ajouter une connexion au Gestionnaire de mots de passe s'affiche.

- Suivez les instructions à l'écran. Pour plus d'informations, reportez-vous à la section [Ajout de connexions à la page 31](#).
- L'icône **Gestionnaire de mots de passe** s'affiche à chaque fois que la connexion à ce site Web ou l'écran de ce programme est ouvert.

2. Sélectionnez la case à cocher pour désactiver l'option d'affichage d'une invite d'ajout de connexions à des écrans de connexion.

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

VeriSign Identity Protection (VIP)

Vous pouvez créer des jetons d'accès à VeriSign VIP à utiliser avec les sites Web compatibles. Ces jetons sont utilisés par le Gestionnaire de mots de passe pour créer des connexions automatisées incluant l'utilisation des jetons déplacés vers les écrans de connexion compatibles ou entrés manuellement dans des champs spécifiques.

Vous pouvez activer VeriSign VIP et créer un jeton depuis le tableau de bord de Security Manager ou dans un site Web compatible. Afin d'utiliser le jeton, vous devez l'enregistrer sur chaque site Web dans lequel il sera utilisé.

Après avoir enregistré et utilisé une première fois un jeton, il peut (éventuellement) être indexé et soumis à vos informations de connexion habituelles. Pour les sites n'autorisant pas l'indexation d'un jeton, vous pouvez le faire glisser ou entrer manuellement ses informations.

Pour activer VeriSign VIP et créer un jeton depuis le tableau de bord de Security Manager :

1. Ouvrez le tableau de bord de Security Manager. Pour plus d'informations, reportez-vous à la section [Ouverture de Security Manager à la page 27](#).
2. Cliquez sur **Gestionnaire de mots de passe**, puis sur **VIP**.
3. Cliquez sur **Get VIP**.

Un jeton VeriSign VIP est créé et s'affiche sur la page VeriSign VIP. Celui-ci s'affichera désormais à chaque fois que vous accéderez à cette page.

Pour activer VeriSign VIP et créer un jeton depuis un site Web :

1. Le Gestionnaire de mots de passe vous alerte à chaque fois que vous consultez un site Web compatible avec VeriSign VIP.
2. Créez une connexion pour l'écran. Pour plus d'informations, reportez-vous à la section [Ajout de connexions à la page 31](#).
3. Dans la boîte de dialogue Créer une connexion, sélectionnez **I want additional account protection with VIP** (Je souhaite une protection supplémentaire du compte avec VIP).

Pour enregistrer un jeton VeriSign VIP pour un site Web :

1. Connectez-vous à un site Web compatible avec VeriSign VIP manuellement ou à l'aide d'une connexion du Gestionnaire de mots de passe.
2. Cliquez sur la bulle VeriSign VIP qui s'affiche afin de créer une connexion pour ce site.
3. Dans la boîte de dialogue Ajouter une connexion au Gestionnaire de mots de passe, sélectionnez **I want VIP security on this site** (Je veux une sécurité VIP sur ce site).

Cette option apparaît uniquement pour les sites pour lesquels la sécurité VeriSign VIP est disponible. Lorsque cette option est prise en charge par le site, vous pouvez également choisir de saisir automatiquement votre code de sécurité VIP, en plus de votre méthode d'authentification habituelle.

Paramètres

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

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

Credential Manager

Vous utilisez les informations d'authentification de Security Manager pour confirmer qu'il s'agit bien de vous. L'administrateur de cet ordinateur peut configurer les informations d'authentification à utiliser pour prouver votre identité lors de la connexion à votre compte Windows, à des sites Web ou à des programmes.

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

- Mot de passe
- SpareKey
- Empreintes digitales
- Smart Card
- Visage

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

Changement de votre mot de passe Windows

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

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

1. Dans le tableau de bord de Security Manager, cliquez sur **Credential Manager**, puis sur **Mot de passe**.
2. Saisissez votre mot de passe actuel dans la zone de texte **Mot de passe Windows actuel**.

3. Saisissez un nouveau mot de passe dans la zone de texte **Nouveau mot de passe Windows**, puis entrez-le à nouveau dans la zone de texte **Confirmer le nouveau mot de passe**.
4. Cliquez sur **Modifier** pour remplacer immédiatement votre mot de passe actuel par celui que vous venez de saisir.

Configuration d'une SpareKey

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

HP ProtectTools Security Manager vous invite à configurer votre SpareKey personnelle lors de l'installation initiale dans l'assistant de mise en route.

Pour configurer votre SpareKey :

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

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

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

Inscription des empreintes digitales

Si l'ordinateur dispose d'un lecteur d'empreintes digitales intégré ou connecté, HP ProtectTools Security Manager vous invite à configurer ou "inscrire" vos empreintes digitales lors de l'installation initiale dans l'assistant de mise en route. Vous pouvez également inscrire vos empreintes digitales dans la page Empreinte, sous **Credential Manager** dans le tableau de bord de Security Manager.

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



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

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

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

Configuration d'une Smart Card

Les administrateurs doivent initialiser et enregistrer la Smart Card avant de pouvoir l'utiliser pour l'authentification.

Initialisation de la Smart Card

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



REMARQUE : Le logiciel ActivIdentity doit être installé.

1. Insérez la carte dans le lecteur.
2. Cliquez sur **Démarrer, Tous les programmes**, puis sur **ActivClient PIN Initialization Tool** (Outil d'initialisation du code PIN d'ActivIdentity).
3. Saisissez et confirmez un code PIN.
4. Cliquez sur **Suivant**.

Le logiciel de la Smart Card fournira une clé de déverrouillage. La plupart des Smart Card se verrouillent si le code PIN n'est pas saisi correctement 5 fois. La clé est utilisée pour déverrouiller la carte.

5. Cliquez sur **Démarrer, Tous les programmes, HP**, puis sur **Console d'administration de HP ProtectTools**.
6. Cliquez sur **Informations d'authentification**, puis sur **Smart Card**.
7. Cliquez sur l'onglet **Administration**.
8. Assurez-vous de sélectionner l'option **Configurer une Smart Card**.
9. Saisissez votre code PIN, cliquez sur **Appliquer**, puis suivez les instructions à l'écran.
10. Après avoir correctement initialisé la Smart Card, vous devrez l'enregistrer.

Enregistrement de la Smart Card

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

1. Sous **Central Management** (Gestion centrale), cliquez sur **Assistant d'installation**.
2. Dans la page Bienvenue, cliquez sur **Suivant**, puis saisissez le mot de passe Windows.
3. Dans la page SpareKey, cliquez sur **Skip SpareKey Setup** (Ignorer la configuration SpareKey) (sauf si vous souhaitez mettre à jour les informations SpareKey).
4. Dans la page Activez les fonctions de sécurité, cliquez sur **Suivant**.
5. Dans la page Choisissez vos informations d'authentification, assurez-vous de sélectionner l'option **Set up your smart card** (Configurer la Smart Card), puis cliquez sur **Suivant**.
6. Dans la page Smart Card, saisissez votre code PIN, puis cliquez sur **Suivant**.
7. Cliquez sur **Terminer**.

Les utilisateurs peuvent également enregistrer une Smart Card dans Security Manager. Pour plus d'informations, reportez-vous à l'aide du logiciel Security Manager for HP ProtectTools.

Configuration de la Smart Card

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

- **Paramètres** : configurez l'ordinateur pour qu'il se verrouille automatiquement lorsqu'une Smart Card est retirée.

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

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

 **REMARQUE :** Les fonctions qui ne sont pas prises en charge par votre Smart Card ne sont pas disponibles.

- ▲ Cliquez sur **Appliquer**.

Inscription de scènes pour la connexion par reconnaissance faciale

Si l'ordinateur dispose d'une webcam intégrée ou connectée, HP ProtectTools Security Manager vous invite à configurer ou "inscrire" vos scènes lors de l'installation initiale dans l'assistant de mise en route. Vous pouvez également inscrire vos scènes dans la page de connexion Visage, sous **Credential Manager** dans le tableau de bord de Security Manager.

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

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

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

Pour inscrire une scène depuis l'assistant de mise en route :

1. Dans la page Visage de l'assistant, cliquez sur **Avancé**, puis configurez une sécurité supplémentaire. Pour plus d'informations, reportez-vous à la section [Paramètres utilisateur avancés à la page 42](#).
2. Cliquez sur **OK**.
3. Cliquez sur **Démarrer** ou sur **Inscrire une nouvelle scène** si vous avez déjà inscrit des scènes.
4. Si vous n'avez sélectionné aucune option de sécurité supplémentaire, vous êtes invité à sélectionner une option de sécurité supplémentaire. Suivez les instructions à l'écran, puis cliquez sur **Suivant**. Pour plus d'informations, reportez-vous à la section [Paramètres utilisateur avancés à la page 42](#).
5. Cliquez sur l'icône **Caméra**, puis suivez les instructions à l'écran pour inscrire votre scène.
Suivez les instructions à l'écran et veillez à regarder votre image lors de la capture des scènes.
6. Cliquez sur **Suivant**.
7. Cliquez sur **Terminer**.

Vous pouvez également inscrire des scènes depuis le tableau de bord de Security Manager :

1. Ouvrez le tableau de bord de Security Manager. Pour plus d'informations, reportez-vous à la section [Ouverture de Security Manager à la page 27](#).
2. Sous **My Logons** (Mes connexions), cliquez sur **Credential Manager**, puis sur **Visage**.
3. Cliquez sur **Avancé**, puis configurez une sécurité supplémentaire. Pour plus d'informations, reportez-vous à la section [Paramètres utilisateur avancés à la page 42](#).
4. Cliquez sur **OK**.
5. Cliquez sur **Démarrer** ou sur **Inscrire une nouvelle scène** si vous avez déjà inscrit des scènes.
6. Si vous n'avez sélectionné aucune option de sécurité supplémentaire, vous êtes invité à sélectionner une option de sécurité supplémentaire. Suivez les instructions à l'écran, puis cliquez sur **Suivant**. Pour plus d'informations, reportez-vous à la section [Paramètres utilisateur avancés à la page 42](#).
7. Cliquez sur l'icône **Caméra**, puis suivez les instructions à l'écran pour inscrire votre scène.
Suivez les instructions à l'écran et veillez à regarder votre image lors de la capture des scènes.

Pour plus d'informations, reportez-vous à l'aide du logiciel Face Recognition en cliquant sur le ? bleu situé dans la partie supérieure droite de la page de connexion Visage.

Paramètres utilisateur avancés

Ces options s'affichent également sur la page Sécurité supplémentaire si aucune sécurité supplémentaire n'a été sélectionnée.

1. Ouvrez le tableau de bord de Security Manager. Pour plus d'informations, reportez-vous à la section [Ouverture de Security Manager à la page 27](#).
2. Sous **My Logons** (Mes connexions), cliquez sur **Credential Manager**, puis sur **Visage**.
3. Cliquez sur **Avancé** pour configurer les options de sécurité suivantes :
 - a. Onglet **Sécurité** : sélectionnez l'une des options suivantes :
 - **Pas de sécurité supplémentaire** : sélectionnez cette option si vous ne souhaitez pas ajouter une sécurité supplémentaire pour la connexion par reconnaissance faciale.
 - **Utiliser un code PIN pour plus de sécurité** : sélectionnez cette option pour demander un code PIN spécifique à l'utilisateur pour la connexion par reconnaissance faciale.
 - Cliquez sur **Créer le code PIN**.
 - Saisissez votre mot de passe Windows.
 - Entrez le nouveau code PIN, puis confirmez-le en le saisissant à nouveau.

Une fois le code PIN créé, vous pouvez sélectionner l'une des options suivantes : **Modifier**, **Réinitialiser** ou **Supprimer un code PIN**.
 - **Utiliser un périphérique Bluetooth pour plus de sécurité** : sélectionnez cette option pour établir une connexion entre votre téléphone équipé du Bluetooth et Face Recognition. Lors de la connexion Windows, une fois votre visage authentifié, Face Recognition vérifie également la présence du téléphone connecté en Bluetooth. S'il est présent (et que le Bluetooth est activé), vous êtes autorisé à vous connecter à Windows.
 - Vérifiez que le Bluetooth est activé sur l'ordinateur et sur le téléphone.

Si aucun téléphone compatible Bluetooth n'est présent, vous êtes invité à activer le téléphone connecté en Bluetooth et à relancer le processus de connexion. Après 30 secondes, la fenêtre de connexion à Face Recognition est suspendue. Pour lancer le processus de connexion, cliquez sur l'icône **Caméra**. En cas d'absence du téléphone compatible Bluetooth, vous pouvez vous connecter à l'aide de votre mot de passe Windows habituel.
 - Cliquez sur **Ajouter**.
 - Lorsque votre périphérique Bluetooth s'affiche, sélectionnez-le, puis cliquez sur **Suivant**.

Cliquez sur **OK**.

b. Onglet **Autres paramètres** : sélectionnez les cases à cocher correspondantes pour activer les options suivantes ou désélectionnez la case à cocher pour désactiver une option. Ces paramètres s'appliquent uniquement à l'utilisateur actuel.

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

Cliquez sur **OK**.

Votre carte d'identité personnelle

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

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

Pour changer le nom affiché :

1. Ouvrez le tableau de bord de Security Manager. Pour plus d'informations, reportez-vous à la section [Ouverture de Security Manager à la page 27](#).
2. Cliquez sur la carte d'identification dans le coin supérieur gauche du tableau de bord.
3. Cliquez sur la zone affichant votre nom d'utilisateur Windows pour ce compte, entrez le nouveau nom, puis cliquez sur **Enregistrer**.

Pour changer la photo affichée :

1. Ouvrez le tableau de bord de Security Manager. Pour plus d'informations, reportez-vous à la section [Ouverture de Security Manager à la page 27](#).
2. Cliquez sur la carte d'identification dans le coin supérieur gauche du tableau de bord.
3. Cliquez sur **Choisir une image**, sur une image, puis sur **Enregistrer**.

Définition de vos préférences

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

Onglet Général

Apparence : affiche l'icône dans la zone de notification de la barre des tâches

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

Onglet Empreinte



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

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

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

- **Retour d'empreinte digitale**—n'est affiché que lorsqu'un lecteur d'empreinte digitale est disponible. Utilisez ce paramètre pour ajuster le retour qui se produit lorsque vous faites glisser votre empreinte digitale.
 - **Activer le retour audio** : le Gestionnaire de sécurité vous donne un retour audio lorsqu'une empreinte digitale a été glissée, jouant différents sons pour des événements spécifiques du programme. Vous pouvez attribuer de nouveaux sons à ces événements à l'aide de l'onglet **Sons** dans le Panneau de configuration Windows ou désactiver le retour audio en effaçant cette option.
 - **Afficher le retour qualité de la lecture**

Pour afficher tous les glissements, sans se soucier de la qualité, sélectionnez la case à cocher.

Pour n'afficher que des glissements de bonne qualité, désélectionnez la case à cocher.

Sauvegarde et restauration de vos données

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

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



REMARQUE : Seules les données sont sauvegardées lorsque vous utilisez cette fonctionnalité.

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

Pour sauvegarder les données :

1. Ouvrez le tableau de bord de Security Manager. Pour plus d'informations, reportez-vous à la section [Ouverture de Security Manager à la page 27](#).
2. Dans le panneau gauche du tableau de bord, cliquez sur **Avancé**, puis sur **Sauvegarder et restaurer**.
3. Cliquez sur **Sauvegarder les données**.
4. Sélectionnez les modules à inclure dans la sauvegarde. Dans la plupart des cas, vous sélectionnez tous les modules.
5. Vérifiez votre identité.
6. Entrez le nom du fichier de stockage. Par défaut, le fichier est enregistré dans le dossier Documents. Cliquez sur **Parcourir** pour choisir un autre emplacement.

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

Pour restaurer les données :

1. Ouvrez le tableau de bord de Security Manager. Pour plus d'informations, reportez-vous à la section [Ouverture de Security Manager à la page 27](#).
2. Dans le panneau gauche du tableau de bord, cliquez sur **Avancé**, puis sur **Sauvegarder et restaurer**.
3. Cliquez sur **Restaurer les données**.
4. Sélectionnez le fichier de stockage créé. Entrez son chemin d'accès dans le champ fourni ou cliquez sur **Parcourir**.
5. Entrez le mot de passe utilisé pour protéger le fichier.
6. Sélectionnez les modules pour lesquels vous souhaitez restaurer les données. Dans la plupart des cas, vous sélectionnez tous les modules répertoriés.
7. Vérifiez votre mot de passe Windows.
8. Cliquez sur **Terminer**.

5 Drive Encryption for HP ProtectTools (certains modèles uniquement)

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

L'assistant d'installation de HP ProtectTools Security Manager permet aux administrateurs Windows d'activer Drive Encryption, de sauvegarder la clé de cryptage et de sélectionner ou désélectionner une ou plusieurs unités. Pour plus d'informations, reportez-vous à l'aide du logiciel HP ProtectTools Security Manager.

Les tâches suivantes peuvent être effectuées avec Drive Encryption :

- Sélection des paramètres de Drive Encryption :
 - Activation d'un mot de passe protégé TPM
 - Cryptage ou décryptage d'unités ou de partitions individuelles à l'aide du cryptage logiciel
 - Cryptage ou décryptage d'unités autocryptées 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
- Récupération d'une clé Drive Encryption
- Activation de l'authentification au préamorçage de Drive Encryption à l'aide d'un mot de passe, d'une empreinte enregistrée ou du code PIN d'une Smart Card

Ouverture de Drive Encryption

Les administrateurs peuvent accéder à Drive Encryption depuis la console d'administration de HP ProtectTools.

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

Tâches générales

Activation de Drive Encryption pour les disques durs standard

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

1. Utilisez l'assistant d'installation de HP ProtectTools Security Manager pour activer Drive Encryption.
2. Suivez les instructions à l'écran jusqu'à ce que la page **Activez les fonctions de sécurité** s'affiche, puis passez à l'étape 4 ci-dessous.

- ou -

1. Cliquez sur **Démarrer, Tous les programmes, HP**, puis sur **Console d'administration de HP ProtectTools**.
2. Dans le volet gauche, cliquez sur l'icône **+** située à gauche de **Sécurité** pour afficher les options disponibles.
3. Cliquez sur **Fonctions**.
4. Cochez la case **Drive Encryption**, puis cliquez sur **Suivant**.

 **REMARQUE :** Si aucun disque dur n'est sélectionné pour le cryptage, l'authentification au préamorçage de Drive Encryption est activée, mais la ou les unités ne seront pas cryptées.

5. Sous **Unités à crypter**, sélectionnez la case à cocher en regard du disque dur à crypter, puis cliquez sur **Suivant**.
6. Pour sauvegarder la clé de cryptage, insérez le périphérique de stockage dans le logement approprié.

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

7. Sous **Back up Drive Encryption keys** (Sauvegarder les clés Drive Encryption), sélectionnez la case à cocher en regard du périphérique de stockage dans lequel sera enregistrée la clé de cryptage.
8. Cliquez sur **Suivant**.

 **REMARQUE :** L'ordinateur redémarre.

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

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

Activation de Drive Encryption pour les unités autocryptées

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

1. Utilisez l'assistant d'installation de HP ProtectTools Security Manager pour activer Drive Encryption.
2. Suivez les instructions à l'écran jusqu'à ce que la page **Activez les fonctions de sécurité** s'affiche, puis passez à l'étape 4 de la rubrique « Cryptage logiciel » ou « Cryptage matériel » ci-dessous.



REMARQUE : Si l'unité autocryptée de votre ordinateur n'est pas conforme aux spécifications OPAL du Trusted Computing Group relatives à la gestion des unités autocryptées, l'option de cryptage matériel n'est pas disponible et le cryptage logiciel est utilisé par défaut.

Si certaines unités sont autocryptées et d'autres sont standard, l'option de cryptage matériel n'est pas disponible et le cryptage logiciel est utilisé par défaut.

- ou -

Cryptage logiciel

1. Cliquez sur **Démarrer, Tous les programmes, HP**, puis sur **Console d'administration de HP ProtectTools**.
2. Dans le volet gauche, cliquez sur l'icône **+** située à gauche de **Sécurité** pour afficher les options disponibles.
3. Cliquez sur **Fonctions**.
4. Sélectionnez la case à cocher **Drive Encryption**, puis cliquez sur **Suivant**.
5. Sous **Unités à crypter**, sélectionnez la case à cocher en regard du disque dur à crypter, puis cliquez sur **Suivant**.
6. Pour sauvegarder la clé de cryptage, insérez le périphérique de stockage dans le logement approprié.



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

7. Sous **Back up Drive Encryption keys** (Sauvegarder les clés Drive Encryption), sélectionnez la case à cocher en regard du périphérique de stockage dans lequel sera enregistrée la clé de cryptage.
8. Cliquez sur **Appliquer**.



REMARQUE : L'ordinateur redémarre.

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

Cryptage matériel

1. Cliquez sur **Démarrer, Tous les programmes, HP**, puis sur **Console d'administration de HP ProtectTools**.
2. Dans le volet gauche, cliquez sur l'icône **+** située à gauche de **Sécurité** pour afficher les options disponibles.
3. Cliquez sur **Fonctions**.
4. Sélectionnez la case à cocher **Drive Encryption**, puis cliquez sur **Suivant**.



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

Si plusieurs unités s'affichent, les cases à cocher correspondantes sont automatiquement cochées, mais ne sont pas grisées.

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

5. Assurez-vous que la case à cocher **Use hardware drive encryption** (Utiliser le cryptage d'unité matériel) est sélectionnée en bas de l'écran.
6. Sous **Unités à crypter**, sélectionnez la case à cocher en regard du disque dur à crypter, puis cliquez sur **Suivant**.
7. Pour sauvegarder la clé de cryptage, insérez le périphérique de stockage dans le logement approprié.



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

8. Sous **Back up Drive Encryption keys** (Sauvegarder les clés Drive Encryption), sélectionnez la case à cocher en regard du périphérique de stockage dans lequel sera enregistrée la clé de cryptage.
9. Cliquez sur **Appliquer**.



REMARQUE : L'ordinateur doit être redémarré.

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

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

Désactivation de Drive Encryption

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

- ▲ Suivez les instructions à l'écran jusqu'à ce que la page **Activez les fonctions de sécurité** s'affiche, puis passez à l'étape 4 ci-dessous.

– ou –

1. Cliquez sur **Démarrer, Tous les programmes, HP**, puis sur **Console d'administration de HP ProtectTools**.
2. Dans le volet gauche, cliquez sur l'icône **+** située à gauche de **Sécurité** pour afficher les options disponibles.
3. Cliquez sur **Fonctions**.
4. Désélectionnez la case à cocher **Drive Encryption**, puis cliquez sur **Suivant**.

La désactivation de Drive Encryption commence.

 **REMARQUE :** Si le cryptage logiciel a été utilisé, le décryptage démarre. Il peut prendre plusieurs heures, en fonction de la taille de l'unité. Une fois le décryptage terminé, Drive Encryption est désactivé.

Si le cryptage matériel a été utilisé, l'unité est instantanément décryptée, ce qui peut prendre quelques minutes, puis Drive Encryption est désactivé.

Une fois l'unité désactivée, l'ordinateur doit être redémarré.

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 :** Dans le cas d'un cryptage matériel, assurez-vous que l'ordinateur est hors tension. Si l'ordinateur n'est pas mis hors tension, puis redémarré, l'écran d'authentification au préamorçage de Drive Encryption ne s'affiche pas.

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, sauf s'il est désactivé.

Lorsque l'ordinateur sort du mode Veille prolongée, l'authentification au préamorçage de Drive Encryption s'affiche.

REMARQUE : Si l'administrateur Windows a activé l'option Sécurité de préamorçage dans HP ProtectTools Security Manager, vous pouvez vous connecter à l'ordinateur immédiatement après sa mise sous tension, au lieu de le faire depuis l'écran de connexion de Drive Encryption.

1. Cliquez sur votre nom d'utilisateur, puis saisissez votre mot de passe Windows ou le code PIN de 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

- Carte Smart Card ActivIdentity 64K V2C
- Carte SIM ActivIdentity 48010-B DEC06
- Clé USB ActivIdentity V3.0 ZFG-48001-A

Lecteurs PCMCIA

- Lecteur interne Express Card 54 SCR3340
- SCR 201
- SCR 243 (de marque HP également)
- ActivCard
- Omnikey 4040
- Cisco

Lecteurs USB

- ActivCard USB v2
- ActivCard USB v3
- ActivCard USB SCR 3310
- Omnikey Cardman 3121
- Omnikey Cardman 3021
- ACR32
- Terminal HP Smart Card

2. Cliquez sur **OK**.



REMARQUE : Si vous utilisez une clé de récupération pour vous connecter sur l'écran de connexion de Drive Encryption, vous êtes invité à vous authentifier à l'aide de votre mot de passe, du code PIN de votre carte Smart Card ou d'une empreinte enregistrée sur l'écran de connexion Windows.

Protection de vos données via le cryptage de votre disque dur

Il est vivement recommandé d'utiliser l'assistant d'installation de HP ProtectTools Security Manager pour protéger vos données en cryptant votre disque dur :

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



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

- ou -

- ▲ Pour les unités cryptées par cryptage matériel, sélectionnez la ou les unités à crypter. Vous devez sélectionner au moins une unité.

Affichage de l'état de cryptage

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



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

1. Ouvrez HP ProtectTools Security Manager.
2. Sous **Mes données**, cliquez sur **Drive Encryption**.

Dans le cas d'un cryptage logiciel, l'un des codes d'état suivants est affiché sous **Etat d'unité** :

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

Dans le cas d'un cryptage matériel, le code d'état suivant est affiché sous **Etat d'unité** :

- Cryptée

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

Tâches avancées

Gestion de Drive Encryption (administrateur uniquement)

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



REMARQUE : Le cryptage matériel ne peut être modifié sur la page Paramètres.

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

Cryptage logiciel

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

Cryptage matériel

- Cryptée

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

Les administrateurs peuvent utiliser la page Paramètres pour crypter un ou plusieurs disques durs sur l'ordinateur ou décrypter une unité qui a déjà été cryptée.

1. Ouvrez la console d'administration de HP ProtectTools.
2. Dans le volet gauche, cliquez sur l'icône + située à gauche de **Drive Encryption** pour afficher les options disponibles.
3. Cliquez sur **Paramètres**.
4. Sous **Etat d'unité**, cochez ou désélectionnez la case à cocher en regard de chaque disque dur à crypter ou à décrypter, puis cliquez sur **Appliquer**.



REMARQUE : Une fois l'unité cryptée ou décryptée, la barre de progression affiche le temps restant avant la fin du processus durant la session en cours.

Si l'ordinateur est mis hors tension ou lance le mode Veille ou Veille prolongée lors du processus de cryptage, puis redémarre, le temps restant sur la barre de progression est réinitialisé, mais le cryptage en cours reprend à l'endroit où il s'est arrêté. La barre de progression, qui affiche un pourcentage, et le temps restant changent plus rapidement pour refléter la progression précédente.

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

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

Sauvegarde et restauration (tâche de l'administrateur)

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

Sauvegarde des clés de cryptage

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

 **ATTENTION :** Veillez à conserver le périphérique de stockage contenant la clé de cryptage dans un endroit sûr, car si vous oubliez votre mot de passe, perdez votre carte Smart Card ou n'avez enregistré aucune empreinte, ce périphérique constitue votre seul accès à votre disque dur.

1. Ouvrez la console d'administration de HP ProtectTools.
2. Dans le volet gauche, cliquez sur l'icône **+** située à gauche de **Drive Encryption** pour afficher les options disponibles.
3. Cliquez sur **Encryption Key Backup** (Sauvegarde de la clé de cryptage).
4. Insérez le périphérique de stockage utilisé pour sauvegarder la clé de cryptage.
5. Sous **Unité**, sélectionnez la case à cocher en regard du périphérique dans lequel vous souhaitez sauvegarder votre clé de cryptage.
6. Cliquez sur **Sauvegarder les clés**.
7. Lisez les informations contenues dans la page qui s'affiche, puis cliquez sur **Suivant**. La clé de cryptage est enregistrée sur le périphérique de stockage sélectionné.

Récupération des clés de cryptage

Les administrateurs peuvent récupérer une clé de cryptage depuis le périphérique de stockage amovible dans lequel elle a été précédemment enregistrée :

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

Votre ordinateur démarre.



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

6 Privacy Manager pour HP ProtectTools (certains modèles)

Privacy Manager for HP ProtectTools vous permet d'utiliser des méthodes de connexion sécurisées avancées (authentification) pour vérifier la source, l'intégrité et la sécurité des communications lors de l'utilisation de documents de messagerie ou de Microsoft® Office.

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

- Authentification par empreinte digitale
- Mot de passe Windows®
- Smart Card
- Reconnaissance faciale

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

Ouverture de Privacy Manager

Pour ouvrir Privacy Manager :

- Pour accéder aux fonctions spécifiques à Outlook dans Microsoft Outlook, cliquez sur **Envoyer en toute sécurité** dans le groupe **Confidentialité** sur l'onglet **Message**.
- Pour accéder à la plupart des fonctions dans les documents Microsoft Office, cliquez sur **Signer et crypter** dans le groupe **Confidentialité** sur l'onglet **Accueil**.
- Pour accéder à des fonctions supplémentaires, accédez au tableau de bord de HP ProtectTools Security Manager.
 - Cliquez sur **Démarrer, Tous les programmes, HP, HP ProtectTools Security Manager**, puis sur **Privacy Manager**.
- ou -
 - Cliquez sur l'icône du gadget de bureau **HP ProtectTools**.
- ou -
 - Cliquez avec le bouton droit sur l'icône **HP ProtectTools** située dans la zone de notification, à l'extrémité droite de la barre des tâches, puis cliquez sur **Privacy Manager** et enfin sur **Configuration**.

Procédures de configuration

Gestion des certificats Privacy Manager

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

Le Gestionnaire de certificats vous permet de réaliser les tâches suivantes :

- [Demande d'un certificat Privacy Manager à la page 60](#)
- [Obtention d'un certificat Privacy Manager d'entreprise préattribué à la page 61](#)
- [Configuration d'un certificat Privacy Manager par défaut à la page 62](#)
- [Importation d'un certificat tiers à la page 61](#)
- [Affichage des détails du certificat Privacy Manager à la page 62](#)
- [Renouvellement d'un certificat Privacy Manager à la page 62](#)
- [Configuration d'un certificat Privacy Manager par défaut à la page 62](#)
- [Suppression d'un certificat Privacy Manager à la page 63](#)
- [Restauration d'un certificat Privacy Manager à la page 63](#)
- [Révocation d'un certificat Privacy Manager à la page 63](#)

Demande d'un certificat Privacy Manager

Afin de pouvoir utiliser les fonctions de Privacy, vous devez demander et installer un certificat Privacy Manager (depuis Privacy Manager) en utilisant une adresse Internet valide. Vous devez configurer l'adresse Internet en tant que compte dans Microsoft Outlook, sur le même ordinateur depuis lequel vous effectuez la demande du certificat Privacy Manager.

1. Ouvrez Privacy Manager, puis cliquez sur **Certificats**.
2. Cliquez sur **Request a Privacy Manager Certificate** (Demander un certificat Privacy Manager).
3. Sur la page de bienvenue, lisez le texte, puis cliquez sur **Suivant**.
4. Sur la page Contrat de licence, lisez le contrat de licence.
5. Assurez-vous de sélectionner la case à cocher en regard de l'option **Cochez cette case pour accepter les termes du contrat de licence**, puis cliquez sur **Suivant**.
6. Sur la page Détails de votre certificat, saisissez les informations requises, puis cliquez sur **Suivant**.
7. Sur la page Demande de certificat acceptée, cliquez sur **Terminer**.

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

Obtention d'un certificat Privacy Manager d'entreprise préattribué

1. Dans Outlook, ouvrez le courrier électronique que vous avez reçu vous indiquant qu'un certificat d'entreprise vous a été préattribué.
2. Cliquez sur **Obtenir**.

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

Reportez-vous à la section [Configuration d'un certificat Privacy Manager à la page 61](#) pour installer le certificat.

Configuration d'un certificat Privacy Manager

1. Lorsque vous recevez le courrier électronique contenant votre certificat Privacy Manager en pièce jointe, ouvrez-le, puis cliquez sur le bouton **Installer** situé dans le coin inférieur droit du message dans Outlook 2007 ou 2010, ou dans le coin supérieur gauche dans Outlook 2003.
2. Authentifiez-vous à l'aide de la méthode de connexion sécurisée choisie.
3. Sur la page Certificat installé, cliquez sur **Suivant**.
4. Sur la page Sauvegarde du certificat, saisissez un nom et un emplacement pour le fichier de sauvegarde ou cliquez sur **Parcourir** pour rechercher un emplacement.

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

5. Saisissez et confirmez un mot de passe, puis cliquez sur **Suivant**.
6. Authentifiez-vous à l'aide de la méthode de connexion sécurisée choisie.
7. Si vous choisissez de démarrer le processus d'invitation de contact authentifié, suivez les instructions à l'écran commençant par l'étape 2 de la rubrique [Ajout de contacts authentifiés à l'aide des contacts Microsoft Outlook à la page 65](#).

- ou -

Si vous cliquez sur **Annuler**, reportez-vous à la section [Gestion des contacts authentifiés à la page 64](#) pour obtenir des informations sur l'ajout ultérieur d'un contact authentifié.

Importation d'un certificat tiers

Vous pouvez importer un certificat tiers dans Privacy Manager grâce à l'assistant Importer un certificat.

Pour utiliser cette fonction, vous devez avoir activé le paramètre **Autoriser l'utilisation de certificats tiers** dans la console d'administration de HP ProtectTools sur la page Paramètres, sous **Privacy Manager**.

1. Ouvrez Privacy Manager, puis cliquez sur **Certificats**.
2. Sélectionnez l'onglet **Gestionnaire de certificats**, puis cliquez sur **Importer les certificats**.

Ce bouton n'est pas affiché si l'importation des certificats n'est pas autorisée.

3. Choisissez d'importer un certificat déjà installé sur cet ordinateur ou un certificat stocké en tant que fichier PFX (Personal Information Exchange/PKCS#12), puis cliquez sur **Suivant**.
 - Pour importer un certificat installé sur cet ordinateur, sélectionnez le certificat souhaité, puis cliquez sur **Suivant**.
 - Pour sélectionner un certificat PFX, cliquez sur **Parcourir**, naviguez jusqu'à l'emplacement du fichier PFX, puis cliquez sur **Suivant**. Saisissez le mot de passe du fichier PFX, puis cliquez sur **Suivant**.
4. Une fois le processus d'importation terminé, cliquez sur **Suivant**.
5. Vous avez la possibilité de sauvegarder le certificat importé.

Il est recommandé d'enregistrer votre certificat à un emplacement autre que le disque dur de votre ordinateur.

Affichage des détails du certificat Privacy Manager

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

Renouvellement d'un certificat Privacy Manager

Lorsque votre certificat Privacy Manager est presque expiré, vous serez averti que vous devez le renouveler :

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



REMARQUE : Le processus de renouvellement du certificat Privacy Manager ne remplace pas votre ancien certificat Privacy Manager. Vous devez obtenir un nouveau certificat Privacy Manager et l'installer en utilisant la même procédure que dans la section [Demande d'un certificat Privacy Manager à la page 60](#).

En ce qui concerne les certificats d'entreprise émis par votre société à l'aide de Microsoft Certificate Authority, l'administrateur CA doit renouveler le vôtre en utilisant la même clé privée que le certificat original, ou vous fournir un nouveau certificat utilisant la même clé privée.

Configuration d'un certificat Privacy Manager par défaut

Seuls les certificats Privacy Manager sont visibles depuis Privacy Manager, même si d'autres certificats émis par des autorités de certificats différentes sont installés sur votre ordinateur.

Si vous avez plusieurs certificats Privacy Manager sur votre ordinateur, installés à partir de Privacy Manager, vous pouvez en spécifier un en tant que certificat par défaut :

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

 **REMARQUE :** Vous n'êtes pas obligé d'utiliser votre certificat Privacy Manager par défaut. Depuis les différentes fonctions de Privacy Manager, vous pouvez utiliser n'importe quel certificat Privacy Manager.

Suppression d'un certificat Privacy Manager

Si vous supprimez un certificat Privacy Manager, vous ne pourrez plus ouvrir les fichiers ou afficher les données que vous avez cryptées avec ce certificat. Si vous avez supprimé accidentellement un certificat Privacy Manager, vous pouvez le restaurer en utilisant le fichier de sauvegarde que vous avez créé lorsque vous avez installé le certificat. Reportez-vous à la section [Restauration d'un certificat Privacy Manager à la page 63](#) pour plus d'informations.

Pour supprimer un certificat Privacy Manager :

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

Restauration d'un certificat Privacy Manager

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

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

Reportez-vous à la section [Configuration d'un certificat Privacy Manager à la page 61](#) ou [Sauvegarde de certificats Privacy Manager et de contacts authentifiés à la page 73](#) pour plus d'informations.

Révocation d'un certificat Privacy Manager

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



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

1. Ouvrez Privacy Manager, puis cliquez sur **Certificats**.
2. Cliquez sur **Paramètres avancés**.
3. Cliquez sur le certificat Privacy Manager que vous souhaitez révoquer, puis sur **Révoquer**.
4. Lorsque la boîte de dialogue de confirmation s'affiche, cliquez sur **Oui**.
5. Authentifiez-vous à l'aide de la méthode de connexion sécurisée choisie.
6. Suivez les instructions à l'écran.

Gestion des contacts authentifiés

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

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

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

Ajout de contacts authentifiés

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

1. Vous envoyez une invitation par courrier électronique à un destinataire Contact authentifié.
2. Le destinataire Contact authentifié répond au courrier électronique.
3. Vous recevez le courrier électronique de réponse du destinataire du contact authentifié, puis cliquez sur **Accepter**.

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

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



REMARQUE : Pour répondre à votre invitation pour devenir un contact authentifié, les destinataires de contact authentifié doivent avoir Privacy Manager installé sur leur ordinateur ou avoir installé le client alternatif. Pour plus d'informations sur l'installation du client alternatif, accédez au site Web de DigitalPersona à l'adresse <http://digitalpersona.com/privacymanager/download>.

Ajout d'un contact authentifié

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

– ou –

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

2. Si la boîte de dialogue de sélection du certificat s'affiche, cliquez sur le certificat Privacy Manager à utiliser, puis sur **OK**.
3. Lorsque la boîte de dialogue d'invitation d'un contact authentifié s'affiche, lisez le texte, puis cliquez sur **OK**.

Un courrier électronique est automatiquement généré.

4. Entrez les adresses électroniques des destinataires que vous souhaitez ajouter en tant que contacts authentifiés.
5. Modifiez le texte et signez avec votre nom (facultatif).
6. Cliquez sur **Envoyer**.

 **REMARQUE :** Si vous n'avez pas obtenu de certificat Privacy Manager, un message vous indique que vous devez disposer d'un certificat Privacy Manager pour envoyer une demande de contact authentifié. Cliquez sur **OK** pour ouvrir l'Assistant Demande de certificat. Reportez-vous à la section [Demande d'un certificat Privacy Manager à la page 60](#) pour plus d'informations.

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

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

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

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

9. Cliquez sur **OK**.

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

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

– ou –

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

2. Lorsque la page Invitation du contact authentifié s'affiche, sélectionnez les adresses électroniques des destinataires à ajouter en tant que contacts authentifiés, puis cliquez sur **Suivant**.
3. Lorsque la page Envoi de l'invitation s'affiche, cliquez sur **Terminer**.

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

4. Modifiez le texte et signez avec votre nom (facultatif).
5. Cliquez sur **Envoyer**.



REMARQUE : Si vous n'avez pas obtenu de certificat Privacy Manager, un message vous indique que vous devez disposer d'un certificat Privacy Manager pour envoyer une demande de contact authentifié. Cliquez sur **OK** pour ouvrir l'Assistant Demande de certificat. Reportez-vous à la section [Demande d'un certificat Privacy Manager à la page 60](#) pour plus d'informations.

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



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

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

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

8. Cliquez sur **OK**.

Affichage des détails d'un contact authentifié

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

Suppression d'un contact authentifié

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

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

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

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

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

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

Tâches générales

Vous pouvez utiliser Privacy Manager avec les produits Microsoft suivants :

- Microsoft Outlook
- Microsoft Office

Utilisation de Privacy Manager dans Microsoft Outlook

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

- **Signer et envoyer un message** (Uniquement avec le bouton Envoyer en toute sécurité) : cette option ajoute une signature numérique au courrier électronique et l'envoie après que vous ayez été authentifié à l'aide de la méthode de connexion sécurisée que vous avez choisi.
- **Sceller pour les contacts authentifiés et envoyer un message** (Uniquement avec le bouton Envoyer en toute sécurité) : cette option ajoute une signature numérique, crypte le courrier électronique et l'envoie après que vous ayez été authentifié à l'aide de la méthode de connexion sécurisée que vous avez choisi.
- **Inviter des contacts** : cette option vous permet d'envoyer une invitation de contact authentifié. Pour plus d'informations, reportez-vous à la section [Ajout d'un contact authentifié à la page 65](#).
- **Inviter mes contacts Outlook** : cette option vous permet d'envoyer une invitation de contact authentifié à tous les contacts de votre carnet d'adresses Microsoft Outlook. Pour plus d'informations, reportez-vous à la section [Ajout de contacts authentifiés à l'aide des contacts Microsoft Outlook à la page 65](#).
- **Ouvrir le logiciel Privacy Manager** : les options Certificats, Contacts authentifiés et Paramètres vous permettent d'ouvrir le logiciel Privacy Manager afin d'ajouter, d'afficher ou de modifier les paramètres actuels. Reportez-vous à la section [Gestion des certificats Privacy Manager à la page 60](#), [Gestion des contacts authentifiés à la page 64](#) ou [Configuration de Privacy Manager pour Microsoft Outlook à la page 68](#) pour plus d'informations.

Configuration de Privacy Manager pour Microsoft Outlook

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

– ou –

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

– ou –

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

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

Signature et envoi d'un message électronique

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

Scellage et envoi d'un message électronique

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

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

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

Affichage d'un message électronique crypté

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

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

Utilisation de Privacy Manager dans un document Microsoft Office 2007

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

- **Signer le document** : cette option ajoute votre signature numérique au document.
- **Ajouter une ligne de signature avant de signer** (Microsoft Word et Microsoft Excel uniquement) : par défaut, une ligne de signature est ajoutée lorsqu'un document Microsoft Word ou Microsoft Excel est signé ou crypté. Pour désactiver cette option, cliquez sur **Ajouter une ligne de signature** pour supprimer la coche.
- **Crypter le document** : cette option ajoute votre signature numérique et crypte le document.
- **Supprimer le cryptage** : cette option supprime le cryptage du document.
- **Ouvrir le logiciel Privacy Manager** : les options Certificats, Contacts authentifiés et Paramètres vous permettent d'ouvrir le logiciel Privacy Manager afin d'ajouter, d'afficher ou de

modifier les paramètres actuels. Reportez-vous à la section [Gestion des certificats Privacy Manager à la page 60](#), [Gestion des contacts authentifiés à la page 64](#) ou [Configuration de Privacy Manager pour Microsoft Office à la page 70](#) pour plus d'informations.

Configuration de Privacy Manager pour Microsoft Office

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

– ou –

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

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

Signature d'un document Microsoft Office

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

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

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

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

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

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



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

4. Cliquez sur la flèche vers le bas située en regard de **Signer et crypter**, puis sur **Signer le document**.
5. Authentifiez-vous à l'aide de la méthode de connexion sécurisée choisie.

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

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

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

1. Dans Microsoft Word ou Microsoft Excel, créez et enregistrez un document.
2. Cliquez sur le menu **Insertion**.
3. Dans le groupe **Texte** de la barre d'outils, cliquez sur la flèche située en regard de **Ligne de signature**, puis sur **Fournisseur de signatures Privacy Manager**.

La boîte de dialogue Configuration de signature s'affiche.

4. Dans la zone sous **Signataire suggéré**, saisissez le nom du signataire suggéré.
5. Dans la zone sous **Instructions destinées au signataire**, saisissez un message pour ce signataire suggéré.

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

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

 **REMARQUE :** Le propriétaire du document assigne les signataires suggérés à son document. Les cases à cocher **Afficher la date de signature dans la ligne de signature** et/ou **Afficher le titre du signataire dans la ligne de signature** doivent être sélectionnées afin que le signataire suggéré puisse afficher la date et/ou le titre dans la ligne de signature.

8. Cliquez sur **OK**.

Ajout d'une ligne de signature pour un signataire suggéré

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

Pour signer le document :

1. Double-cliquez sur la ligne de signature appropriée.
2. Authentifiez-vous à l'aide de la méthode de connexion sécurisée choisie.

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

Cryptage d'un document Microsoft Office

Vous pouvez crypter un document Microsoft Office pour vous et vos contacts authentifiés. Lorsque vous cryptez un document et le fermez, vous et le(s) contact(s) authentifié(s) que vous avez sélectionné(s) devez vous authentifier avant de l'ouvrir.

Pour crypter un document Microsoft Office :

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

La boîte de dialogue de sélection des contacts authentifiés s'affiche.

4. Cliquez sur le nom d'un contact authentifié qui pourra ouvrir le document et afficher son contenu.



REMARQUE : Pour sélectionner plusieurs noms de contacts authentifiés, maintenez la touche **ctrl** enfoncée, puis cliquez sur les noms individuels.

5. Cliquez sur **OK**.

Si vous décidez de modifier le document ultérieurement, suivez les étapes de la section [Suppression du cryptage d'un document Microsoft Office à la page 72](#). Lorsque le cryptage est supprimé, vous pouvez modifier le document. Suivez les étapes de cette section pour crypter à nouveau le document.

Suppression du cryptage d'un document Microsoft Office

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

Pour supprimer le cryptage d'un document Microsoft Office :

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

Envoi d'un document Microsoft Office crypté

Vous pouvez joindre un document Microsoft Office crypté à un message électronique sans avoir à signer ou crypter le message lui-même. Pour ce faire, créez et envoyez un courrier électronique avec un document signé ou crypté, tout comme vous le feriez avec un courrier électronique classique avec une pièce jointe.

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

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

1. Dans Microsoft Outlook, cliquez sur **Nouveau** ou sur **Répondre**.
2. Saisissez votre message électronique.

3. Joignez le document Microsoft Office.
4. Pour plus d'instructions, reportez-vous à la section [Scellage et envoi d'un message électronique à la page 69](#).

Affichage d'un document Microsoft Office signé



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

Lors de l'ouverture d'un document Microsoft Office signé, une icône Signatures numériques s'affiche dans la barre d'état, au bas de la fenêtre du document.

1. Cliquez sur l'icône **Signatures numériques** pour afficher la boîte de dialogue Signatures, qui contient le nom de chaque utilisateur ayant signé le document, ainsi que la date de chaque signature.
2. Pour afficher des détails supplémentaires sur chaque signature, cliquez avec le bouton droit sur un nom dans la boîte de dialogue Signatures, puis sélectionnez **Détails de la signature**.

Affichage d'un document Microsoft Office crypté

Pour afficher un document Microsoft Office crypté sur un autre ordinateur, vous devez y installer Privacy Manager. Vous devez également restaurer le certificat Privacy Manager utilisé pour crypter le fichier.

Si le certificat a été perdu, vous devez restaurer le certificat Privacy Manager utilisé pour crypter le fichier afin d'afficher le document Microsoft Office crypté.

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

Tâches avancées

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

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

Sauvegarde de certificats Privacy Manager et de contacts authentifiés

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

1. Ouvrez Privacy Manager, puis cliquez sur **Migration**.
2. Cliquez sur **Sauvegarde**.
3. Sur la page Sélectionner les données, sélectionnez les catégories de données à inclure dans le fichier de migration, puis cliquez sur **Suivant**.

4. Sur la page Fichier de migration, saisissez un nom de fichier ou cliquez sur **Parcourir** pour rechercher un emplacement, puis cliquez sur **Suivant**.
5. Saisissez et confirmez un mot de passe, puis cliquez sur **Suivant**.



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

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

Restauration de certificats Privacy Manager et de contacts authentifiés

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

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

Administration centrale de Privacy Manager

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

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

7 File Sanitizer pour HP ProtectTools

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) et de nettoyer le disque dur de manière périodique.



REMARQUE : Cette version de File Sanitizer prend en charge le disque dur de l'ordinateur uniquement.

Destruction

Une destruction diffère d'une suppression Windows® standard (également appelée une suppression simple dans File Sanitizer). 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.

Lorsque vous choisissez un profil de destruction (**Haute sécurité**, **Sécurité moyenne** ou **Sécurité basse**), une liste prédéfinie de ressources et une méthode d'effacement sont automatiquement sélectionnées pour la destruction. Vous pouvez également personnaliser un profil de destruction en indiquant le nombre de cycles de destruction, les ressources à inclure pour la destruction, les ressources à confirmer avant la destruction et les ressources à exclure de la destruction. Pour plus d'informations, reportez-vous à la section [Sélection ou création d'un profil de destruction à la page 80](#).

Vous pouvez configurer une programmation de destruction automatique ou activer manuellement la destruction à l'aide de l'icône **HP ProtectTools** dans la zone de notification, à l'extrémité droite de la barre des tâches. Pour plus d'informations, reportez-vous à la section [Définition d'une programmation de destruction à la page 79](#), [Destruction manuelle d'une ressource à la page 84](#) ou [Destruction manuelle de tous les éléments sélectionnés à la page 85](#).



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

Nettoyage de l'espace libre

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

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



REMARQUE : Un nettoyage de l'espace libre peut être effectué de manière occasionnelle pour les ressources que vous supprimez en sélectionnant **Paramètres de suppression simple** dans File Sanitizer, en déplaçant les ressources dans la corbeille Windows ou en supprimant les ressources manuellement. Le nettoyage de l'espace libre ne fournit aucune sécurité supplémentaire aux ressources détruites.

Vous pouvez définir une programmation de nettoyage automatique de l'espace libre ou activer manuellement le nettoyage de l'espace libre à l'aide de l'icône **HP ProtectTools** dans la zone de notification, à l'extrémité droite de la barre des tâches. Pour plus d'informations, reportez-vous à la section [Définition d'une programmation de nettoyage de l'espace libre à la page 79](#) ou [Activation manuelle du nettoyage de l'espace libre à la page 85](#).

Ouverture de File Sanitizer

1. Cliquez successivement sur **Démarrer**, **Tous les programmes**, **HP**, puis sur **HP ProtectTools Security Manager**.

2. Cliquez sur **File Sanitizer**.

- ou -

▲ Double-cliquez sur l'icône **File Sanitizer** sur le bureau.

- ou -

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

Procédures de configuration

Définition d'une programmation de destruction

Vous pouvez sélectionner un profil de destruction prédéfini ou créer votre propre profil de destruction. Pour plus d'informations, reportez-vous à la section [Sélection ou création d'un profil de destruction à la page 80](#). Vous pouvez également détruire manuellement des ressources à tout moment. Pour plus d'informations, reportez-vous à la section [Utilisation d'une séquence de touches pour démarrer la destruction à la page 83](#).



REMARQUE : Une tâche planifiée démarre à une heure spécifique. Si le système est hors tension ou en mode Veille/Veille prolongée à l'heure planifiée, File Sanitizer n'essaie pas de relancer la tâche.

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



REMARQUE : Une boîte de dialogue s'ouvre à l'arrêt et vous demande si vous souhaitez poursuivre la destruction des ressources sélectionnées ou ignorer la procédure.

Cliquez sur **Oui** pour ignorer la procédure de destruction ou sur **Non** pour poursuivre la destruction.

- **Ouverture de navigateur Web** : permet de détruire toutes les ressources Web sélectionnées, telles que l'historique des URL du navigateur, lorsque vous ouvrez un navigateur Web.
- **Fermeture de navigateur Web** : permet de détruire toutes les ressources Web sélectionnées, telles que l'historique des URL du navigateur, lorsque vous fermez un navigateur Web.
- **Séquence de touches** : permet de spécifier une séquence de touches pour démarrer la destruction. Pour plus d'informations, reportez-vous à la section [Utilisation d'une séquence de touches pour démarrer la destruction à la page 83](#).



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

3. Pour planifier un prochain moment de destruction des ressources sélectionnées, sélectionnez la case à cocher **Activer le planificateur**, entrez votre mot de passe Windows, puis sélectionnez un jour et une heure.
4. Cliquez sur **Appliquer**.

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

Un nettoyage de l'espace libre peut être effectué de manière occasionnelle pour les ressources que vous supprimez en sélectionnant **Paramètres de suppression simple** dans File Sanitizer, en déplaçant les ressources dans la corbeille Windows ou en supprimant les ressources manuellement. Le nettoyage de l'espace libre ne fournit aucune sécurité supplémentaire aux ressources détruites.

 **REMARQUE :** Une tâche planifiée démarre à une heure spécifique. Si le système est hors tension ou en mode Veille/Veille prolongée à l'heure planifiée, File Sanitizer n'essaie pas de relancer la tâche.

1. Ouvrez File Sanitizer, puis cliquez sur **Nettoyage**.
2. Pour planifier ultérieurement le nettoyage des ressources supprimées du disque dur, sélectionnez la case à cocher **Activer le planificateur**, saisissez votre mot de passe Windows, puis sélectionnez un jour et une heure.
3. Cliquez sur **Appliquer**.

 **REMARQUE :** L'opération de nettoyage de l'espace libre peut prendre beaucoup de temps. Bien qu'elle soit effectuée en tâche de fond, l'utilisation accrue du processeur peut affecter les performances de l'ordinateur.

Sélection ou création d'un profil de destruction

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

Sélection d'un profil de destruction prédéfini

Lorsque vous choisissez un profil de destruction prédéfini, une méthode d'effacement prédéfinie et une liste de ressources sont sélectionnées automatiquement. Vous pouvez également afficher la liste prédéfinie des ressources sélectionnées pour la destruction.

1. Ouvrez File Sanitizer, puis cliquez sur **Paramètres**.
2. Cliquez sur un profil de destruction prédéfini :
 - **Haute sécurité**
 - **Sécurité moyenne**
 - **Sécurité basse**
3. Pour afficher les ressources sélectionnées pour la destruction, cliquez sur **Afficher les détails**.
 - a. **Les éléments sélectionnés seront détruits et un message de confirmation s'affichera. Les éléments non sélectionnés seront détruits sans message de confirmation.** : sélectionnez la case à cocher pour afficher un message de confirmation avant la destruction de l'élément ou désélectionnez-la pour détruire l'élément sans afficher de message de confirmation.

 **REMARQUE :** Une ressource sera détruite même si sa case est décochée.

- b. Cliquez sur **Appliquer**.
4. Cliquez sur **Appliquer**.

Personnalisation d'un profil de destruction

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

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



REMARQUE : Le nombre de cycles de destruction sélectionné sera effectué pour chaque ressource. Par exemple, si vous choisissez trois cycles de destruction, un algorithme obscurcissant les données est exécuté à trois reprises. Si vous choisissez les cycles de destruction à sécurité plus élevée, la destruction peut prendre beaucoup de temps. Cependant, plus le nombre de cycles de destruction spécifié est élevé, moins il y a de chances que les données soient récupérées.

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

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

4. **Les éléments sélectionnés seront détruits et un message de confirmation s'affichera. Les éléments non sélectionnés seront détruits sans message de confirmation.** : sélectionnez la case à cocher pour afficher un message de confirmation avant la destruction de l'élément ou désélectionnez-la pour détruire l'élément sans afficher de message de confirmation.



REMARQUE : Une ressource sera détruite même si sa case est décochée.

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

5. Pour protéger des fichiers ou des dossiers d'une destruction automatique :
 - a. Sous **Ne pas détruire les éléments suivants**, cliquez sur **Ajouter** puis naviguez vers le fichier ou le dossier ou saisissez son chemin d'accès.
 - b. Cliquez sur **Ouvrir**, puis sur **OK**.

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

6. Cliquez sur **Appliquer**.

Personnalisation d'un profil de suppression simple

Le profil de suppression simple effectue une suppression standard des ressources sans destruction. Vous pouvez personnaliser un profil de suppression simple en spécifiant les ressources à inclure, celles à confirmer avant la suppression et celles à exclure.



REMARQUE : Si vous sélectionnez **Paramètres de suppression simple**, un nettoyage de l'espace libre peut être exécuté de manière occasionnelle sur les ressources qui ont été supprimées manuellement en utilisant la corbeille de Windows.

1. Ouvrez File Sanitizer, cliquez sur **Paramètres, Paramètres de suppression simple**, puis sur **Détails**.
2. Sélectionnez les ressources à supprimer :
 - a. Sous **Options de suppression disponibles**, cliquez sur une ressource, puis sur **Ajouter**.
 - b. Pour ajouter une ressource personnalisée, cliquez sur **Ajouter une option personnalisée**, naviguez vers le fichier ou le dossier ou saisissez son chemin d'accès, puis cliquez sur **OK**.
 - c. Cliquez sur la ressource personnalisée, puis sur **Ajouter**.

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

3. **Les éléments sélectionnés seront détruits et un message de confirmation s'affichera. Les éléments non sélectionnés seront détruits sans message de confirmation.** : sélectionnez la case à cocher pour afficher un message de confirmation avant la destruction de l'élément ou désélectionnez-la pour détruire l'élément sans afficher de message de confirmation.



REMARQUE : Une ressource sera détruite même si sa case est décochée.

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

4. Pour protéger des ressources d'une suppression automatique :
 - a. Sous **Ne pas supprimer les éléments suivants**, cliquez sur **Ajouter** puis naviguez vers le fichier ou le dossier ou saisissez son chemin d'accès.
 - b. Cliquez sur **Ouvrir**, puis sur **OK**.

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

5. Cliquez sur **Appliquer**.

Tâches générales

Vous pouvez utiliser File Sanitizer pour réaliser les tâches suivantes :

- Utiliser une séquence de touches pour démarrer la destruction : Cette fonction permet de créer une séquence de touches (par exemple, **ctrl+alt+s**) pour démarrer la destruction. Pour plus de détails, reportez-vous à la section [Utilisation d'une séquence de touches pour démarrer la destruction à la page 83](#).
- Utiliser l'icône File Sanitizer pour démarrer la destruction : Cette fonction est similaire à la fonction de glisser-déplacer de Windows. Pour plus de détails, reportez-vous à la section [Utilisation de l'icône File Sanitizer à la page 84](#).
- Détruire manuellement une ressource spécifique ou toutes les ressources sélectionnées : Cette fonction permet de détruire manuellement des éléments sans attendre que la destruction planifiée soit invoquée. Pour plus de détails, reportez-vous à la section [Destruction manuelle d'une ressource à la page 84](#) ou [Destruction manuelle de tous les éléments sélectionnés à la page 85](#).
- Activer manuellement le nettoyage de l'espace libre : Cette fonction permet d'activer manuellement le nettoyage de l'espace libre. Pour plus de détails, reportez-vous à la section [Activation manuelle du nettoyage de l'espace libre à la page 85](#).
- Annuler une opération de destruction ou de nettoyage de l'espace libre : Cette fonction permet d'arrêter une opération de destruction ou de nettoyage de l'espace libre. Pour plus de détails, reportez-vous à la section [Abandon d'une opération de destruction ou de nettoyage de l'espace libre à la page 85](#).
- Afficher les fichiers journaux : Cette fonction permet d'afficher les fichiers journaux de destruction et de nettoyage de l'espace libre contenant des erreurs ou des échecs ayant eu lieu lors de la dernière opération de destruction ou de nettoyage de l'espace libre. Pour plus de détails, reportez-vous à la section [Affichage des fichiers journaux à la page 85](#).

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

Utilisation d'une séquence de touches pour démarrer la destruction

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

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

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

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

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

Utilisation de l'icône File Sanitizer

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

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

Destruction manuelle d'une ressource

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

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



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

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

– ou –

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

– ou –

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

Destruction manuelle de tous les éléments sélectionnés

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

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

– ou –

1. Cliquez avec le bouton droit sur l'icône **File Sanitizer** du bureau, puis cliquez sur **Détruire maintenant**.

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

– ou –

1. Ouvrez File Sanitizer, puis cliquez sur **Détruire**.

2. Cliquez sur le bouton **Détruire maintenant**.

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

Activation manuelle du nettoyage de l'espace libre

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

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

– ou –

1. Ouvrez File Sanitizer, puis cliquez sur **Nettoyage de l'espace libre**.

2. Cliquez sur **Nettoyer maintenant**.

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

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

Lorsqu'une opération de destruction ou de nettoyage de l'espace libre est en cours, un message s'affiche au dessus de l'icône de HP ProtectTools Security Manager dans la zone de notification, située à l'extrémité droite de la barre des tâches. Il fournit des détails sur le processus de destruction ou de nettoyage de l'espace libre (pourcentage effectué) et permet d'abandonner l'opération.

▲ Pour annuler l'opération, cliquez sur le message, puis sur **Arrêter**.

Affichage des fichiers journaux

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



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

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

- 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 :

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

8 Device Access Manager pour HP ProtectTools (certains modèles)

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



REMARQUE : Certains périphériques de saisie ou d'interface utilisateur comme une souris, un clavier, un pavé tactile ou un lecteur d'empreintes digitales, ne sont pas contrôlés par Device Access Manager. Pour plus d'informations, reportez-vous à la section [Classes de périphériques non gérées à la page 99](#).

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

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

Ouverture de Device Access Manager

1. Connectez-vous en tant qu'Administrateur.
2. Cliquez sur **Démarrer, Tous les programmes, HP**, puis sur **Console d'administration de HP ProtectTools**.
3. Dans le volet gauche, cliquez sur **Device Access Manager**.

Les utilisateurs peuvent afficher la stratégie de HP ProtectTools Device Access Manager en utilisant HP ProtectTools Security Manager. Cette console fournit une vue en lecture seule.

Procédures de configuration

Configuration de l'accès aux périphériques

HP ProtectTools Device Access Manager fournit quatre vues :

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

Configuration simple

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

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

Pour autoriser ou refuser l'accès à une classe de périphérique pour l'ensemble des utilisateurs non chargés de l'administration des périphériques, procédez comme suit :

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

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

3. Cliquez sur **Appliquer**.



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

4. Cliquez sur **OK**.

Démarrage du service d'arrière-plan

Le première fois qu'une nouvelle stratégie est définie et appliquée, le service d'arrière-plan Verrouillage des périphériques / Audition HP ProtectTools démarre automatiquement et il est configuré pour démarrer automatiquement à chaque fois que le système démarre.



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

Les administrateurs peuvent également démarrer ou arrêter ce service :

1. Dans Windows 7, cliquez sur **Démarrer, Panneau de configuration**, puis sur **Système et sécurité**.

- ou -

Dans Windows Vista®, cliquez sur **Démarrer, Panneau de configuration**, puis sur **Système et maintenance**.

- ou -

Dans Windows XP, cliquez sur **Démarrer, Panneau de configuration**, puis sur **Performances et maintenance**.

2. Cliquez sur **Outils d'administration**, puis sur **Services**.
3. Sélectionnez le service **Verrouillage des périphériques / Audition HP ProtectTools**.
4. Pour démarrer le service, cliquez sur **Démarrer**.

- ou -

Pour arrêter le service lorsqu'il est en cours d'exécution, cliquez sur **Arrêter**.

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

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

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

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

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

Configuration de classe de périphérique

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

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

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

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



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

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

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

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

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

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

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

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

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

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

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

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

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

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

Interdiction d'accès à un utilisateur ou à un groupe

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

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



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

Autorisation d'accès pour un utilisateur ou un groupe

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

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

La boîte de dialogue Select Users or Groups (Sélectionner des utilisateurs ou des groupes) s'ouvre.
4. Cliquez sur **Avancés**, puis sur **Rechercher maintenant** pour rechercher des utilisateurs ou des groupes à ajouter.
5. Cliquez sur un utilisateur ou un groupe à ajouter à la liste des utilisateurs ou des groupes disponibles, puis cliquez sur **OK**.
6. Cliquez de nouveau sur **OK**.
7. Cliquez sur **Autoriser** pour octroyer l'accès à cet utilisateur.
8. Cliquez sur **Appliquer**.

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

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

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

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

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

1. Dans le volet gauche de la console d'administration de HP ProtectTools, cliquez sur **Device Access Manager**, puis sur **Configuration de classe de périphérique**.
2. Dans la liste des périphériques, cliquez sur la classe de périphérique à configurer, puis naviguez vers le dossier situé en dessous.
3. Sous **Utilisateur/groupe**, cliquez sur **Autoriser** à côté du groupe pour lequel autoriser l'accès.
4. Cliquez sur **Refuser** à côté du groupe pour lequel refuser l'accès.
5. Naviguez vers le périphérique spécifique auquel l'accès est à autoriser à l'utilisateur dans la liste des périphériques.
6. Cliquez sur **Ajouter**.
La boîte de dialogue Select Users or Groups (Sélectionner des utilisateurs ou des groupes) s'ouvre.
7. Cliquez sur **Avancés**, puis sur **Rechercher maintenant** pour rechercher des utilisateurs ou des groupes à ajouter.
8. Cliquez sur un utilisateur pour lequel autoriser l'accès, puis sur **OK**.
9. Cliquez sur **Autoriser** pour autoriser l'accès à cet utilisateur.
10. Cliquez sur **Appliquer**.

Suppression des paramètres pour un utilisateur ou un groupe

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

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

Réinitialisation de la configuration

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

Pour rétablir les paramètres d'usine :

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

Configuration JITA

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

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

- **Scénario** : une stratégie de configuration simple est configurée pour empêcher tous les utilisateurs non chargés de l'administration des périphériques d'accéder au lecteur de DVD/CD-ROM.
- **Résultat** : un utilisateur pour lequel l'authentification JITA est activée qui tente d'accéder au lecteur de DVD/CD-ROM reçoit le même message "accès refusé" qu'un utilisateur n'ayant pas l'authentification JITA activée. Puis un message infobulle s'affiche, demandant si l'utilisateur souhaite un accès JITA. Si l'utilisateur clique sur l'infobulle, la boîte de dialogue d'authentification de l'utilisateur s'affiche. Lorsque l'utilisateur saisit les informations d'authentification avec succès, l'accès au lecteur de DVD/CD-ROM est octroyé.

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

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

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

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

- Lecteurs de DVD/CD-ROM
- Supports amovibles

Création d'une JITA pour un utilisateur ou un groupe

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

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

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

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

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

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

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

Désactivation d'une JITA pour un utilisateur ou un groupe

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

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

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

Paramètres avancés

Les paramètres avancés fournissent les fonctions suivantes :

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

Le groupe Administrateurs de périphériques est utilisé pour exclure les utilisateurs fiables (fiables par rapport à l'accès à un périphérique) des restrictions imposées par une stratégie de Device Access Manager. Les utilisateurs fiables comprennent généralement les administrateurs système. Reportez-vous à la section [Groupe Administrateurs de périphériques à la page 98](#) pour plus d'informations.

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

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

Pour démarrer ces services :

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

- ou -

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

```
sc start flcdlock
```

Appuyez sur [entrée](#).

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

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

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

Groupe Administrateurs de périphériques

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

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

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

Pour ajouter des utilisateurs au groupe Administrateurs de périphériques :

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

Les méthodes alternatives pour gérer l'adhésion à ce groupe sont :

- Pour Windows 7 Professionnel ou Windows Vista, les utilisateurs peuvent être ajoutés à ce groupe en utilisant le composant logiciel enfichable de Microsoft Management Console (MMC) Utilisateurs et groupes locaux standard.
- Pour les versions familiales de Windows 7, Windows Vista, or Windows XP, depuis un compte avec les privilèges administrateurs, saisissez le code suivant dans une fenêtre d'invite de commande :

```
net localgroup "Device Administrators" username /add
```

Dans cette commande, "username" est le nom d'utilisateur de l'utilisateur que souhaitez ajouter à ce groupe.

Assistance eSATA

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

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

Classes de périphériques non gérées

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

- Périphériques d'entrée/de sortie
 - Biométrique
 - Souris
 - Clavier
 - Imprimante
 - Imprimantes Plug and play (PnP)
 - Mise à niveau d'imprimante
 - Périphériques d'interface utilisateur infrarouge
 - Lecteur de Smart Card

- Série multi-port
- Unité de disque
- Contrôleur de disquette (FDC)
- Contrôleur de disque dur (HDC)
- Classe de périphérique d'interface utilisateur infrarouge (HID)
- Alimentation
 - Batterie
 - Support de gestion de l'alimentation avancé (APM)
- Divers
 - Ordinateur
 - Décodeur
 - Affichage
 - Processeur
 - Système
 - Inconnu
 - Volume
 - Volume instantané
 - Périphériques de sécurité
 - Accélérateur de sécurité
 - Pilote d'affichage unifié Intel®
 - Pilote multimédia
 - Changeur de média
 - Multifonction
 - Legacard
 - Client Net
 - Service Net
 - Net trans
 - Adaptateur SCSI

9 Récupération en cas de Vol

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

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

Pour activer Computrace for HP ProtectTools :

1. Connectez-vous à l'Internet.
2. Cliquez sur **Démarrer, Tous les programmes, HP**, puis sur **HP ProtectTools Security Manager**.
3. Dans le volet gauche de Security Manager, cliquez sur **Récupération en cas de vol**.
4. Pour lancer l'Assistant d'activation de Computrace, cliquez sur le bouton **Activer maintenant**.
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 **Identifiant de connexion** et **Mot de passe**, saisissez les informations d'authentification que vous avez reçues dans le courrier électronique de confirmation, puis cliquez sur le bouton **Connexion**.

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

- Surveiller les ordinateurs.
- Protéger vos données à distance.
- Signaler le vol de n'importe quel ordinateur protégé par Computrace.
- ▲ Pour plus d'informations sur Computrace for HP ProtectTools, cliquez sur **En savoir plus**.

10 Embedded Security for HP ProtectTools (sur certains modèles uniquement)



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

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

- Cryptage de fichiers et de dossiers EFS (Encryption File System) Microsoft®
- Création d'un lecteur sécurisé personnel (PSD) pour la protection de données utilisateur
- Fonctions de gestion de données, telles que la sauvegarde et la restauration de la hiérarchie de clés
- Prise en charge d'applications d'autres sociétés (telles que Microsoft Outlook et Internet Explorer) pour les opérations protégées impliquant l'utilisation de certificats numériques avec la sécurité intégrée

La puce de sécurité intégrée TPM permet d'améliorer et d'activer d'autres fonctions de sécurité de HP ProtectTools Security Manager. Ainsi, Credential Manager for HP ProtectTools peut utiliser la puce intégrée en tant que facteur d'authentification lorsque l'utilisateur ouvre une session Windows.

Procédures de configuration

⚠ ATTENTION : Pour réduire les risques liés à la sécurité, nous recommandons vivement à l'administrateur informatique d'initialiser immédiatement la puce de sécurité intégrée. Si la puce de sécurité intégrée n'est pas initialisée, un utilisateur non autorisé, un vers informatique ou un virus risque de détourner l'ordinateur et de contrôler les tâches du propriétaire, telles que la gestion des archives de restauration d'urgence ou la configuration des paramètres d'accès utilisateur.

Suivez les étapes indiquées dans les sections suivantes pour activer et initialiser la puce de sécurité intégrée.

Activation de la puce de sécurité intégrée dans Computer Setup

Vous devez activer la puce de sécurité intégrée dans l'Assistant d'initialisation rapide ou dans l'utilitaire Computer Setup.

Pour activer la puce de sécurité intégrée dans Computer Setup :

1. Ouvrez Computer Setup en démarrant/redémarrant l'ordinateur, puis appuyez sur **f10** lorsque le message "F10 = ROM Based Setup" (F10 = Configuration ROM) s'affiche dans l'angle inférieur gauche de l'écran.
2. Si vous n'avez pas défini de mot de passe administrateur, utilisez les touches de direction pour sélectionner **Sécurité, Mot de passe de configuration**, puis appuyez sur la touche **entrée**.
3. Entrez votre mot de passe dans les champs **Nouveau mot de passe** et **Vérifier le nouveau mot de passe**, puis appuyez sur **f10**.
4. Dans le menu **Sécurité**, utilisez les touches de direction pour sélectionner **Sécurité intégrée TPM**, puis appuyez sur **entrée**.
5. Sous **Sécurité intégrée**, si le périphérique est masqué, sélectionnez **Disponible**.
6. Sélectionnez l'option **Etat du périphérique de sécurité intégré**, puis modifiez le paramètre en **Activer**.
7. Appuyez sur **f10** pour accepter les modifications apportées à la configuration de sécurité intégrée.
8. Pour enregistrer les préférences et quitter l'utilitaire Computer Setup, utilisez les touches de direction afin de sélectionner **Fichier**, sélectionnez l'option **Enregistrer les modifications et quitter**, puis suivez les instructions qui s'affichent à l'écran.

Initialisation de la puce de sécurité intégrée

Dans le processus d'initialisation de la sécurité intégrée, vous effectuerez les opérations suivantes :

- Définition d'un mot de passe propriétaire pour la puce de sécurité intégrée, afin de protéger l'accès à toutes les fonctions propriétaire sur cette dernière.
- Définition de l'archive de restauration d'urgence, qui est une zone de stockage protégée permettant le recryptage des clés utilisateur de base pour tous les utilisateurs.

Pour initialiser la puce de sécurité intégrée :

1. Cliquez avec le bouton droit sur l'icône **HP ProtectTools Security Manager** située dans la zone de notification, à l'extrémité droite de la barre des tâches, puis sélectionnez l'option **Embedded Security Initialization** (Initialisation d'Embedded Security).

L'Assistant Initialisation de la sécurité intégrée HP ProtectTools s'affiche.

2. Suivez les instructions à l'écran.

Configuration du compte utilisateur de base

La définition d'un compte utilisateur de base dans Embedded Security :

- Produit une clé utilisateur de base qui protège les informations cryptées, et définit un mot de passe de la clé utilisateur de base qui protège cette dernière.
- Définit un lecteur sécurisé personnel (PSD) pour le stockage de fichiers et de dossiers cryptés.

 **ATTENTION :** Protégez le mot de passe de la clé utilisateur de base. Les informations cryptées ne sont pas accessibles ou ne peuvent pas être restaurées sans ce mot de passe.

Pour configurer un compte utilisateur de base et activer les fonctions de sécurité intégrée :

1. Si l'Assistant d'initialisation de l'utilisateur Embedded Security n'est pas ouvert, cliquez successivement sur **Démarrer**, sur **Tous les programmes**, sur **HP** et sur **HP ProtectTools Security Manager**.
2. Dans le volet gauche, cliquez sur **Sécurité intégrée**, puis sur **Paramètres utilisateur**.
3. Dans le volet droit, sous **Fonctions de sécurité intégrée**, cliquez sur **Configurer**.

L'Assistant Initialisation de l'utilisateur de la sécurité intégrée s'affiche.

4. Suivez les instructions à l'écran.

 **REMARQUE :** Pour utiliser la messagerie électronique sécurisée, vous devez d'abord configurer le client de messagerie en vue d'utiliser un certificat numérique créé via le module Embedded Security. Si aucun certificat numérique n'est disponible, vous devez en obtenir un à partir d'une autorité de certification. Pour obtenir des instructions de configuration de votre messagerie électronique, ainsi qu'un certificat numérique, reportez-vous à l'aide relative au logiciel du client de messagerie.

Tâches générales

Une fois le compte utilisateur de base défini, vous pouvez effectuer les tâches suivantes :

- Cryptage de fichiers et dossiers
- Envoi et réception de courrier électronique crypté

Utilisation du lecteur sécurisé personnel

Une fois le lecteur PSD configuré, vous êtes invité à saisir le mot de passe de la clé utilisateur de base à la connexion suivante. Si ce mot de passe est correctement saisi, vous pouvez accéder au lecteur PSD directement à partir de l'Explorateur Windows.

Cryptage de fichiers et dossiers

Lors de l'utilisation de fichiers cryptés, respectez les règles suivantes :

- Seuls les fichiers et dossiers situés sur des partitions NTFS peuvent être cryptés. Les fichiers et dossiers situés sur des partitions FAT ne peuvent pas être cryptés.
- Les fichiers système et les fichiers compressés ne peuvent pas être cryptés, et les fichiers cryptés ne peuvent pas être compressés.
- Il est recommandé de crypter les dossiers temporaires car les pirates s'y intéressent particulièrement.
- Une stratégie de restauration est automatiquement définie lorsque vous cryptez un fichier ou un dossier pour la première fois. Grâce à cette stratégie, si vous perdez vos certificats de cryptage et clés privées, vous pourrez utiliser un agent de restauration pour décrypter vos informations.

Pour crypter des fichiers et dossiers :

1. Cliquez avec le bouton droit sur le fichier ou dossier à crypter.
2. Cliquez sur **Crypter**.
3. Cliquez sur une des options suivantes :
 - **Appliquer les modifications à ce dossier uniquement**
 - **Appliquer les modifications à ce dossier, aux sous-dossiers et aux fichiers**
4. Cliquez sur **OK**.

Envoi et réception de courrier électronique crypté

Le module Embedded Security vous permet d'envoyer et recevoir des courriers électroniques cryptés, mais les procédures requises varient selon le programme que vous utilisez pour accéder à votre courrier électronique. Pour plus d'informations, reportez-vous à l'aide sur le logiciel Embedded Security, ainsi qu'à celle relative à votre programme de messagerie.

Modification du mot de passe de la clé utilisateur de base

Pour modifier le mot de passe de la clé utilisateur de base :

1. Cliquez sur **Démarrer, Tous les programmes, HP**, puis sur **HP ProtectTools Security Manager**.
2. Dans le volet gauche, cliquez sur **Sécurité intégrée**, puis sur **Paramètres utilisateur**.
3. Dans le volet droit, sous **Basic User password** (Mot de passe utilisateur de base), cliquez sur **Modifier**.
4. Entrez l'ancien mot de passe, puis définissez et confirmez le nouveau mot de passe.
5. Cliquez sur **OK**.

Tâches avancées

Les administrateurs peuvent effectuer les tâches suivantes dans Sécurité intégrée :

- Sauvegarde et restauration des informations d'authentification de Sécurité intégrée, paramètres de Sécurité intégrée et lecteur sécurisé personnel
- Changement du mot de passe du propriétaire
- Réinitialisation d'un mot de passe utilisateur
- Migration sécurisée des informations d'identification de sécurité d'utilisateur d'une plateforme source vers une plateforme destination

Sauvegarde et restauration

La fonction de sauvegarde de la sécurité intégrée crée une archive qui contient des informations de certification à restaurer en cas d'urgence.

Création d'un fichier de sauvegarde

Pour créer un fichier de sauvegarde :

1. Cliquez sur **Démarrer, Tous les programmes, HP**, puis sur **Console d'administration de HP ProtectTools**.
2. Dans le volet gauche, cliquez sur **Sécurité intégrée**, puis sur **Sauvegarde**.
3. Dans le volet droit, cliquez sur **Configurer**. L'Assistant de sauvegarde de HP Embedded Security for ProtectTools s'ouvre.
4. Suivez les instructions à l'écran.

Restauration des données de certification à partir du fichier de sauvegarde

Pour restaurer des données à partir du fichier de sauvegarde :

1. Cliquez sur **Démarrer, Tous les programmes, HP**, puis sur **Console d'administration de HP ProtectTools**.
2. Dans le volet gauche, cliquez sur **Sécurité intégrée**, puis sur **Sauvegarde**.
3. Dans le volet droit, cliquez sur **Restaurer tout**. L'Assistant de sauvegarde de HP Embedded Security for ProtectTools s'ouvre.
4. Suivez les instructions à l'écran.

Modification du mot de passe propriétaire

Les administrateurs peuvent changer le mot de passe du propriétaire :

1. Cliquez sur **Démarrer, Tous les programmes, HP**, puis sur **Console d'administration de HP ProtectTools**.
2. Dans le volet gauche, cliquez sur **Sécurité intégrée**, puis sur **Avancé**.
3. Dans le volet droit, sous **Mot de passe propriétaire**, cliquez sur **Modifier**.
4. Entrez l'ancien mot de passe propriétaire, puis définissez et confirmez le nouveau mot de passe propriétaire.
5. Cliquez sur **OK**.

Réinitialisation d'un mot de passe utilisateur

Un administrateur peut aider un utilisateur à réinitialiser un mot de passe oublié. Pour plus d'informations, reportez-vous à l'aide sur le logiciel.

Migration de clés avec l'Assistant de migration

La migration est une tâche avancée d'administrateur qui permet la gestion, la restauration et le transfert de clés et de certificats.

Pour plus de détails sur la migration, consultez l'aide sur le logiciel Embedded Security.

11 Exceptions de mot de passe localisé

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

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

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

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

Par exemple, dans le cas de certaines installations de Windows XP en version japonaise, l'IME par défaut est appelé Microsoft IME Standard 2002 pour le japonais qui traduit en réalité selon la disposition du clavier E0010411. Cependant, il s'agit bien d'un IME et pas d'une disposition de clavier. (Le plan de codage de disposition de clavier est réservé par Microsoft pour les IME, ce qui étend le concept de disposition de clavier.) Puisqu'il ne s'agit pas d'une disposition de clavier qui peut être représenté dans l'environnement de saisie pour l'invite du mot de passe de sécurité de préamorçage du BIOS ou de l'invite du mot de passe de HP Drive Encryption, tout mot de passe saisi avec cet IME est rejeté par HP ProtectTools. Microsoft IME Standard 2002 pour le japonais est également différent du « Nom Commun » dans Microsoft Windows Vista®. Windows cartographie certains IME selon une disposition de clavier. Dans pareil cas, l'IME est pris en charge par HP ProtectTools parce que la définition de disposition de clavier sous-jacente (le code hexadécimal) est utilisée.

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 cartographie vers une disposition de clavier supportée, alors HP ProtectTools peut prendre en charge la configuration.

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

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

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



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

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

Gestion des touches spéciales

- Chinois, slovaque, français canadien et tchèque.

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

- Coréen

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

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

Langue	Windows	BIOS	Drive Encryption
Arabe	Les touches ٱ, ٲ et ٳ génèrent deux caractères.	Les touches ٱ, ٲ et ٳ génèrent un caractère.	Les touches ٱ, ٲ et ٳ génèrent un caractère.
Français canadien	ç, è, à et é deviennent Ç, È, À, and É lors de l'utilisation de Maj. dans Windows.	ç, è, à et é deviennent ç, è, à et é lors de l'utilisation de Maj. dans Sécurité de préamorçage du BIOS.	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 vers c0a. Cependant, en raison de différences subtiles entre les dispositions de clavier, il est recommandé aux utilisateurs de langue espagnole de modifier la disposition de leur clavier sous Windows afin d'utiliser 1040a (variation espagnole) ou 080a (Amérique latine).	n/a	n/a
US international	<ul style="list-style-type: none"> ◦ Les touches j, ñ, ' , ' , ¥ et ×, situées sur la ligne du haut, sont rejetées. ◦ Les touches à, ®, 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

Langue	Windows	BIOS	Drive Encryption
Tchèque	<ul style="list-style-type: none"> ◦ La touche ě est rejetée. ◦ La touche ě est rejetée. ◦ La touche ů est rejetée. ◦ Les touches é, í, et ž sont rejetées. ◦ Les touches ě, ě, ě, ě, et ř sont rejetées. 	n/a	n/a
Slovaque	La touche ž est rejetée.	<ul style="list-style-type: none"> ◦ Les touches š, š, et š sont rejetées lors de la saisie mais acceptées si saisies à l'aide du clavier virtuel. ◦ La touche morte ț génère deux caractères. 	n/a
Hongrois	La touche ž est rejetée.	La touche ț génère deux caractères.	n/a

Langue	Windows	BIOS	Drive Encryption
Slovène	La touche žŽ est rejetée dans Windows et la touche alt génère une touche morte dans le BIOS.	Les touches ú, Ú, ů, Ů, ŷ, Š, š, Š, š, et Š sont rejetées dans le BIOS.	n/a
Japonais	<p>Pour Windows XP uniquement, la disposition de clavier pour le japonais standard, 411, est totalement prise en charge. Un IME, représenté communément dans Windows Xp en tant que Microsoft Standard IME 2002, ne serait pas pris en charge. Cependant, des tests empiriques ont démontré que cet IME est un duplicata proche de la disposition de clavier 411 lors de la saisie de caractères simples. Le logiciel bascule donc cet IME vers une disposition de clavier 411 pendant la sécurisation du BIOS et de HP Drive Encryption à l'aide de mots de passe japonais.</p> <p>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.</p>	n/a	n/a

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. Cliquez sur **Démarrer**, sur **Panneau de configuration**, puis sur **Options régionales et de langue**.
 2. Cliquez sur l'onglet **Langues**.
 3. Cliquez sur le bouton **Détails**.
 4. Sur l'onglet **Paramètres**, cliquez sur le bouton **Ajouter** pour ajouter clavier pris en charge (ajoute clavier américain sous langue d'entrée chinois).
 5. Définissez le clavier pris en charge comme entrée par défaut.
 6. Redémarrez HP ProtectTools, puis saisissez à nouveau le mot de passe.
- Un utilisateur utilise un caractère non pris en charge. Pour résoudre ce problème :
 1. Modifiez le mot de passe de Windows de manière à n'utiliser que des caractères pris en charge. Les caractères non pris en charge sont listés dans [Gestion des touches spéciales à la page 115](#).
 2. Exécutez à nouveau l'assistant d'installation de Security Manager, puis saisissez le nouveau mot de passe de Windows.

Glossaire

activation

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

administrateur

Reportez-vous à la section *administrateur Windows*.

administrateur Windows

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

archive de restauration d'urgence

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

ATM

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

authentification

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

authentification à la mise sous tension

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

authentification unique

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

autorité de certification (AC)

Service chargé d'émettre les certificats requis pour l'exécution d'une infrastructure de clé publique.

biométrie

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

bouton Envoyer en toute sécurité

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

bouton Signer et crypter

Un bouton logiciel qui est affiché sur la barre d'outils des applications Microsoft Office. Cliquer sur ce bouton vous permet de signer, de crypter, ou de supprimer le cryptage d'un document Microsoft Office.

carte d'identité

Un gadget de bureau de Windows servant à identifier visuellement votre bureau à l'aide de votre nom d'utilisateur et d'une image choisie. Cliquez sur la carte d'identité pour ouvrir la console d'administration de HP ProtectTools.

certificat numérique

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

certificat Privacy Manager

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

classe de périphérique

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

compte réseau

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

compte utilisateur Windows

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

connexion

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

console

Emplacement central dans lequel vous pouvez accéder aux fonctions et paramètres de la Console d'administration de HP ProtectTools et les gérer.

contact authentifié

Personne ayant accepté une invitation de contact authentifié.

cryptage

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

cryptographie

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

cycle de destruction

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

décryptage

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

destinataire de contact authentifié

Personne recevant une invitation à devenir un contact authentifié.

destruction

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

destruction automatique

Destruction planifiée que l'utilisateur configure dans File Sanitizer.

destruction manuelle

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

domaine

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

Drive Encryption

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

DriveLock

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

écran de connexion de Drive Encryption

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

EFS (Encryption File System)

Système qui crypte tous les fichiers et sous-dossiers du dossier sélectionné.

empreinte digitale

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

expéditeur authentifié

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

fournisseur de service cryptographique

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

groupe

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

HP SpareKey

Copie de sauvegarde de la clé de cryptage de l'unité.

identité

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

informations d'authentification

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

invitation de contact authentifié

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

jeton

Reportez-vous à la section *Méthode de connexion sécurisée*.

jeton USB

Périphérique de sécurité qui stocke les informations permettant d'identifier un utilisateur. Tout comme une carte Smart Card ou un lecteur biométrique, celui-ci est utilisé pour authentifier le propriétaire d'un ordinateur.

jeton virtuel

Fonction de sécurité dont le fonctionnement est très similaire à celui d'une carte Smart Card ou d'un lecteur de carte. Le jeton est enregistré sur le disque dur de l'ordinateur ou dans le registre Windows. Lorsque vous vous connectez à l'aide d'un jeton virtuel, vous devez saisir un code PIN utilisateur pour mener à bien l'authentification.

JITA

Authentification Just-In-Time.

lecteur sécurisé personnel

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

ligne de signature

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

liste des contacts authentifiés

Liste complète des contacts authentifiés.

message authentifié

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

méthode de connexion sécurisée

Méthode utilisée pour la connexion à l'ordinateur.

migration

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

mode du périphérique SATA

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

mot de passe de révocation

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

nettoyage de l'espace libre

Écriture sécurisée de données aléatoires par-dessus les ressources supprimées permettant de déformer le contenu de la ressource supprimée.

PIN

Code d'identification personnel.

PKI

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

profil de destruction

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

Puce de sécurité intégrée TPM (Trusted Platform Module)

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

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.

sceller pour les contacts authentifiés

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

scène

Photo d'un utilisateur inscrit utilisée pour l'authentification.

sécurité de connexion Windows

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

séquence de touches

Combinaison de touches spécifique dont l'utilisation permet de démarrer une destruction automatique ; par exemple [ctrl+alt+s](#).

service en arrière-plan

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

signataire suggéré

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

signature numérique

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

Smart Card

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

stratégie de contrôle d'accès aux périphériques

Liste des périphériques auxquels un utilisateur est autorisé ou non à accéder.

suppression simple

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

tableau de bord

Un emplacement central dans lequel vous pouvez accéder aux fonctions et paramètres de Security Manager for HP ProtectTools et les gérer.

TXT

Trusted Execution Technology (technologie d'exécution sécurisée).

utilisateur

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

Index

A

- abandon d'une opération de destruction ou de nettoyage 85
- accès
 - contrôle 87
 - protection contre un accès non autorisé 8
- accès non autorisé, protection 8
- activation
 - Drive Encryption pour les disques durs standard 49
 - Drive Encryption pour les unités autocryptées 50
- activation de la puce TPM 104
- activation du nettoyage de l'espace libre 85
- administration centrale 74
- affichage
 - document Microsoft Office crypté 73
 - document Microsoft Office signé 73
 - message électronique crypté 69
- affichage des fichiers journaux 85
- ajout
 - ligne de signature 70
 - ligne de signature pour un signataire suggéré 71
 - signataires suggérés 71
- annulation d'une opération de destruction ou de nettoyage 85
- applications, configuration 24
- assistant, Configuration de HP ProtectTools 13
- Assistant de configuration 13
- authentification 19
- autorisation d'accès 93

C

- carte d'identité 44
- certificat, préattribué 61
- certificat numérique
 - affichage des détails 62
 - configuration 61
 - configurer par défaut 62
 - demande 60
 - réception 61
 - renouvellement 62
 - restauration 63
 - révocation 63
 - suppression 63
- certificat préattribué 61
- certificat Privacy Manager
 - affichage des détails 62
 - configuration 61
 - configurer par défaut 62
 - demande 60
 - réception 61
 - renouvellement 62
 - restauration 63
 - révocation 63
 - suppression 63
- certificats Privacy Manager
 - restauration 74
 - sauvegarde 73
- certificat tiers, importation 61
- changements de mot de passe à l'aide de différentes dispositions de clavier 114
- classe de périphérique, autoriser l'accès à un utilisateur 93
- classes de périphériques, non gérées 99
- classes de périphériques non gérées 99
- clé de cryptage
 - recupération 56
 - sauvegarde 56
- code PIN de la carte Smart Card 11
- compte, utilisateur de base 106
- compte utilisateur de base 106
- Computrace 101
- configuration
 - accès aux périphériques 89
 - applications 24
 - classe de périphérique 90
 - Console d'administration 19
 - pour Microsoft Outlook 68
 - pour un document Microsoft Office 70
 - réinitialisation 94
 - simple 89
- configuration de classe de périphérique 90
- configuration de l'authentification Just-In-Time (JITA) 95
- configuration JITA 95
- configuration simple 89
- connexion à l'ordinateur 52
- connexions
 - ajout 31
 - catégories 33
 - gestion 34
 - menu 33
 - modification 32
- console d'administration
 - utilisation 18
- Console d'administration
 - configuration 19
- console d'administration de HP ProtectTools 16
- console d'administration de HP ProtectTools, ouverture 17

- contacts authentifiés
 - affichage des détails 66
 - ajout 64
 - restauration 74
 - sauvegarde 73
 - suppression 66
 - vérification de l'état de révocation 66
 - contrôle d'accès aux périphériques 87
 - création d'un profil de destruction 80
 - Credential Manager 37
 - cryptage
 - logiciel 50, 51, 55
 - matériel 50, 51
 - suppression 72
 - cryptage d'unités 47
 - cryptage de fichiers et dossiers 107
 - cryptage du disque dur 53, 55
 - cryptage logiciel 50, 51, 55
 - cryptage matériel 50, 51
 - cycle de destruction 81
- D**
- décryptage d'unités 47
 - décryptage du disque dur 55
 - définition
 - programmation de destruction 79
 - programmation de nettoyage 79
 - définition des ressources à confirmer
 - avant la destruction 81
 - avant la suppression 82
 - demande d'un certificat numérique 60
 - désactivation de Drive Encryption 51
 - destruction
 - abandon 85
 - annulation 85
 - automatique 83
 - manuelle 84, 85
 - séquence de touches 83
 - destruction manuelle
 - tous les éléments sélectionnés 85
 - une ressource 84
 - Device Access Manager for HP ProtectTools, ouverture 88
 - Device Access Manager pour HP ProtectTools 87
 - document Microsoft Office
 - cryptage 71
 - envoi par courrier électronique, crypté 72
 - signature 70
 - suppression du cryptage 72
 - documents cryptés, envoi par courrier électronique 72
 - données
 - limitation de l'accès 8
 - restauration 45
 - sauvegarde 45
 - Drive Encryption for HP ProtectTools
 - activation 49
 - connexion après activation de Drive Encryption 49
 - cryptage d'unités individuelles 55
 - décryptage d'unités individuelles 55
 - désactivation 49
 - gestion de Drive Encryption 55
 - sauvegarde et restauration 56
- E**
- Embedded Security for HP ProtectTools
 - activation de la puce TPM 104
 - Clé utilisateur de base 106
 - compte utilisateur de base 106
 - courrier électronique crypté 107
 - création de fichier de sauvegarde 109
 - cryptage de fichiers et dossiers 107
 - initialisation de la puce 105
- F**
- lecteur sécurisé personnel 107
 - migration de clés 111
 - modification du mot de passe propriétaire 110
 - Mot de passe de la clé utilisateur de base, modification 108
 - procédures de configuration 104
 - réinitialisation du mot de passe utilisateur 110
 - restauration de données de certification 109
 - emergency recovery 105
 - empreintes digitales paramètres 22
 - empreintes digitales, inscription 38
 - envoi par courrier électronique d'un document Microsoft Office crypté 72
 - eSATA 99
 - état de cryptage, affichage 53
 - Etat des applications de sécurité 29
 - Excel, ajout d'une ligne de signature 70
 - exceptions de mot de passe 112
 - exclusion de ressources d'une suppression automatique 82
- G**
- gestion
 - cryptage ou décryptage d'unités 55
 - informations d'authentification 37
 - mots de passe 30, 31

gestion, outils 25
Gestion centrale 25
gestion des mots de passe 24
gestion des touches spéciales
115
gestion des utilisateurs 20
Gestionnaire de mots de passe
24, 30, 31
groupe
autorisation d'accès 93
interdiction d'accès 92
suppression 94

H

HP ProtectTools, fonctions 2
HP ProtectTools Security
Manager 26
HP ProtectTools Security
Manager : mot de passe pour la
sauvegarde et la restauration
10

I

icône, utilisation 84
importation, certificat tiers 61
informations d'authentification
spécification 21
initialisation de la puce de sécurité
intégrée 105
inscription
empreintes digitales 38
scènes 40
interdiction 92

J

JITA
création extensible pour un
utilisateur ou un groupe 96
création pour un utilisateur ou
un groupe 96
désactivation pour un utilisateur
ou un groupe 96

L

lecteur sécurisé personnel
(PSD) 107
limitation
accès aux données
confidentielles 8

M

message électronique
affichage d'un message
crypté 69
scellage pour les contacts
authentifiés 69
signature 69
messages 25
Microsoft Excel, ajout d'une ligne
de signature 70
Microsoft Word, ajout d'une ligne
de signature 70
mise en route 89
mises à jour 25
mot de passe
changement 37
Clé utilisateur de base 108
gestion 10
HP ProtectTools 10
instructions 12
jeton emergency recovery
105
modification du propriétaire
110
propriétaire 105
réinitialisation pour utilisateur
110
sécurisé 12
stratégies 9
mot de passe de connexion
Windows 10
Mot de passe de la clé utilisateur
de base
changement 108
définition 106
mot de passe du jeton emergency
recovery, définition 105
mot de passe propriétaire
définition 105
mot de passe rejeté 118

N

nettoyage
abandon 85
activation 85
annulation 85
manuelle 85
programmation 79
nettoyage de l'espace libre 79

O

objectifs, sécurité 8
objectifs de sécurité
fondamentaux 8
onglet Applications, paramètres
24
onglet Général, paramètres 24
ouverture
Device Access Manager for HP
ProtectTools 88
File Sanitizer for HP
ProtectTools 78
ouverture de Drive Encryption 48
ouverture de la console
d'administration de
HP ProtectTools 17
ouverture de Privacy Manager 59
ouverture de Security Manager
27

P

paramètres
ajout 24, 28
applications 24, 28
icône 35
onglet Général 24
utilisateur avancé 42
paramètres avancés 98
paramètres de périphérique
empreinte digitale 22
SpareKey 21
visage 23
paramètres de périphérique, carte
Smart Card 22, 40
paramètres du tableau de bord
28
périphérique, autoriser l'accès à un
utilisateur 94
personnalisation
profil de destruction 81
profil de suppression simple
82
préférences, définition 44
Privacy Manager
méthodes d'authentification
58
méthodes de connexion
sécurisée 58
ouverture 59

- utilisation avec Microsoft
 - Outlook 68
 - utilisation dans un document Microsoft Office 2007 69
- Privacy Manager for HP ProtectTools
 - gestion des contacts authentifiés 64
- Privacy Manager pour HP ProtectTools
 - gestion des certificats Privacy Manager 60
 - migration de certificats Privacy Manager et de contacts authentifiés vers un autre ordinateur 73
 - procédures de configuration 60
- profil de destruction
 - création 80, 81
 - personnalisation 81
 - sélection 80
- profil de destruction prédéfini 80
- programmation de destruction, définition 79
- propriétaire, mot de passe
 - modification 110
- protection des ressources d'une destruction automatique 81
- puce TPM
 - activation 104
 - initialisation 105

R

- récupération de la clé de cryptage 56
- récupération en cas de Vol 101
- réinitialisation 94
- restauration de certificats Privacy Manager et de contacts authentifiés 74
- restauration des données 45
- restauration des informations d'authentification de HP ProtectTools 12
- restriction
 - accès aux périphériques 87
- rôles de sécurité 10

S

- sauvegarde de certificats Privacy Manager et de contacts authentifiés 73
- sauvegarde de la clé de cryptage 56
- sauvegarde des données 45
- sauvegarde des informations d'authentification de HP ProtectTools 12
- sauvegarde et restauration information de certification 109
 - sécurité intégrée 109
- scellage 69
- scènes, inscription 40
- sécurité
 - objectifs fondamentaux 8
 - récapitulatif 29
 - rôles 10
- Security Manager, ouverture 27
- sélection
 - profil de destruction 80
 - ressources à détruire 80
- séquence de touches 83
- service d'arrière-plan 90
- signataire suggéré
 - ajout 71
 - ajout d'une ligne de signature 71
- signature
 - document Microsoft Office 70
 - message électronique 69
- Smart Card
 - configuration 22, 40
 - enregistrement 39
 - initialisation 39
- SpareKey, configuration 38
- SpareKey, paramètres 21
- spécification des paramètres de sécurité 20
- suppression de l'accès 94
- suppression du cryptage d'un document Microsoft Office 72
- suppression simple, personnalisation 82

T

- tâches avancées, Embedded Security 109

U

- utilisateur
 - autorisation d'accès 93
 - interdiction d'accès 92
 - suppression 94

V

- VeriSign Identity Protection (VIP) 35
- visage
 - paramètres 23
- vol, protection 8

W

- Word, ajout d'une ligne de signature 70

