

Manuel HP ProtectTools Security Manager

Ordinateurs d'entreprise HP Compaq



© Copyright 2006 Hewlett-Packard Development Company, L.P. Les informations de ce document sont susceptibles d'être modifiées sans préavis.

Microsoft et Windows sont des marques déposées de la société Microsoft aux États-Unis et dans d'autres pays.

Intel et SpeedStep sont des marques d'Intel Corporation aux États-Unis et dans d'autres pays.

Les garanties applicables aux produits et services HP sont énoncées dans les textes de garantie accompagnant ces produits et services. Aucune partie du présent document ne saurait être interprétée comme constituant un quelconque supplément de garantie. HP ne peut être tenu responsable des erreurs ou omissions techniques ou de rédaction de ce document.

Ce document contient des informations protégées par des droits d'auteur. Aucune partie de ce document ne peut être photocopiée, reproduite ou traduite dans une autre langue sans l'accord écrit préalable de Hewlett-Packard.

Manuel HP ProtectTools Security Manager

Ordinateurs d'entreprise HP Compaq

Première édition (août 2006)

Référence : 431330-051

À propos de ce livre

Ce manuel fournit des instructions concernant la configuration et l'utilisation de HP ProtectTools Security Manager.



AVERTISSEMENT Le non-respect de ces instructions expose l'utilisateur à des risques potentiellement très graves.



ATTENTION Le non-respect de ces instructions présente des risques, tant pour le matériel que pour les informations qu'il contient.



Remarque Le texte ainsi défini fournit des informations importantes supplémentaires.

Sommaire

1 Introduction

HP ProtectTools Security Manager	1
Accès à ProtectTools Security Manager	1
Compréhension des rôles de sécurité	2
Gestion de mots de passe ProtectTools	2
Session Credential Manager avec authentification multifacteur	5
Création d'un mot de passe sécurisé	6
Tâches avancées	7
Gestion de paramètres ProtectTools	7
Activation/Désactivation de la prise en charge d'authentification à la mise sous tension de carte Java	7
Activation/Désactivation de la prise en charge d'authentification à la mise sous tension pour la sécurité intégrée	7
Gestion de mots de passe Computer Setup	8
Définition du mot de passe de mise sous tension (si disponible)	8
Modification du mot de passe de mise sous tension (si disponible)	9
Configuration système	9
Modification de la prise en charge d'authentification à la mise sous tension	9
Modification de comptes utilisateur	10
Définition du mot de passe administrateur Computer Setup	10
Modification du mot de passe administrateur Computer Setup	11
Comportement d'attaque de type Dictionnaire avec authentification à la mise sous tension	12
Défense contre une attaque Dictionnaire	12

2 HP BIOS Configuration for ProtectTools

Concepts élémentaires	13
Modification des paramètres du BIOS	13

3 HP Embedded Security for ProtectTools

Concepts élémentaires	15
Procédures de configuration	16

4 HP Credential Manager for ProtectTools

Concepts élémentaires	17
Procédure de lancement	17
Première connexion	18

5 HP Java Card Security for ProtectTools	
Concepts élémentaires	19
6 Solutions de partie tierce	
7 HP Client Manager pour déploiement distant	
Vue d'ensemble	23
Initialisation	23
Maintenance	23
8 Résolution des problèmes	
Credential Manager for ProtectTools	25
Embedded Security for ProtectTools	30
Divers	38
Glossaire	41
Index	45

1 Introduction

HP ProtectTools Security Manager

Le logiciel ProtectTools Security Manager fournit des fonctions de sécurité destinées à aider à protéger l'ordinateur, les réseaux et les données critiques contre les accès non autorisés. La fonctionnalité de sécurité améliorée est fournie par les modules suivants :

- HP BIOS Configuration for ProtectTools
- HP Embedded Security for ProtectTools
- HP Credential Manager for ProtectTools
- HP Java Card Security for ProtectTools

Les modules disponibles pour l'ordinateur peuvent varier en fonction du modèle. Les modules ProtectTools peuvent être préinstallés, fournis sur le CD livré avec l'ordinateur ou disponibles à partir du site Web HP. Pour plus d'informations, consultez le site <http://www.hp.com>.



Remarque Pour obtenir des instructions spécifiques concernant les modules ProtectTools, reportez-vous aux écrans d'aide ProtectTools.

Pour utiliser le module TPM (Trusted Platform Module), les plates-formes contenant un module TPM requièrent une pile TSS (TCG Software Stack) et un logiciel de sécurité intégrée. Certains modèles proposent la pile TSS. Si celle-ci n'est pas fournie, elle peut être achetée auprès de HP. En outre, le logiciel d'activation du module TPM peut être acheté séparément pour certains modèles. Pour plus de détails, reportez-vous à la section [Solutions de partie tierce](#).

Accès à ProtectTools Security Manager

Pour accéder à ProtectTools Security Manager à partir du Panneau de configuration Microsoft Windows :

- ▲ Windows XP : Cliquez sur **Démarrer > Panneau de configuration > Security Center > ProtectTools Security Manager**.
- ▲ Windows 2000 : Cliquez sur **Démarrer > Tous les programmes > HP ProtectTools Security Manager**.



Remarque Une fois le module Credential Manager configuré, vous pouvez également vous connecter au module Credential Manager directement à partir de l'écran de session Windows. Pour plus d'informations, reportez-vous à la section [HP Credential Manager for ProtectTools](#).

Compréhension des rôles de sécurité

Dans la gestion de la sécurité d'ordinateurs (particulièrement dans des organisations de grande taille), une pratique importante est de répartir les responsabilités et les droits parmi divers types d'administrateurs et d'utilisateurs.



Remarque Dans une petite organisation ou dans le cas d'utilisateurs individuels, ces rôles peuvent tous être détenus par la même personne.

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

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



Remarque Un grand nombre des fonctions ProtectTools peuvent être personnalisées par le responsable de la sécurité en coopération avec HP. Pour plus d'informations, consultez le site <http://www.hp.com>.

- Administrateur informatique — Applique et supervise les fonctions de sécurité définies par le responsable de la sécurité. Peut également activer et désactiver certaines fonctions. Par exemple, si le responsable de la sécurité a décidé de déployer des cartes Java, l'administrateur informatique peut activer le mode de sécurité BIOS des cartes Java.
- Utilisateur — Utilise les fonctions de sécurité. Par exemple, si le responsable de la sécurité et l'administrateur informatique ont activé des cartes Java pour le système, l'utilisateur peut définir le numéro PIN de carte Java et utiliser la carte pour l'authentification.

Il est conseillé aux administrateurs d'appliquer des règles de bonne pratique pour limiter les privilèges et l'accès des utilisateurs.

Gestion de mots de passe ProtectTools

La plupart des fonctions ProtectTools Security Manager sont protégées par des mots de passe. Le tableau ci-dessous répertorie les mots de passe les plus 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 définis et utilisés uniquement par les administrateurs informatiques sont également indiqués dans ce tableau. Tous les autres mots de passe peuvent être définis par des administrateurs ou utilisateurs normaux.

Tableau 1-1 Gestion de mots de passe

Mot de passe ProtectTools	Défini dans ce module ProtectTools	Fonction
Mot de passe administrateur Computer Setup	BIOS Configuration, par administrateur informatique	Protège l'accès à l'utilitaire Computer Setup et aux paramètres de sécurité.

 **Remarque** Également connu en tant que mot de passe administrateur BIOS, configuration F10 ou configuration de sécurité

Tableau 1-1 Gestion de mots de passe (suite)

Mot de passe de mise sous tension	BIOS Configuration	La prise en charge de l'authentification à la mise sous tension HP ProtectTools est un outil de sécurité TPM conçu pour empêcher tout accès non autorisé à l'ordinateur à sa mise sous tension. Cette fonction utilise le mot de passe utilisateur de base de sécurité intégrée HP ProtectTools. Une fois l'authentification à la mise sous tension activée dans Computer Setup, le mot de passe est défini à la première ou prochaine fois que la clé d'utilisateur de base de sécurité intégrée est initialisée. La puce TPM de sécurité intégrée protège le mot de passe d'authentification à la mise sous tension.
Mot de passe administrateur de carte Java	Java Card Security, par administrateur informatique	Lie la carte Java à l'ordinateur pour des besoins d'identification. Permet à un administrateur d'ordinateur d'activer ou de désactiver des mots de passe Computer Setup, de générer une nouvelle carte d'administrateur, ainsi que de créer des fichiers de récupération pour restaurer des cartes d'administrateur ou d'utilisateur.
 Remarque Également connu en tant que mot de passe de carte d'administrateur du BIOS		
PIN de carte Java	Java Card Security	Protège l'accès au contenu d'une carte Java et l'accès à un ordinateur lorsqu'un lecteur et une carte Java en option sont utilisés. Vérifie si le mot de passe utilisateur de carte Java est dupliqué vers le numéro PIN. Il est utilisé pour enregistrer l'authentification de carte Java.
Mot de passe de fichier de récupération de carte Java (si disponible)	Java Card Security	Protège l'accès au fichier de récupération qui contient les mots de passe BIOS.
Mot de passe utilisateur de carte Java (si disponible)	Java Card Security	Lie la carte Java à l'ordinateur pour des besoins d'identification. Permet à un utilisateur de créer un fichier de récupération pour restaurer une carte d'utilisateur.
 Remarque Également connu en tant que mot de passe de carte d'utilisateur du BIOS		
Mot de passe utilisateur de base	Embedded Security	Utilisé pour accéder aux fonctions de sécurité intégrée, telles que cryptage de messagerie sécurisée, de fichiers et de dossiers. Lorsque ce mot de passe est activé en tant que mot de passe de prise en charge de l'authentification à la mise sous tension du BIOS, protège l'accès au contenu de l'ordinateur lorsque ce dernier est mis sous tension, redémarré ou restauré à partir du mode hibernation. Également utilisé pour authentifier le PSD (Personal Secure Drive) et pour enregistrer l'authentification TPM.
 Remarque Également connu en tant que : mot de passe de sécurité intégrée, mot de passe de préamorçage TPM		
Mot de passe de jeton de récupération d'urgence	Embedded Security, par administrateur informatique	Protège l'accès au jeton de récupération d'urgence, qui est un fichier de

Tableau 1-1 Gestion de mots de passe (suite)

	Remarque Également connu en tant que : clé de jeton de récupération d'urgence	sauvegarde de la puce de sécurité intégrée TPM.
Mot de passe propriétaire	Embedded Security, par administrateur informatique	Protège le système et la puce TPM d'un accès non autorisé à toutes les fonctions propriétaire de la sécurité intégrée.
Mot de passe de session Credential Manager	Credential Manager	Ce mot de passe propose 2 options : <ul style="list-style-type: none"> • Il peut être utilisé à la place du processus de connexion Windows, en permettant d'accéder simultanément à Windows et à Credential Manager. • Il peut être utilisé en tant que connexion distincte pour accéder à Credential Manager après une connexion à Microsoft Windows.
Mot de passe de fichier de récupération Credential Manager	Credential Manager, par administrateur informatique	Protège l'accès au fichier de récupération Credential Manager.
Mot de passe de session Windows	Panneau de configuration Windows	Peut être utilisé dans une connexion manuelle ou enregistré sur la carte Java.
Mot de passe de planificateur de sauvegarde	Embedded Security, par administrateur informatique	Configure le planificateur de sauvegarde pour la sécurité intégrée.
	Remarque Un mot de passe utilisateur Windows est employé pour configurer le planificateur de sauvegarde pour la sécurité intégrée.	
Mot de passe PKCS #12	Embedded Security, par administrateur informatique	Mot de passe utilisé pour la clé de cryptage à partir d'autres certificats, si importés.
	Remarque Chaque certificat importé est doté d'un mot de passe spécifique à ce certificat.	
Remarque Non requis pour un fonctionnement logiciel normal. L'utilisateur peut opter de définir ce mot de passe lors de l'utilisation de la sécurité intégrée pour envoyer des certificats importants.		
Jeton de réinitialisation de mot de passe	Embedded Security, par administrateur informatique	Outil fourni par le client qui permet au propriétaire de réinitialiser le mot de passe utilisateur de base en cas de perte. Un mot de passe est utilisé pour réaliser cette opération de réinitialisation.
Mot de passe administrateur d'agent de récupération Microsoft	Microsoft, par administrateur de sécurité informatique	Assure que les données cryptées PSD (Personal Secure Drive) peuvent être récupérées. Pour plus d'informations, consulter l'adresse http://www.microsoft.com/technet/prodtechnol/winxppro/support/dataprot.mspx .

Tableau 1-1 Gestion de mots de passe (suite)

	Remarque L'agent de récupération de sécurité peut être tout administrateur de machine locale. Si l'agent de récupération est créé, toute personne souhaitant se connecter en tant que cet administrateur requiert un mot de passe. L'agent de récupération peut décrypter les données chiffrées de tous les utilisateurs juste en les ouvrant (aucun assistant requis).		Remarque Non requis pour un fonctionnement logiciel normal. L'utilisateur peut opter de définir ce mot de passe lors de l'utilisation de la sécurité intégrée pour envoyer des certificats importants.
PIN principal de jeton virtuel	Credential Manager	Option du client qui permet de stocker des identités avec Credential Manager.	
PIN utilisateur de jeton virtuel	Credential Manager	Option du client qui permet de stocker des identités avec Credential Manager.	
Mot de passe d'assistant de sauvegarde d'identité	Credential Manager, par administrateur informatique	Utilisé pour protéger l'accès à une sauvegarde d'identité lors de l'utilisation de Credential Manager.	
Mot de passe d'authentification de jeton virtuel	Credential Manager	Utilisé pour enregistrer une authentification de jeton virtuel avec Credential Manager.	
Alias d'authentification TPM	Credential Manager	Utilisé à la place du mot de passe utilisateur de base par le gestionnaire d'identités, suivant le choix de l'administrateur ou de l'utilisateur.	
Connexion via empreinte digitale	Credential Manager	Credential Manager permet à l'utilisateur de remplacer la connexion par mot de passe Windows par une session de connexion conviviale et sécurisée par empreinte digitale. À la différence du mot de passe, les identités par empreinte digitale ne peuvent pas être partagées, communiquées, perdues ou violées. Utilisé par Credential Manager.	
Authentification de jeton USB	Credential Manager	Utilisé par Credential Manager en tant qu'authentification de jeton au lieu d'un mot de passe.	

Session Credential Manager avec authentification multifacteur

L'ouverture de session Credential Manager permet à la technologie d'authentification multifacteur de se connecter au système d'exploitation Windows. Ceci élève la sécurité de connexion par mot de passe Windows standard en requérant une puissante authentification multifacteur. Cette fonction améliore également la convivialité d'une connexion quotidienne en éliminant le besoin de mémoriser des mots de passe utilisateur. Une fonction unique de cette connexion Credential Manager consiste en sa possibilité de cumuler plusieurs identités en une identité utilisateur unique, ce qui permet d'employer l'authentification multifacteur une seule fois et de fournir de multiples accès à différents comptes Windows avec le même ensemble d'identités.

L'authentification utilisateur multifacteur prend en charge toute combinaison de mots de passe utilisateur, de mots de passe dynamiques ou à utilisation unique, de données TPM, de cartes Java, de jetons USB, de jetons virtuels et de données biométriques. Credential Manager prend également en

charge des méthodes d'authentification alternatives, en offrant la possibilité de plusieurs privilèges d'accès utilisateur pour la même application ou le même service. Un utilisateur peut consolider toutes ses identités, mots de passe d'application et comptes réseau en une unité de données unique appelée Identité d'utilisateur. L'identité d'utilisateur est toujours cryptée et protégée par l'authentification multifacteur.

Création d'un mot de passe sécurisé

Lors de la création de mots de passe, vous devez d'abord respecter toutes les spécifications définies par le programme. En règle générale, cependant, tenez compte des instructions suivantes pour vous aider à créer des mots de passe robustes et réduire les risques encourus par vos mots de passe.

- Utilisez des mots de passe contenant plus de 6 caractères, et de préférence plus de 8.
- Mélangez la casse des lettres dans votre mot de passe.
- Lorsque possible, mélangez les caractères alphanumériques et incluez des caractères spéciaux et des signes de ponctuation.
- Remplacez des lettres par des caractères spéciaux ou des nombres dans un mot clé. Par exemple, vous pouvez utiliser le nombre 1 pour la lettre l ou L.
- Combinez des mots provenant de 2 langues ou plus.
- Divisez un mot ou une phrase par des nombres ou des caractères spéciaux au milieu (par exemple, « Mary22Cat45 »).
- N'utilisez pas un mot figurant dans un dictionnaire.
- N'utilisez pas votre nom comme mot de passe, ou toute autre information personnelle, telle qu'une date de naissance, le nom de votre chien ou le nom de jeune fille de votre mère, même si vous l'épelez à l'envers.
- Modifiez régulièrement vos mots de passe. Vous pouvez changer uniquement quelques caractères par incrémentation.
- Si vous prenez note de votre mot de passe, ne le placez pas dans un lieu visible et proche de l'ordinateur.
- N'enregistrez pas le mot de passe dans un fichier, tel qu'un courrier électronique, sur l'ordinateur.
- Ne partagez pas de comptes et ne communiquez votre mot de passe à personne.

Tâches avancées

Gestion de paramètres ProtectTools

Certaines des fonctions de ProtectTools Security Manager peuvent être gérées dans le module BIOS Configuration.

Activation/Désactivation de la prise en charge d'authentification à la mise sous tension de carte Java

Si cette option est disponible, son activation permet d'utiliser la carte Java pour l'authentification d'utilisateur lorsque vous mettez l'ordinateur sous tension.



Remarque Pour activer intégralement la fonction d'authentification à la mise sous tension, vous devez également configurer la carte Java en utilisant le module Java Card Security for ProtectTools.

Pour activer la prise en charge d'authentification à la mise sous tension de carte Java :

1. Sélectionnez **Démarrer > Tous les programmes > HP ProtectTools Security Manager**.
2. Dans le volet gauche, sélectionnez **BIOS Configuration**.
3. Entrez votre mot de passe administrateur Computer Setup à l'invite de mot de passe administrateur BIOS, puis cliquez sur **OK**.
4. Dans le volet gauche, sélectionnez **Security**.
5. Sous **Java Card Security** (Sécurité de carte Java), sélectionnez **Enable** (Activer).



Remarque Pour désactiver l'authentification à la mise sous tension de carte Java, sélectionnez **Disable** (Désactiver).

6. Dans la fenêtre **ProtectTools**, cliquez sur **Apply** (Appliquer), puis sur **OK** pour enregistrer les modifications.

Activation/Désactivation de la prise en charge d'authentification à la mise sous tension pour la sécurité intégrée

Si cette option est disponible, son activation permet au système d'utiliser la puce de sécurité intégrée TPM pour l'authentification d'utilisateur lorsque vous mettez l'ordinateur sous tension.



Remarque Pour activer intégralement la fonction d'authentification à la mise sous tension, vous devez également configurer la puce de sécurité intégrée TPM en utilisant le module Embedded Security for ProtectTools.

Pour activer la prise en charge d'authentification à la mise sous tension pour la sécurité intégrée :

1. Sélectionnez **Démarrer > Tous les programmes > HP ProtectTools Security Manager**.
2. Dans le volet gauche, sélectionnez **BIOS Configuration**.
3. Entrez votre mot de passe administrateur Computer Setup à l'invite de mot de passe administrateur BIOS, puis cliquez sur **OK**.
4. Dans le volet gauche, sélectionnez **Security**.

5. Sous **Embedded Security**, sélectionnez **Enable Power-On Authentication Support** (Activer la prise en charge d'authentification à la mise sous tension).



Remarque Pour désactiver l'authentification à la mise sous tension pour la sécurité intégrée, sélectionnez **Disable** (Désactiver).

6. Dans la fenêtre **ProtectTools**, cliquez sur **Apply** (Appliquer), puis sur **OK** pour enregistrer les modifications.

Gestion de mots de passe Computer Setup

Vous pouvez utiliser BIOS Configuration pour définir et modifier les mots de passe de mise sous tension et de configuration dans Computer Setup, ainsi que pour gérer divers paramètres de mot de passe.



ATTENTION Les mots de passe que vous définissez via la page **Passwords** de BIOS Configuration sont immédiatement enregistrés lorsque vous cliquez sur le bouton **Apply** (Appliquer) ou **OK** de la fenêtre **ProtectTools**. Assurez-vous de mémoriser le mot de passe que vous avez défini car vous ne pouvez pas annuler une définition de mot de passe sans fournir le mot de passe antérieur.

Le mot de passe de mise sous tension peut protéger l'ordinateur d'un accès non autorisé.



Remarque Une fois que vous avez défini un mot de passe de mise sous tension, le bouton **Set** (Définir) de la page **Passwords** est remplacé par le bouton **Change** (Modifier).

Le mot de passe administrateur Computer Setup protège les paramètres de configuration et les informations d'identification système dans Computer Setup. Une fois ce mot de passe défini, il doit être saisi pour accéder à Computer Setup.

Si vous avez défini un mot de passe administrateur, vous serez invité à le fournir avant l'ouverture de la partie BIOS Configuration de ProtectTools.



Remarque Une fois que vous avez défini un mot de passe administrateur, le bouton **Set** (Définir) de la page **Passwords** est remplacé par le bouton **Change** (Modifier).

Définition du mot de passe de mise sous tension (si disponible)

Pour définir le mot de passe de mise sous tension :

1. Sélectionnez **Démarrer > Tous les programmes > HP ProtectTools Security Manager**.
2. Dans le volet gauche, sélectionnez **BIOS Configuration**, puis **Security** (Sécurité).
3. Dans le volet droit, en regard de **Power-On Password** (Mot de passe de mise sous tension), cliquez sur **Set** (Définir).
4. Entrez et confirmez le mot de passe dans les zones **Enter Password** (Entrer le mot de passe) et **Verify Password** (Vérifier le mot de passe).
5. Dans la boîte de dialogue **Passwords** (Mots de passe), cliquez sur **OK**.
6. Dans la fenêtre **ProtectTools**, cliquez sur **Apply** (Appliquer), puis sur **OK** pour enregistrer les modifications.

Modification du mot de passe de mise sous tension (si disponible)

Pour modifier le mot de passe de mise sous tension :

1. Sélectionnez **Démarrer > Tous les programmes > HP ProtectTools Security Manager**.
2. Dans le volet gauche, sélectionnez **BIOS Configuration**, puis **Security** (Sécurité).
3. Dans le volet droit, en regard de **Power-On Password** (Mot de passe de mise sous tension), cliquez sur **Change** (Modifier).
4. Entrez le mot de passe actuel dans la zone **Old Password** (Ancien mot de passe).
5. Définissez et confirmez le nouveau mot de passe dans les zones **Enter New Password** (Entrer le nouveau mot de passe) et **Verify New Password** (Vérifier le nouveau mot de passe).
6. Dans la boîte de dialogue **Passwords** (Mots de passe), cliquez sur **OK**.
7. Dans la fenêtre **ProtectTools**, cliquez sur **Apply** (Appliquer), puis sur **OK** pour enregistrer les modifications.

Configuration système

1. Initialisez HP ProtectTools Embedded Security.
2. Initialisez la clé d'utilisateur de base.

La prise en charge d'authentification à la mise sous tension HP démarre dès que la clé d'utilisateur de base est définie et que le mot de passe utilisateur de base est configuré pour la mise sous tension. Au prochain réamorçage, la prise en charge d'authentification à la mise sous tension HP est initialisée et le mot de passe utilisateur de base doit être utilisé pour démarrer l'ordinateur. Une fois que la prise en charge d'authentification à la mise sous tension fonctionne, l'option de saisie de la configuration du BIOS n'est plus visible. Si l'utilisateur entre le mot de passe de configuration dans la fenêtre de prise en charge d'authentification à la mise sous tension, il accède au BIOS.

Si le mot de passe utilisateur de base de sécurité intégrée est déjà défini, le mot de passe doit être modifié pour établir une protection par mot de passe en utilisant l'authentification à la mise sous tension.

Modification de la prise en charge d'authentification à la mise sous tension

La prise en charge d'authentification à la mise sous tension par mot de passe utilise le mot de passe utilisateur de base de sécurité intégrée. Pour modifier le mot de passe :

1. Accédez aux paramètres F10 BIOS (vous devez disposer du mot de passe de configuration comme décrit dans la procédure Configuration ci-dessous), puis naviguez vers **Security > Embedded Security Device > Reset authentication credential** (Sécurité > Périphérique de sécurité intégrée > Réinitialiser les identités d'authentification).
2. Appuyez sur la touche fléchée pour modifier le paramètre de **Do not reset** (Ne pas réinitialiser) en **Reset** (Réinitialiser).
3. Naviguez vers **Security Manager > Embedded Security > User Settings > Basic User Password > Change** (Gestionnaire de sécurité > Sécurité intégrée > Paramètres utilisateur > Mot de passe utilisateur de base > Modifier).
4. Entrez l'ancien mot de passe, puis entrez et confirmez le nouveau mot de passe.
5. Redémarrez via la prise en charge d'authentification à la mise sous tension.

La fenêtre de mot de passe demande à l'utilisateur de saisir d'abord l'ancien mot de passe.

6. Entrez l'ancien mot de passe, puis entrez le nouveau mot de passe. (Une saisie incorrecte du nouveau mot de passe trois fois de suite affiche une nouvelle fenêtre qui indique que le mot de passe n'est pas valide et que l'authentification à la mise sous tension sera restaurée sur le mot de passe de sécurité intégrée d'origine [F1 = Boot]).

À ce stade, les mots de passe ne seront pas synchronisés et l'utilisateur doit à nouveau modifier le mot de passe de sécurité intégrée pour les resynchroniser.

Modification de comptes utilisateur

L'authentification à la mise sous tension ne prend en charge qu'un seul utilisateur à la fois. La procédure suivante permet de modifier des comptes utilisateur qui contrôlent l'authentification à la mise sous tension.

1. Naviguez vers **F10 BIOS > Security > Embedded Security Device > Reset authentication credential** (F10 BIOS > Sécurité > Périphérique de sécurité intégrée > Réinitialiser les informations d'authentification).
2. Appuyez sur la touche fléchée pour déplacer le curseur latéralement, puis appuyez sur une touche quelconque pour continuer.
3. Appuyez deux fois sur **F10**, puis sur **Entrée** pour enregistrer les modifications et quitter (**Save Changes and Exit**).
4. Créez un utilisateur Microsoft Windows modifié ciblé ou connectez-vous en tant qu'un tel utilisateur existant.
5. Ouvrez le module Embedded Security et initialisez une clé d'utilisateur de base pour le nouveau compte utilisateur Windows. Si une clé d'utilisateur de base existe déjà, modifiez le mot de passe utilisateur de base pour prendre le contrôle de l'authentification à la mise sous tension.

L'authentification à la mise sous tension accepte désormais uniquement le mot de passe utilisateur de base du nouvel utilisateur.



ATTENTION Plusieurs produits sont disponibles au client pour protéger les données via un cryptage logiciel, un cryptage matériel et un matériel. La plupart d'entre eux sont gérés à l'aide de mots de passe. Un échec de gestion de ces outils et mots de passe peut entraîner une perte de données et un verrouillage du matériel, ce qui peut même amener à un remplacement. Passez en revue tous les fichiers d'aide appropriés avant de tenter d'utiliser ces outils.

Définition du mot de passe administrateur Computer Setup

Pour définir le mot de passe administrateur Computer Setup :

1. Sélectionnez **Démarrer > Tous les programmes > HP ProtectTools Security Manager**.
2. Dans le volet gauche, sélectionnez **BIOS Configuration**, puis **Security** (Sécurité).
3. Dans le volet droit, en regard de **Setup Password** (Mot de passe de configuration), cliquez sur **Set** (Définir).
4. Entrez et confirmez le mot de passe dans les zones **Enter Password** (Entrer le mot de passe) et **Confirm Password** (Confirmer le mot de passe).

5. Dans la boîte de dialogue **Passwords** (Mots de passe), cliquez sur **OK**.
6. Dans la fenêtre **ProtectTools**, cliquez sur **Apply** (Appliquer), puis sur **OK** pour enregistrer les modifications.

Modification du mot de passe administrateur Computer Setup

Pour modifier le mot de passe administrateur Computer Setup :

1. Sélectionnez **Démarrer > Tous les programmes > HP ProtectTools Security Manager**.
2. Dans le volet gauche, sélectionnez **BIOS Configuration**, puis **Security** (Sécurité).
3. Dans le volet droit, en regard de **Setup Password** (Mot de passe de configuration), cliquez sur **Change** (Modifier).
4. Entrez le mot de passe actuel dans la zone **Old Password** (Ancien mot de passe).
5. Définissez et confirmez le nouveau mot de passe dans les zones **Enter New Password** (Entrer le nouveau mot de passe) et **Verify New Password** (Vérifier le nouveau mot de passe).
6. Dans la boîte de dialogue **Passwords** (Mots de passe), cliquez sur **OK**.
7. Dans la fenêtre **ProtectTools**, cliquez sur **Apply** (Appliquer), puis sur **OK** pour enregistrer les modifications.

Comportement d'attaque de type Dictionnaire avec authentification à la mise sous tension

Une attaque Dictionnaire est une méthode utilisée pour pénétrer les systèmes de sécurité en testant de manière systématique tous les mots de passe possibles afin de passer outre un système de sécurité. Une attaque Dictionnaire contre le module Embedded Security peut essayer de détecter le mot de passe propriétaire, le mot de passe utilisateur de base ou les clés protégées par mot de passe. Le module Embedded Security propose une défense améliorée contre une telle attaque.

Défense contre une attaque Dictionnaire

La défense du module Embedded Security contre une attaque Dictionnaire contre le mot de passe consiste à détecter les tentatives d'authentification ayant échoué et de désactiver temporairement le module TPM lorsqu'un niveau d'échec donné est atteint. Une fois le niveau d'échec atteint, non seulement le module TPM est désactivé et un redémarrage est requis, mais des délais de verrouillage croissants sont mis en œuvre. Durant la temporisation, la saisie du mot de passe correct sera ignorée. La saisie d'un mot de passe incorrect double la dernière temporisation.

Une documentation supplémentaire sur ce processus est disponible dans l'aide du module Embedded Security. Cliquez sur **Welcome to the HP Embedded Security for ProtectTools Solution > Advanced Embedded Security Operation > Dictionary Attack Defense** (Bienvenue dans la solution HP Embedded Security for ProtectTools > Fonctionnement avancé de sécurité intégrée > Défense contre une attaque Dictionnaire).



Remarque Normalement, un utilisateur reçoit des avertissements indiquant que son mot de passe est incorrect. Les avertissements signalent le nombre de tentatives restantes à l'utilisateur avant que le module TPM ne se désactive lui-même.

Le processus d'authentification à la mise sous tension a lieu dans la ROM avant le chargement du système d'exploitation. La défense contre une attaque Dictionnaire est fonctionnelle, mais le seul avertissement reçu par l'utilisateur est le symbole de clé X.

2 HP BIOS Configuration for ProtectTools

Concepts élémentaires

Le module BIOS Configuration for ProtectTools permet d'accéder aux paramètres de sécurité et de configuration de l'utilitaire Computer Setup. Il permet d'accéder via Windows aux fonctions de sécurité gérées par Computer Setup.

BIOS Configuration permet de réaliser les opérations suivantes :

- Gérer des mots de passe de mise sous tension et des mots de passe administrateur.
- Configurer d'autres fonctions d'authentification à la mise sous tension, telles que l'activation de mots de passe de carte Java et la prise en charge d'authentification de sécurité intégrée.
- Activer et désactiver des fonctions matérielles, telles que l'amorçage via un CD-ROM ou différents ports matériels.
- Configurer des options d'amorçage, notamment le multiamorçage (MultiBoot) et la modification de l'ordre d'amorçage.



Remarque Plusieurs des fonctions de BIOS Configuration for ProtectTools sont également disponibles dans Computer Setup.

Modification des paramètres du BIOS

BIOS Configuration permet de gérer divers paramètres de l'ordinateur qui, sinon, seraient uniquement accessibles par une pression sur la touche **F10** au démarrage et via l'accès à l'utilitaire Computer Setup. Pour plus d'informations sur les paramètres et les fonctions, reportez-vous au *Manuel de l'utilitaire Computer Setup (F10)* disponible sur le CD *Documentation et diagnostics* livré avec l'ordinateur. Pour accéder aux fichiers d'aide du module BIOS Configuration, cliquez sur **Security Manager > BIOS Configuration > Help**.



Remarque Pour obtenir des instructions spécifiques concernant le module BIOS Configuration, reportez-vous aux écrans d'aide ProtectTools.

3 HP Embedded Security for ProtectTools

Concepts élémentaires

S'il est disponible, le module Embedded Security for ProtectTools offre une protection contre tout accès non autorisé aux données utilisateur ou identités. Ce module propose les fonctions de sécurité suivantes :

- Cryptage de fichiers et dossiers EFS (Enhanced Microsoft Encrypting File System)
- Création d'une unité PSD (Personal Secure Drive) pour cryptage des données utilisateur
- Fonctions de gestion des données, telles que sauvegarde et restauration de la hiérarchie des clés
- Prise en charge d'applications tierces basées sur l'interface de programmation MSCAPI (telles que Microsoft Outlook et Microsoft Internet Explorer) et d'applications basées sur les normes PKCS#11 (telle que Netscape) pour les opérations protégées par un certificat numérique, conjointement avec l'utilisation du logiciel de sécurité intégrée.

La puce de sécurité intégrée TPM (Trusted Platform Module) améliore et active d'autres fonctions de sécurité de ProtectTools Security Manager. Par exemple, Credential Manager for ProtectTools peut utiliser la puce de sécurité intégrée TPM comme facteur d'authentification lorsque l'utilisateur se connecte à Windows. Sur certains modèles, la puce de sécurité intégrée TPM active également des fonctions de sécurité du BIOS, accessibles via BIOS Configuration for ProtectTools.

Le matériel consiste en un module TPM conforme aux exigences des normes TPM 1.2 publiées par le Trusted Computing Group. La puce est intégrée sur la carte mère. Certaines mises en œuvre TPM (selon le modèle acheté) intègrent le module TPM comme partie de la carte réseau (NIC). Dans ces configurations NIC et TPM, la mémoire intégrée et non intégrée, les fonctions et le microprogramme sont stockés dans une mémoire flash externe incorporée à la carte mère. Toutes les fonctions TPM sont cryptées ou protégées pour sécuriser les données de la mémoire flash et les communications.

Ce logiciel comporte également une fonction appelée PSD (Personal Secure Drive). Il s'agit d'une fonction complémentaire au cryptage EFS qui se base sur l'algorithme AES (Advanced Encryption Standard). Il convient de noter que cette fonction PSD n'est active que si le module TPM est lui-même activé avec le logiciel approprié, installé avec des droits de propriétaire, et si la configuration de l'utilisateur est initialisée.

Procédures de configuration



ATTENTION Pour réduire les risques de sécurité, il est fortement recommandé que l'administrateur informatique initialise immédiatement la puce de sécurité TPM. Si la puce de sécurité TPM n'est pas initialisée, un utilisateur non autorisé ou un ver informatique pourrait avoir accès à l'ordinateur ou un virus pourrait initialiser la puce TPM et restreindre l'accès à l'ordinateur.

La puce de sécurité TPM peut être activée dans l'utilitaire BIOS Computer Setup, le module BIOS Configuration for ProtectTools ou l'application HP Client Manager.

Pour activer la puce de sécurité intégrée TPM :

1. Ouvrez Computer Setup en démarrant ou redémarrant l'ordinateur, puis en appuyant sur la touche **F10** lorsque le message **F10 = ROM Based Setup** s'affiche dans l'angle inférieur gauche de l'écran.
2. Utilisez les touches de direction pour sélectionner **Security > Setup Password** (Sécurité > Mot de passe de configuration). Définissez un mot de passe.
3. Sélectionnez **Embedded Security Device** (Périphérique de sécurité intégrée).
4. Utilisez les touches de direction pour sélectionner **Embedded Security Device—Disable** (Périphérique de sécurité intégrée—Désactiver). Utilisez les touches de direction pour modifier l'entrée en **Embedded Security Device—Enable** (Périphérique de sécurité intégrée—Activer).
5. Sélectionnez **Enable > Save changes and exit** (Activer > Enregistrer les modifications et quitter).



Remarque Pour obtenir des instructions spécifiques concernant le module ProtectTools Embedded Security, reportez-vous aux écrans d'aide ProtectTools.

4 HP Credential Manager for ProtectTools

Concepts élémentaires

Le module Credential Manager for ProtectTools est doté de fonctions de sécurité qui fournissent un environnement informatique sécurisé et convivial. Ces fonctions incluent les suivantes :

- Alternatives aux mots de passe lors de la connexion à Microsoft Windows, telles que l'utilisation d'une carte Java Card ou d'un lecteur biométrique
- Fonction de signature unique qui mémorise automatiquement les identités (ID utilisateur et mots de passe) pour l'accès aux sites Web, aux applications et aux ressources réseau protégées
- Prise en charge de périphériques de sécurité optionnels, tels que cartes Java et lecteurs biométriques
- Prise en charge de paramètres de sécurité supplémentaires, comme l'obligation d'une authentification par un périphérique optionnel pour déverrouiller l'ordinateur et accéder aux applications
- Cryptage renforcé pour le stockage des mots de passe, en cas d'utilisation d'une puce de sécurité intégrée TPM

Procédure de lancement

Pour lancer Credential Manager, si disponible :

1. Cliquez sur **Démarrer > Panneau de configuration > Security Center > ProtectTools Security Manager > Credential Manager**.
2. Cliquez sur **Log On** (Connexion) dans l'angle supérieur droit du volet.

Vous pouvez vous connecter à Credential Manager de l'une des manières suivantes :

- Assistant de connexion à Credential Manager (recommandé)
- ProtectTools Security Manager



Remarque Si vous utilisez l'invite de connexion à Credential Manager dans l'écran d'ouverture de session Windows pour accéder à Credential Manager, vous vous connectez simultanément à Windows.

Première connexion

La première fois que vous ouvrez Credential Manager, connectez-vous avec votre mot de passe de connexion Windows normal. Un compte Credential Manager est ensuite automatiquement créé avec votre identité de connexion Windows.

Une fois connecté à Credential Manager, vous pouvez enregistrer des informations de connexion supplémentaires, telles qu'une empreinte digitale ou une carte Java.

À la connexion suivante, vous pouvez sélectionner la stratégie de connexion et utiliser toute combinaison des informations de connexion enregistrées.



Remarque Pour obtenir des instructions spécifiques concernant ProtectTools Security Manager, reportez-vous aux écrans d'aide ProtectTools.

5 HP Java Card Security for ProtectTools

Concepts élémentaires

Java Card Security for ProtectTools permet de gérer l'installation et la configuration de cartes Java pour les ordinateurs équipés d'un lecteur de carte Java en option.

HP Java Card Security for ProtectTools permet d'effectuer les opérations suivantes :

- Accéder aux fonctions de sécurité de carte Java
- Initialiser une carte Java afin de pouvoir l'utiliser avec d'autres modules ProtectTools, tels que Credential Manager for ProtectTools
- Si disponible, travailler avec l'utilitaire Computer Setup pour activer l'authentification de cartes Java dans un environnement de préamorçage, et pour configurer des cartes Java distinctes pour un administrateur et un utilisateur. Ceci requiert qu'un utilisateur insère la carte Java et entre au besoin un numéro PIN avant d'autoriser le chargement du système d'exploitation.
- Si disponible, définir et modifier le mot de passe utilisé pour authentifier les utilisateurs de la carte Java
- Si disponible, sauvegarder et restaurer des mots de passe BIOS de carte Java stockés sur la carte Java
- Si disponible, enregistrer le mot de passe BIOS sur la carte Java



Remarque Pour obtenir des instructions spécifiques concernant ProtectTools Security Manager, reportez-vous aux écrans d'aide ProtectTools.

6 Solutions de partie tierce

Les plates-formes contenant un module TPM requièrent une pile TSS (TCG Software Stack) et un logiciel de sécurité intégrée. Tous les modèles sont dotés de la pile TSS, mais le logiciel de sécurité intégrée doit être acheté séparément pour certains modèles. Pour ces modèles, une pile TSS NTRU est fournie pour la prise en charge d'un logiciel de sécurité intégrée de partie tierce acheté par le client. Nous recommandons des solutions de partie tierce telles que Wave Embassy Trust Suite.

7 HP Client Manager pour déploiement distant

Vue d'ensemble

Les plates-formes HP Trustworthy équipées d'une puce TPM (Trusted Platform Module) sont livrées avec le module TPM désactivé (état par défaut). L'activation du module TPM est une option d'administration protégée par des stratégies mises en œuvre par le BIOS HP. L'administrateur doit être présent pour accéder aux options de configuration du BIOS (options F10) pour activer le module TPM. En outre, les spécifications TCG (Trusted Computing Group) requièrent qu'une présence humaine (physique) explicite soit établie pour activer un module TPM. Cette exigence assure que les droits de confidentialité d'un utilisateur sont respectés (en fournissant un modèle de participation à utiliser) et qu'une application inadéquate, un virus ou un cheval de Troie ne puisse pas activer le module TPM à des fins malicieuses. L'établissement d'une présence physique et l'exigence de la présence locale d'un administrateur posent un défi intéressant pour les superviseurs informatiques qui tentent de déployer cette technologie au niveau d'une entreprise de grande taille.

Initialisation

HP Client Manager (HPCM) fournit une méthode d'activation à distance du module TP et de la prise de contrôle de ce module dans un environnement d'entreprise. Cette méthode ne requiert pas la présence physique d'un administrateur informatique, mais satisfait tout de même les exigences TCG.

HPCM permet à l'administrateur informatique de définir certaines options du BIOS, puis de redémarrer le système pour activer le module TPM sur le système distant. Durant ce réamorçage, le BIOS, par défaut, affiche une invite. En réponse, l'utilisateur final doit appuyer sur une touche pour prouver une présence physique, comme spécifié par les exigences TCG. Le système distant poursuit son amorçage et le script se termine en prenant le contrôle du module TPM sur le système. Durant cette procédure, une archive de récupération d'urgence et un jeton de récupération d'urgence sont créés à un emplacement spécifié par l'administrateur informatique.

HPCM n'exécute pas l'initialisation de l'utilisateur du module TPM sur le système distant dans la mesure où l'utilisateur doit être autorisé à choisir le mot de passe. L'initialisation de l'utilisateur du module TPM doit être réalisée par l'utilisateur final de ce système.

Maintenance

HP Client Manager peut être utilisé pour réinitialiser à distance le mot de passe utilisateur sans que l'administrateur informatique ne soit averti de ce mot de passe. HPCM peut également récupérer à distance l'identité de l'utilisateur. Des mots de passe administrateur corrects doivent être fournis pour ces deux fonctions.

8 Résolution des problèmes

Credential Manager for ProtectTools

Brève description	Détails	Solution
En utilisant l'option de comptes réseau Credential Manager, un utilisateur peut sélectionner un compte de domaine pour ouvrir une session. Lorsque l'authentification TPM est utilisée, cette option n'est pas disponible. Toutes les autres méthodes d'authentification fonctionnent correctement.	Avec une authentification TPM, l'utilisateur ne peut ouvrir une session que sur l'ordinateur local.	À l'aide des outils de signature unique Credential Manager, l'utilisateur peut authentifier d'autres comptes.
L'identification par jeton USB n'est pas disponible lors d'une ouverture de session Windows XP Service Pack 1.	Après avoir installé le logiciel du jeton USB, enregistré sa légitimation et configuré Credential Manager comme gestionnaire principal d'ouverture de session, le jeton USB n'apparaît pas dans la liste et n'est pas disponible dans la boîte de dialogue d'ouverture de session Credential Manager ou d'authentification et d'identification graphique. En revenant à Windows pour fermer puis rouvrir la session Credential Manager et sélectionner de nouveau le jeton USB comme légitimation principale, l'ouverture de session par jeton USB fonctionne normalement.	Cela se produit uniquement avec Windows Service Pack 1 ; l'installation du Service Pack 2 via Windows Update résout le problème. Comme solution de rechange en gardant le Service Pack 1, ouvrez une nouvelle session Windows avec une autre légitimation (mot de passe Windows) afin de fermer et rouvrir la session Credential Manager.
Des pages Web de certaines applications génèrent des erreurs qui empêchent l'utilisateur d'accomplir ou de terminer des tâches.	Certaines applications Web cessent de fonctionner et signalent des erreurs en raison du caractère d'invalidation de la signature unique. Par exemple, un ! dans un triangle jaune indiquant qu'une erreur s'est produite, peut être observé dans Internet Explorer.	La signature unique du Credential Manager ne prend pas en charge toutes les interfaces Web. Désactivez la prise en charge de la signature unique pour les pages Web en question. Pour obtenir une documentation plus complète sur la fonction de signature unique, reportez-vous aux fichiers d'aide de Credential Manager. Si une signature unique ne peut pas être désactivée pour une application donnée, appelez l'assistance HP et demandez un support de 3ème niveau via votre contact de service HP.
Aucune option Browse for Virtual Token	L'utilisateur ne peut pas déplacer l'emplacement des jetons virtuels	Cette option Parcourir a été supprimée des versions actuelles du logiciel parce qu'elle permettait à des

Brève description	Détails	Solution
(Parcourir les jetons virtuels) lors de l'ouverture de session.	enregistrés dans Credential Manager, car l'option Parcourir à été supprimée pour des raisons de sécurité.	utilisateurs non enregistrés de supprimer et de renommer des fichiers et de prendre le contrôle de Windows.
L'ouverture de session avec authentification TPM ne présente pas l'option Network Accounts (Comptes réseau).	Avec l'option Network Accounts (Comptes réseau), un utilisateur peut sélectionner un compte de domaine pour ouvrir une session. Lorsque l'authentification TPM est utilisée, cette option n'est pas disponible.	HP recherche actuellement un palliatif pour les prochaines versions du logiciel.
Les administrateurs de domaines ne peuvent pas changer le mot de passe Windows, même avec autorisation.	Cela se produit lorsqu'un administrateur de domaines se connecte à un domaine et enregistre l'identité de ce domaine dans Credential Manager sous un compte avec droits d'administrateur sur le domaine et sur l'ordinateur local. Lorsque l'administrateur de domaines tente de modifier le mot de passe Windows dans Credential Manager, il obtient un message d'échec d'ouverture de session : User account restriction (Restriction du compte utilisateur).	Credential Manager ne peut pas modifier le mot de passe d'un compte utilisateur de domaine par le biais de l'option Change Windows password (Changer le mot de passe Windows). Credential Manager ne peut changer que les mots de passe des comptes de l'ordinateur local. L'utilisateur d'un domaine peut modifier son mot de passe à l'aide de l'option Windows security > Change password (Sécurité Windows > Modifier le mot de passe) mais, comme l'utilisateur du domaine ne possède pas de compte physique sur l'ordinateur local, Credential Manager peut uniquement changer le mot de passe utilisé pour l'ouverture de session.
Le paramétrage par défaut de la signature unique dans Credential Manager devrait afficher une invite afin d'éviter une boucle.	Par défaut, la signature unique est définie de manière à ouvrir automatique la session de l'utilisateur. Cependant, lors de la création d'un second document protégé par un mot de passe différent, Credential Manager utilise le dernier mot de passe enregistré (celui du premier document).	HP recherche actuellement un palliatif pour les prochaines versions du logiciel.
Problèmes d'incompatibilité avec l'authentification et l'identification graphique du mot de passe Corel WordPerfect 12.	Si l'utilisateur ouvre une session Credential Manager, crée un document dans WordPerfect et l'enregistre avec une protection par mot de passe, Credential Manager ne peut pas détecter ou reconnaître le mot de passe d'authentification et d'identification graphique, que ce soit manuellement ou automatiquement.	HP recherche actuellement un palliatif pour les prochaines versions du logiciel.
Credential Manager ne reconnaît pas le bouton Connect (Connecter) à l'écran.	Si les légitimations de signature unique pour la connexion RDP (Remote Desktop Connection) sont définies sur Connect , la signature unique, au redémarrage, entre toujours Save As (Enregistrer sous) au lieu de Connect (Connecter).	HP recherche actuellement un palliatif pour les prochaines versions du logiciel.
L'assistant de configuration ATI Catalyst ne peut pas être utilisé avec Credential Manager.	La signature unique de Credential Manager entre en conflit avec l'assistant de configuration ATI Catalyst.	Désactivez la signature unique de Credential Manager.
Lors d'une ouverture de session avec authentification TPM, le bouton Back (Précédent) saute l'option et passe à une autre méthode d'authentification.	Si l'utilisateur se servant de l'authentification TPM pour Credential Manager saisit son mot de passe, le bouton Back (Précédent) ne fonctionne pas correctement et affiche immédiatement l'écran d'ouverture de session Windows.	HP recherche actuellement un palliatif pour les prochaines versions du logiciel.

Brève description	Détails	Solution
<p>Credential Manager apparaît à la sortie de l'état de veille, alors qu'il est configuré pour ne pas le faire.</p>	<p>Lorsque l'option use Credential Manager log on to Windows (Utiliser Credential Manager pour ouvrir une session Windows) n'est pas sélectionnée, le fait de permettre au système de passer dans l'état S3, puis de le réactiver provoque l'apparition du dialogue d'ouverture de session Credential Manager.</p>	<p>Sans mot de passe administrateur, l'utilisateur ne peut pas ouvrir une session Windows via Credential Manager en raison des restrictions de compte invoquées par Credential Manager.</p> <ul style="list-style-type: none"> • Sans carte Java/jeton, l'utilisateur peut annuler la boîte de dialogue Credential Manager, ce qui fait apparaître la fenêtre d'ouverture de session Windows. L'utilisateur peut alors ouvrir une session. • Sans carte Java/jeton, le palliatif suivant permet à l'utilisateur d'activer/désactiver l'ouverture de Credential Manager à l'insertion de la carte Java. <ol style="list-style-type: none"> 1. Cliquez sur Advanced Settings (Paramètres avancés). 2. Cliquez sur Service & Applications. 3. Cliquez Java Cards and Tokens (Cartes Java et jetons). 4. Cliquez lorsque la carte Java ou le jeton est inséré. 5. Cochez la case Advise to log-on (Conseiller l'ouverture de session).
<p>Si le module TPM est retiré ou endommagé, les utilisateurs perdent toutes les légitimations de Credential Manager protégées par le module TPM.</p>	<p>Les utilisateurs perdent toutes les légitimations protégées par le module TPM si celui-ci est retiré ou endommagé.</p>	<p>Le système est ainsi conçu.</p> <p>Le module TPM est conçu pour protéger les légitimations de Credential Manager. Il est donc conseillé à l'utilisateur de sauvegarder les identités gérées par Credential Manager avant de retirer le module TPM.</p>
<p>Credential Manager n'est pas configuré pour l'ouverture de session principale sous Windows 2000.</p>	<p>Lors de l'installation de Windows 2000, la règle d'ouverture de session est réglée sur « ouverture manuelle » ou « ouverture admin. automatique ». Si le mode automatique est sélectionné, la valeur 1 est enregistrée dans le registre Windows comme valeur par défaut et Credential Manager ne la remplace pas.</p>	<p>Le système est ainsi conçu.</p> <p>Si l'utilisateur souhaite modifier le paramétrage du système d'exploitation pour l'ouverture admin. automatique, la clé du registre est <code>HKEY_LOCAL_MACHINE/Software/Microsoft/WindowsNT/CurrentVersion/WinLogon</code>.</p>
<p> ATTENTION Vous utilisez l'éditeur de registre à vos propres risques ! Une utilisation incorrecte de l'éditeur de registre (regedit) peut causer de sérieux problèmes qui peuvent vous obliger à réinstaller le système d'exploitation. Il n'existe aucune garantie de pouvoir résoudre les problèmes résultant d'un mauvais usage de l'éditeur de registre.</p>		
<p>Le message d'ouverture de session par empreinte digitale apparaît, qu'un lecteur d'empreinte soit ou non installé ou enregistré.</p>	<p>Si l'utilisateur sélectionne l'écran d'ouverture de session Windows, l'alerte suivante apparaît dans la barre des tâches de Credential Manager : You can place your finger on the fingerprint reader to log on to Credential Manager (Vous pouvez placer votre doigt sur le lecteur d'empreinte pour vous connecter à Credential Manager).</p>	<p>Le but de cette alerte est de prévenir l'utilisateur que l'authentification par empreinte digitale est disponible, si elle a été configurée.</p>

Brève description	Détails	Solution
<p>L'écran d'ouverture de session Credential Manager pour Windows 2000 indique insert card (insérer la carte) alors qu'aucun lecteur de carte n'est branché.</p>	<p>L'écran d'accueil de Credential Manager suggère que l'utilisateur peut ouvrir une session par insertion d'une carte alors qu'aucun lecteur de carte Java n'est connecté à l'ordinateur.</p>	<p>Le but de cette alerte est de prévenir l'utilisateur que l'authentification par carte Java est disponible, si elle a été configurée.</p>
<p>Impossible d'ouvrir une session dans Credential Manager après un passage de l'état de veille à l'état de veille prolongée sous Windows XP Service Pack 1 uniquement.</p>	<p>Après avoir permis au système de passer de l'état de veille à l'état de veille prolongée, l'administrateur ou l'utilisateur est incapable d'ouvrir une session dans Credential Manager et l'écran d'ouverture de session Windows reste affiché quelle que soit la légitimation sélectionnée (mot de passe, empreinte digitale ou carte Java).</p>	<p>Ce problème semble résolu par Microsoft dans le Service Pack 2. Pour plus d'informations sur la cause du problème, consultez la Base de connaissances Microsoft, article 813301, à l'adresse http://www.microsoft.com.</p> <p>Pour ouvrir une session, l'utilisateur doit sélectionner Credential Manager et s'y connecter. Une fois la session Credential Manager ouverte, l'utilisateur est invité à ouvrir une session Windows (il se peut qu'il ait à sélectionner l'option d'écran d'accueil Windows) pour achever l'ouverture de session.</p> <p>Si l'utilisateur commence par ouvrir une session Windows, il doit ensuite se connecter manuellement à Credential Manager.</p>

Brève description	Détails	Solution
La restauration de la sécurité intégrée provoque l'échec de Credential Manager.	Une fois le module ROM de sécurité intégrée restauré sur les paramètres usine, Credential Manager ne réussit pas à enregistrer des identités.	<p>Le logiciel HP Credential Manager for ProtectTools ne réussit pas à accéder au module TPM si la ROM a été réinitialisée sur les paramètres usine après l'installation de Credential Manager.</p> <p>La puce de sécurité TPM peut être activée dans l'utilitaire BIOS Computer Setup, le module BIOS Configuration for ProtectTools ou l'application HP Client Manager. Pour activer la puce de sécurité intégrée TPM :</p> <ol style="list-style-type: none"> 1. Ouvrez Computer Setup en démarrant ou redémarrant l'ordinateur, puis en appuyant sur la touche F10 lorsque le message F10 = ROM Based Setup s'affiche dans l'angle inférieur gauche de l'écran. 2. Utilisez les touches de direction pour sélectionner Security > Setup Password (Sécurité > Mot de passe de configuration). Définissez un mot de passe. 3. Sélectionnez Embedded Security Device (Périphérique de sécurité intégrée). 4. Utilisez les touches de direction pour sélectionner Embedded Security Device—Disable (Périphérique de sécurité intégrée—Désactiver). Utilisez les touches de direction pour modifier l'entrée en Embedded Security Device—Enable (Périphérique de sécurité intégrée—Activer). 5. Sélectionnez Enable > Save changes and exit (Activer > Enregistrer les modifications et quitter). <p>HP recherche d'autres solutions pour les prochaines versions du logiciel.</p>
Le processus de sécurité Restore Identity (Restaurer l'identité) perd l'association avec le jeton virtuel.	Lorsque l'utilisateur restaure son identité, Credential Manager peut perdre l'association avec l'emplacement du jeton virtuel dans l'écran d'ouverture de session. Bien que Credential Manager ait enregistré le jeton virtuel, l'utilisateur doit le réenregistrer pour rétablir l'association.	<p>Le système est ainsi conçu.</p> <p>Lorsque Credential Manager est désinstallé sans garder les identités, la partie système (serveur) du jeton est détruite, de sorte que le jeton ne peut plus être utilisé pour l'ouverture de session, même si la partie client du jeton est rétablie par une restauration d'identité.</p> <p>HP recherche des solutions à long terme.</p>

Embedded Security for ProtectTools

Brève description	Détails	Solution
Le chiffrement de dossiers, sous-dossiers et fichiers sur PSD cause un message d'erreur.	Si l'utilisateur copie des fichiers et des dossiers sur l'unité PSD et tente de chiffrer des dossiers/fichiers ou des dossiers/sous-dossiers, le message Error Applying Attributes (Erreur d'application des attributs) s'affiche. L'utilisateur peut chiffrer les mêmes fichiers du disque C:\ sur un disque dur supplémentaire.	Le système est ainsi conçu. Le fait de déplacer des fichiers/dossiers vers l'unité PSD entraîne leur chiffrement. Il n'est pas nécessaire de chiffrer deux fois les fichiers ou dossiers. Toute tentative de chiffrer des fichiers ou dossiers déjà chiffrés provoquera l'affichage de ce message d'erreur.
Prise de possession impossible avec un autre système d'exploitation sur une plate-forme à plusieurs amorçages.	Si un disque dur est configuré pour le démarrage de plusieurs systèmes d'exploitation, la prise de possession ne peut être faite que par l'assistant d'initialisation d'un seul système d'exploitation.	Le système est ainsi conçu pour des raisons de sécurité.
Un administrateur non autorisé peut consulter, supprimer, renommer ou déplacer le contenu de dossiers EFS chiffrés.	Le chiffrement d'un dossier n'empêche pas un intrus possédant des droits d'administrateur de consulter, supprimer ou déplacer le contenu d'un dossier.	Le système est ainsi conçu. Il s'agit d'une caractéristique du système EFS, pas du module TPM de sécurité intégrée. La sécurité intégrée utilise le logiciel EFS de Microsoft dans lequel tous les administrateurs conservent leurs droits d'accès aux fichiers et dossiers.
Les dossiers chiffrés par le système EFS dans Windows 2000 ne sont pas mis en surbrillance en vert.	Les dossiers chiffrés par le système EFS apparaissent en vert dans Windows XP, mais pas dans Windows 2000.	Le système est ainsi conçu. Il s'agit d'une caractéristique propre au système EFS, que le module TPM de sécurité intégrée soit installé ou non.
Le système EFS ne requiert pas de mot de passe pour consulter des fichiers chiffrés dans Windows 2000.	Si un utilisateur initialise la sécurité intégrée, ouvre une session d'administrateur, puis la referme et la rouvre en tant qu'administrateur, il peut ensuite voir les fichiers et dossiers dans Windows 2000 sans mot de passe. Ceci se produit uniquement dans le premier compte administrateur sous Windows 2000. Si une session est établie via un compte administrateur secondaire, ceci ne se produit pas.	Le système est ainsi conçu. Il s'agit d'une caractéristique propre au système EFS sous Windows 2000. Sous Windows XP, le système EFS ne permet pas à l'utilisateur d'ouvrir des dossiers ou des fichiers sans mot de passe.
Le logiciel ne devrait pas être installé sur une partition restaurée en FAT32.	Si l'utilisateur tente de restaurer le disque dur au format FAT32, il n'y aura aucune option de chiffrement pour tous les fichiers ou dossiers utilisant le système EFS.	Le système est ainsi conçu. Le système EFS de Microsoft est uniquement pris en charge par le système de fichiers NTFS et ne fonctionne pas en FAT32. Il s'agit d'une particularité du système EFS de Microsoft qui n'a aucun lien avec le logiciel HP ProtectTools.
Un utilisateur Windows 2000 peut partager une quelconque unité PSD sur le réseau en partage masqué (\$).	Un utilisateur Windows 2000 peut partager une quelconque unité PSD sur le réseau en partage masqué (\$). Le partage masqué est accessible sur le réseau à l'aide du partage masqué (\$).	En principe, l'unité PSD n'est pas partagée sur le réseau, mais elle peut l'être via le partage masqué (\$) sous Windows 2000 uniquement. Il est vivement recommandé de protéger le compte Administrateur par un mot de passe.
Il est possible pour l'utilisateur de chiffrer ou de supprimer le fichier	Par conception, la liste des autorisations d'accès à ce dossier n'est pas définie ; un utilisateur peut donc accidentellement ou volontairement supprimer le fichier et	Le système est ainsi conçu. Les utilisateurs ont accès à un fichier d'archives de secours afin d'enregistrer ou de mettre à jour la copie

Brève description	Détails	Solution
d'archive de restauration XML.	le rendre ainsi inaccessible. Une fois ce fichier chiffré ou supprimé, plus personne ne peut utiliser le logiciel TPM.	de sauvegarde de leur clé utilisateur de base. Il convient donc d'adopter des règles de bonne pratique en matière de sécurité et d'instruire les utilisateurs afin qu'ils ne procèdent pas au chiffrement ou à la suppression des fichiers d'archives.
L'interaction entre le système EFS de la sécurité intégrée HP ProtectTools et Symantec Antivirus ou Norton Antivirus produit des temps d'analyse et de chiffrement/déchiffrement plus longs.	Les fichiers chiffrés interfèrent avec l'analyse Symantec Antivirus ou Norton Antivirus 2005 à la recherche de virus. Pendant l'analyse, l'invite de mot de passe de la clé utilisateur de base demande d'entrer un mot de passe tous les 10 fichiers environ. Si l'utilisateur n'entre pas de mot de passe, le dépassement de temps de l'invite de mot de passe permet à NAV2005 de poursuivre l'analyse. Le chiffrement des fichiers à l'aide du système EFS de la sécurité intégrée HP ProtectTools demande plus de temps lorsque Symantec Antivirus ou Norton Antivirus est activé.	Pour réduire le temps d'analyse des fichiers EFS HP ProtectTools, l'utilisateur peut soit entrer le mot de passe de chiffrement avant l'analyse, soit déchiffrer les fichiers avant de les analyser. Pour minimiser le temps de chiffrement/déchiffrement des données à l'aide du système EFS de la sécurité intégrée HP ProtectTools, l'utilisateur doit désactiver la protection automatique de Symantec Antivirus ou Norton Antivirus.
Le stockage de l'archive de récupération d'urgence sur un support amovible n'est pas pris en charge.	Si l'utilisateur insère une carte mémoire MMC ou SD lors de la création du chemin d'accès au fichier d'archives pendant l'initialisation de la sécurité intégrée, un message d'erreur s'affiche.	Le système est ainsi conçu. Le stockage de l'archive de récupération sur un support amovible n'est pas pris en charge. L'archive de récupération peut être stockée sur un disque réseau ou sur un disque dur local autre que l'unité C.
Impossible de chiffrer des données dans l'environnement Windows 2000 en version française (France).	Le menu contextuel affiché par un clic droit sur l'icône d'un fichier ne présente pas d'option de chiffrement.	Il s'agit d'une limitation du système d'exploitation Microsoft. Si une autre option régionale est sélectionnée (par exemple, français [Canada]), l'option Chiffrer apparaît. Pour contourner le problème, procédez au chiffrement du fichier comme suit : cliquez avec le bouton droit sur l'icône du fichier et sélectionnez Propriétés > Avancées > Chiffrer le contenu .
Des erreurs se produisent après une coupure de courant survenue pendant la prise de possession lors de l'initialisation de la sécurité intégrée.	Si une coupure de courant se produit pendant l'initialisation de la puce de sécurité intégrée, les problèmes suivants apparaissent : <ul style="list-style-type: none"> Lorsque vous tentez de lancer l'assistant d'initialisation de la sécurité intégré, vous obtenez le message d'erreur The Embedded security cannot be initialized since the Embedded Security chip has already an Embedded Security owner (La sécurité intégrée ne peut pas être initialisée car le propriétaire de la puce de sécurité intégrée est déjà défini). Lorsque vous tentez de lancer l'assistant d'initialisation de l'utilisateur, vous obtenez le message d'erreur The Embedded security is not initialized. (La sécurité intégrée n'est pas initialisée.) To use the wizard, the 	Pour restaurer l'état normal après une coupure de courant, procédez comme suit : <p> Remarque Utilisez les touches de direction pour sélectionner différents menus, leurs options, puis changez les valeurs (sauf si indiqué autrement).</p> <ol style="list-style-type: none"> Démarrez ou redémarrez l'ordinateur. Appuyez sur la touche F10 lorsque le message F10=Setup apparaît à l'écran (ou dès que le voyant vert du moniteur s'allume). Sélectionnez l'option de langue appropriée. Appuyez sur Entrée. Sélectionnez Security > Embedded Security (Sécurité > Sécurité intégrée).

Breve description	Détails	Solution
	Embedded Security must be initialized first. (Pour pouvoir utiliser l'Assistant, la sécurité intégrée doit être initialisée.)	<ol style="list-style-type: none"> 6. Définissez l'option Embedded Security Device (Périphérique de sécurité intégrée) sur Enable (Activer). 7. Appuyez sur F10 pour accepter la modification. 8. Sélectionnez File > Save Changes and Exit (Fichier > Enregistrer les modifications et quitter). 9. Appuyez sur ENTRÉE. 10. Appuyez sur F10 pour enregistrer les modifications et quitter l'utilitaire Setup (F10).
Le mot de passe de l'utilitaire Computer Setup (F10) peut être supprimé après l'activation du module TPM.	L'activation du module TPM requiert un mot de passe Computer Setup (F10). Une fois le module TPM activé, l'utilisateur peut supprimer le mot de passe. Cela permet à n'importe qui d'accéder directement au système pour réinitialiser le module TPM avec une perte possible de données.	<p>Le système est ainsi conçu.</p> <p>Le mot de passe de l'utilitaire Computer Setup (F10) ne peut être supprimé que par un utilisateur connaissant ce mot de passe. Il est toutefois vivement recommandé de protéger en permanence l'utilitaire Computer Setup (F10) par un mot de passe.</p>
La boîte de dialogue de mot de passe de l'unité PSD ne s'affiche plus lorsque le système sort d'un mode veille.	Lorsqu'un utilisateur ouvre une session sur le système après avoir créé une unité PSD, le module TPM lui demande le mot de passe utilisateur de base. Si l'utilisateur n'entre pas le mot de passe et que le système passe en mode veille, la boîte de dialogue de mot de passe n'est plus disponible lorsque le système sort du mode veille.	<p>Le système est ainsi conçu.</p> <p>L'utilisateur doit fermer sa session et en ouvrir une nouvelle pour accéder de nouveau à la boîte de dialogue de mot de passe.</p>
Aucun mot de passe n'est requis pour modifier les règles de la plate-forme de sécurité.	L'accès aux règles de la plate-forme de sécurité (machine et utilisateur) ne requiert pas de mot de passe pour les utilisateurs qui ont des droits d'administrateur sur le système.	<p>Le système est ainsi conçu.</p> <p>Tout administrateur peut modifier les règles de la plate-forme de sécurité avec ou sans initialisation TPM.</p>
Microsoft EFS ne fonctionne pas intégralement sous Windows 2000.	Un administrateur peut accéder aux informations chiffrées du système sans connaître le mot de passe correct. Si l'administrateur saisit un mot de passe incorrect ou annule la boîte de dialogue de mot de passe, le fichier chiffré s'ouvre comme si l'administrateur avait saisi correctement le mot de passe. Cela se produit quels que soient les paramètres de sécurité utilisés lors du chiffrement des données. Ceci se produit uniquement dans le premier compte administrateur sous Windows 2000.	<p>La règle de restauration des données est automatiquement configurée de manière à désigner un administrateur comme agent de restauration. Lorsqu'une clé d'utilisateur ne peut pas être récupérée (comme dans le cas d'un mot de passe incorrect ou de l'annulation de la boîte de dialogue de saisie du mot de passe), le fichier est automatiquement déchiffré à l'aide de la clé de restauration.</p> <p>Il s'agit d'une particularité du système EFS de Microsoft. Pour plus d'informations, reportez-vous à l'article Q257705 de la Base de connaissances de Microsoft à l'adresse http://www.microsoft.com.</p> <p>Les documents ne peuvent pas être ouverts par un utilisateur qui ne possède pas de droits d'administrateur.</p>
Lors de la consultation d'un certificat, celui-ci n'apparaît pas comme certificat de confiance.	Une fois HP ProtectTools installé et après avoir exécuté l'Assistant d'initialisation, l'utilisateur peut consulter le certificat émis ; ce certificat n'apparaît cependant pas comme certificat de confiance. Bien qu'il puisse être installé en cliquant sur le bouton Installer,	Les certificats auto-signés ne sont pas des certificats de confiance. Dans un environnement d'entreprise convenablement configuré, les certificats EFS de confiance sont émis en ligne par des autorités de certification.

Brève description	Détails	Solution
	l'installation n'en fait pas un certificat de confiance.	
Erreurs intermittentes de chiffrement et de déchiffrement : Le processus ne peut pas accéder au fichier parce qu'il est utilisé par un autre processus.	Une erreur extrêmement rare se produit pendant le chiffrement ou le déchiffrement, indiquant que le fichier est utilisé par un autre processus, alors que ce fichier ou dossier n'est pas traité par le système d'exploitation ou une application.	Pour résoudre ce problème : <ol style="list-style-type: none"> 1. Redémarrez le système. 2. Déconnectez-vous. 3. Connectez-vous à nouveau.
Une perte de données sur un support amovible se produit si le support est retiré avant un transfert ou une nouvelle génération de données.	Après le retrait d'un support de stockage tel qu'un disque dur MultiBay, le système indique toujours la disponibilité de l'unité PSD et ne génère par d'erreur lors de l'ajout ou de la modification de données sur l'unité PSD. Après redémarrage du système, l'unité PSD ne reflète pas les modifications apportées dans les fichiers après son retrait.	Ce problème ne se rencontre que si l'utilisateur accède à l'unité PSD, puis retire le disque dur avant la fin d'un transfert ou de la génération de nouvelles données. Si l'utilisateur tente d'accéder à l'unité PSD alors que le disque dur n'est pas présent, un message d'erreur s'affiche indiquant que le périphérique n'est pas prêt .
Lors de la désinstallation, si l'utilisateur ouvre l'outil Administration sans avoir initialisé la clé utilisateur de base, l'option Disable (Désactiver) n'est pas disponible et le programme de désinstallation s'arrête tant que l'outil Administration n'est pas refermé.	L'utilisateur a la possibilité de désactiver ou non le module TPM (à l'aide de l'outil Administration) avant de procéder à la désinstallation. L'accès à l'outil Administration requiert l'initialisation de la clé utilisateur de base. Si l'initialisation de base n'est pas faite, l'utilisateur ne peut accéder à aucune option. Comme l'utilisateur a explicitement choisi d'ouvrir l'outil Admin (en cliquant sur Yes (Oui) à l'invite Click Yes to open Embedded Security Administration tool) (Cliquez sur Oui pour ouvrir l'outil d'administration de la sécurité intégrée), le programme de désinstallation attend que l'outil Admin soit refermé. Si l'utilisateur clique sur No (Non), l'outil Admin ne s'ouvre pas du tout et la désinstallation se poursuit.	L'outil Admin permet de désactiver la puce TPM, mais cette option n'est pas disponible tant que la clé utilisateur de base n'est pas initialisée. Si c'est le cas, sélectionnez OK ou Cancel (Annuler) pour poursuivre la désinstallation.
Blocage intermittent du système après avoir créé une unité PSD sur 2 comptes utilisateur et utilisé le changement rapide d'utilisateur dans des systèmes à 128 Mo.	Lors du changement rapide d'utilisateur avec un minimum de mémoire, le système peut se bloquer sur un écran noir et ne répond plus au clavier ni à la souris, au lieu d'afficher l'écran d'accueil (ouverture de session).	La cause première soupçonnée est un problème de trop horloge dans les configurations à minimum de mémoire. L'adaptateur graphique intégré utilise une architecture UMA qui se réserve 8 Mo de mémoire en ne laissant que 120 Mo à l'utilisateur. Ces 120 Mo sont partagés par deux utilisateurs qui ont ouvert une session et qui sont en cours de changement rapide au moment où l'erreur s'est produite. La solution de rechange consiste à redémarrer le système ; il est ensuite vivement conseillé d'augmenter la taille de la mémoire (HP ne livre pas de configurations à 128 Mo avec des modules de sécurité).
L'authentification de l'utilisateur par le système EFS (demande de mot de passe) dépasse la limite de temps avec le	La boîte de dialogue EFS d'authentification de l'utilisateur s'ouvre de nouveau après avoir cliqué sur OK ou lorsque l'état normal est restauré après une mise en veille.	Le système est ainsi conçu. Pour éviter tout problème avec le système EFS de Microsoft, une minuterie de surveillance de 30 secondes est activée pour générer le message d'erreur.

Brève description	Détails	Solution
message access denied (accès refusé).		
La description fonctionnelle est légèrement tronquée pendant l'installation japonaise.	Les descriptions fonctionnelles sont tronquées lors de l'installation personnalisée à l'aide de l'Assistant d'installation.	Ce problème sera résolu par HP dans une prochaine version.
Le chiffrement EFS fonctionne sans entrer de mot de passe à l'invite.	Par un dépassement de temps de l'invite du mot de passe utilisateur, le chiffrement d'un fichier ou d'un dossier est toujours possible.	Cette possibilité de chiffrement ne requiert pas de mot de passe d'authentification, car il s'agit d'une particularité du système EFS de Microsoft. Pour le déchiffrement, il sera toutefois nécessaire de fournir le mot de passe utilisateur.
La messagerie sécurisée est prise en charge, même si cette option n'est pas cochée dans l'Assistant d'initialisation ou si la configuration de la messagerie sécurisée est désactivée dans les règles de l'utilisateur.	Le logiciel de sécurité intégrée et l'Assistant ne vérifient pas le paramétrage d'un client de messagerie (Outlook, Outlook Express ou Netscape).	Ce comportement découle de la conception. La configuration des paramètres de messagerie TPM n'interdit pas l'édition de paramètres de chiffrement dans le client de messagerie. L'utilisation d'une messagerie sécurisée est définie et contrôlée par des applications de partie tierce. L'assistant HP autorise la liaison aux trois applications de référence pour une personnalisation immédiate.
L'exécution d'un déploiement à grande échelle pour une seconde fois sur le même ordinateur, ou sur un ordinateur précédemment initialisé, remplace les fichiers de secours et de restauration d'urgence des clés. Les nouveaux fichiers sont inutilisables pour une restauration.	L'exécution d'un déploiement à grande échelle sur tout système initialisé avec un module de sécurité intégrée HP ProtectTools rend inutilisables les fichiers de restauration xml en les remplaçant par d'autres.	HP s'efforce de résoudre ce problème de remplacement des fichiers xml et fournira une solution dans un prochain SoftPaq.
Les scripts d'ouverture de session automatique ne fonctionnent pas pendant la restauration de l'utilisateur dans la sécurité intégrée.	<p>L'erreur se produit après avoir</p> <ul style="list-style-type: none"> • initialisé le propriétaire et l'utilisateur dans la sécurité intégrée (à l'aide des emplacements par défaut Mes documents), • restauré les paramètres par défaut du BIOS du module TPM, • redémarré l'ordinateur, • commencé à restaurer la sécurité intégrée. Pendant le processus de restauration, l'utilitaire Credential Manager demande à l'utilisateur si le système peut automatiser l'ouverture de session sur « Infineon TPM User Authentication ». Si l'utilisateur choisit Yes (Oui), l'emplacement SPemRecToken apparaît automatiquement dans la zone de texte. 	Cliquez sur le bouton Parcourir pour sélectionner l'emplacement. Le processus de restauration continue.

Brève description	Détails	Solution
	<p>Bien que cet emplacement soit correct, le message d'erreur suivant s'affiche : No Emergency Recovery Token is provided. (Aucun jeton de récupération d'urgence fourni.) Select the token location the Emergency Recovery Token should be retrieved from. (Sélectionnez l'emplacement à partir duquel il doit être récupéré.)</p>	
<p>Les unités PSD de plusieurs utilisateurs ne fonctionnent pas dans un environnement à changement rapide d'utilisateur.</p>	<p>Cette erreur se produit lorsque plusieurs utilisateurs ont été définis et ont reçu une unité PSD identifiée par la même lettre. Lorsqu'un changement rapide d'utilisateur a lieu, une unité PSD étant chargée, l'unité PSD du second utilisateur n'est plus accessible.</p>	<p>L'unité PSD du second utilisateur ne sera de nouveau disponible que si elle est reconfigurée avec une autre lettre d'unité ou si le premier utilisateur ferme sa session.</p>
<p>L'unité PSD est désactivée et ne peut pas être supprimée après formatage du disque dur sur lequel elle a été créée.</p>	<p>L'unité PSD est désactivée et ne peut pas être supprimée après formatage du disque dur secondaire sur lequel elle a été créée. L'icône PSD est toujours visible, mais le message unité de disque inaccessible s'affiche lorsque l'utilisateur tente d'accéder à l'unité PSD.</p> <p>L'utilisateur ne parvient pas à supprimer l'unité PSD et obtient le message : your PSD is still in use, please ensure that your PSD contains no open files and is not accessed by another process (votre unité PSD est en cours d'utilisation, veuillez vous assurer qu'elle ne contient pas de fichiers ouverts et qu'elle n'est pas utilisée par un autre processus). L'utilisateur doit redémarrer le système afin que l'unité PSD soit supprimée et ne soit plus rechargée après le redémarrage.</p>	<p>Le système est ainsi conçu : si un utilisateur force la suppression ou se déconnecte de l'emplacement de stockage des données PSD, l'émulation d'unité PSD de la sécurité intégrée continue de fonctionner et génère des erreurs par perte de liaison aux données manquantes.</p> <p>Solution : après le redémarrage suivant, l'émulation PSD échoue et l'utilisateur peut supprimer l'ancienne émulation PSD et en créer une nouvelle.</p>
<p>Une erreur interne a été détectée lors d'une restauration à partir du fichier de sauvegarde automatique.</p>	<p>Si l'utilisateur</p> <ul style="list-style-type: none"> • Cliquez sur l'option Restore under Backup (Restaurer sous sauvegarde) du logiciel Embedded Security dans HPPTSM, pour effectuer une restauration à partir de la sauvegarde automatique. • Sélectionne SPSystemBackup .xml. <p>L'Assistant de restauration échoue et le message d'erreur suivant s'affiche : The selected Backup Archive does not match the restore reason. (Le fichier de sauvegarde ne correspond pas au motif de restauration). Please select another archive and continue. (Sélectionnez un autre fichier de sauvegarde et poursuivez.)</p>	<p>Si l'utilisateur sélectionne le fichier SpSystemBackup.xml est requis, l'Assistant Embedded Security échoue et affiche le message : An internal Embedded Security error has been detected. (Une erreur interne a été détectée dans la sécurité intégrée.)</p> <p>L'utilisateur doit alors sélectionner le fichier .xml correct qui correspond au motif de restauration.</p> <p>Les processus fonctionnent convenablement tels qu'ils ont été conçus ; le message d'erreur interne de la sécurité intégrée n'est toutefois pas clair et devrait être précisé. HP s'occupe de cette amélioration pour les futures versions.</p>

Brève description	Détails	Solution
Erreur de restauration du système de sécurité avec plusieurs utilisateurs.	Pendant le processus de restauration, si l'administrateur sélectionne les utilisateurs à restaurer, ceux qui ne sont pas sélectionnés ne peuvent plus ultérieurement restaurer les clés. Un message d'erreur s'affiche indiquant l'échec du processus de déchiffrement .	Les utilisateurs non sélectionnés peuvent être restaurés en réinitialisant le module TPM, puis en exécutant la restauration et en sélectionnant tous les utilisateurs avant que la prochaine sauvegarde automatique journalière ne s'exécute. Si cette sauvegarde automatique a lieu, elle remplace les utilisateurs non restaurés et leurs données sont perdues. Si une nouvelle sauvegarde du système est stockée, les utilisateurs précédemment non sélectionnés ne peuvent plus être restaurés. De plus, l'utilisateur doit restaurer la sauvegarde système dans son ensemble. Une sauvegarde d'archives peut être individuellement restaurée.
La restauration de la ROM système sur les paramètres par défaut masque le module TPM.	Lorsque les valeurs par défaut de la ROM système sont restaurées, le module TPM n'est plus visible dans Windows. Il en résulte que le logiciel de sécurité intégrée ne fonctionne plus convenablement et que les données chiffrées par le module TPM ne sont plus accessibles.	Réactivez le module TPM dans le BIOS : Ouvrez l'utilitaire Computer Setup (F10), naviguez vers Security > Device security (Sécurité > Sécurité des périphériques), changez l'option Hidden (Masqué) en Available (Disponible).
La sauvegarde automatique ne fonctionne pas avec une unité mappée.	Lorsqu'un administrateur configure la sauvegarde automatique dans la sécurité intégrée, il crée une entrée dans Windows > Tâches > Tâches planifiées . La tâche planifiée dans Windows est définie de manière à utiliser les droits de NT AUTHORITY\ SYSTEM pour l'exécution de la sauvegarde. Cela fonctionne convenablement sur n'importe quelle unité locale. En revanche, si l'administrateur configure la sauvegarde automatique sur une unité mappée, le processus échoue parce que NT AUTHORITY\SYSTEM ne dispose pas des droits permettant l'utilisation d'une unité mappée. Si l'exécution de la sauvegarde automatique est planifiée à l'ouverture de session, l'icône TNA de la sécurité intégrée affiche le message suivant : The Backup Archive location is currently not accessible. (L'emplacement de l'archive de sauvegarde n'est pas accessible actuellement.) Click here if you want to backup to a temporary archive until the Backup Archive is accessible again. (Cliquez ici si vous désirez créer un fichier de sauvegarde temporaire jusqu'à ce que l'archive de sauvegarde soit de nouveau accessible.) Si la sauvegarde automatique est planifiée à une heure spécifique, elle échoue sans que cet échec soit annoncé.	La solution de rechange consiste à changer NT AUTHORITY\SYSTEM en (nom_ordinateur \ (nom_administrateur)). Il s'agit de la configuration par défaut lorsque la tâche planifiée est créée manuellement. Dans les prochaines versions du logiciel, HP prévoira d'inclure [nom_ordinateur/nom_administrateur] comme paramétrage par défaut.
Impossible de désactiver temporairement l'état de	La version actuelle 4.0 du logiciel a été conçue pour les portables HP Notebook	Ce problème sera résolu par HP dans les prochaines versions.

Brève description	Détails	Solution
la sécurité intégrée dans l'interface graphique du logiciel.	1.1B, ainsi que pour les ordinateurs de bureau HP Desktop 1.2. Cette option de désactivation est toujours prise en charge dans l'interface du logiciel pour les plates-formes TPM 1.1.	

Divers

Logiciel affecté — Brève description	Détails	Solution
<p>HP ProtectTools Security Manager — message d'avertissement : The security application can not be installed until the HP Protect Tools Security Manager is installed (L'application de sécurité ne peut pas être installée tant que le logiciel HP Protect Tools Security Manager n'est pas installé)</p>	<p>Toutes les applications de sécurité comme la sécurité intégrée et les périphériques à carte Java ou biométriques sont des applications additionnelles de l'interface HP Security Manager. Le logiciel HP Security Manager doit donc être installé avant de pouvoir charger une application additionnelle approuvée par HP.</p>	<p>Le logiciel HP ProtectTools Security Manager doit être installé avant d'installer une quelconque application d'extension.</p>
<p>Utilitaire de mise à jour du microprogramme HP ProtectTools TPM pour modèles dc7600 et modèles contenant un module TPM Broadcom. — L'outil mis à disposition sur le site Web HP signale ownership required (possession requise).</p>	<p>Il s'agit d'un comportement attendu de l'utilitaire du microprogramme TPM pour les modèles dc7600 et ceux contenant un module TPM Broadcom.</p> <p>L'outil de mise à jour permet à l'utilisateur de mettre à jour le microprogramme avec ou sans clé d'autorisation (EK). Lorsqu'il n'y a pas de clé, aucune autorisation n'est requise pour accomplir la mise à jour du microprogramme.</p> <p>Lorsqu'il y a une clé d'autorisation, le propriétaire du module TPM doit exister, étant donné que la mise à jour requiert son autorisation. Une fois la mise à jour réussie, la plate-forme doit être redémarrée pour que le nouveau microprogramme prenne effet.</p> <p>Si les paramètres par défaut du BIOS du module TPM sont restaurés, la possession est supprimée et il n'est plus possible de mettre à jour le microprogramme tant que la plate-forme et l'utilisateur n'ont pas été configurés dans l'Assistant d'initialisation.</p> <p>*Un redémarrage est toujours recommandé après une mise à jour du microprogramme. La version du microprogramme n'est correctement détectée qu'après redémarrage.</p>	<ol style="list-style-type: none"> 1. Réinstallez le logiciel HP ProtectTools Embedded Security. 2. Exécutez l'assistant de configuration de la plate-forme et de l'utilisateur. 3. Vérifiez que Microsoft .NET Framework 1.1 est installé sur le système : <ol style="list-style-type: none"> a. Cliquez sur Démarrer. b. Cliquez sur Panneau de configuration. c. Cliquez sur Ajout ou suppression de programmes. d. Vérifiez que Microsoft .NET Framework 1.1 figure dans la liste des programmes. 4. Vérifiez la configuration matérielle et logicielle : <ol style="list-style-type: none"> a. Cliquez sur Démarrer. b. Cliquez sur Tous les programmes. c. Cliquez sur HP ProtectTools Security Manager. d. Sélectionnez Embedded Security (Sécurité intégrée) dans le menu d'arborescence. e. Cliquez sur More Details (Détails). Le système devrait présenter la configuration suivante : <ul style="list-style-type: none"> • Product version (Version de produit) = V4.0.1 • Embedded Security State (État de la sécurité intégrée) : Chip State (Puce) = Enabled (Activée), Owner State (Propriétaire) = Initialized (Initialisé), User State (Utilisateur) = Initialized (Initialisé)

Logiciel affecté — Brève description	Détails	Solution
Une erreur se produit parfois lors de la fermeture de l'interface du Security Manager.	Occasionnellement (1 fois sur 12) une erreur se produit en cliquant sur l'icône de fermeture dans l'angle supérieur droit de la fenêtre du Security Manager avant que le chargement des applications additionnelles soit terminé.	<ul style="list-style-type: none"> • Component Info (Info composants) : TCG Spec. Version = 1.2 • Vendor (Fabricant) = Broadcom Corporation • FW Version (Version microprog.) = 2.18 (ou ultérieure) • TPM Device driver library version (Version de la bibliothèque de drivers de périphériques TPM) = 2.0.0.9 (ou ultérieure) <p>5. Si la version du microprogramme ne correspond pas à 2.18, téléchargez et mettez à jour le microprogramme du module TPM. Le SoftPaq de mise à jour du microprogramme TPM est disponible sur le site http://www.hp.com.</p>
HP ProtectTools * En général— Un accès illimité ou des privilèges d'administration non contrôlés posent un risque pour la sécurité.	Divers risques sont possibles lorsque l'accès au PC client est illimité : <ul style="list-style-type: none"> • suppression de l'unité PSD • modification malveillante des paramètres utilisateur • désactivation des règles et des fonctions de sécurité 	Il est conseillé aux administrateurs d'appliquer des règles de bonne pratique pour limiter les privilèges et l'accès des utilisateurs finaux. Des privilèges d'administration ne devraient pas être accordés à des utilisateurs non autorisés.
Les mots de passe de sécurité intégrée et du BIOS ne sont pas synchronisés.	Si l'utilisateur ne valide pas un nouveau mot de passe en tant que mot de passe de sécurité intégrée du BIOS, le mot de passe de sécurité intégrée du BIOS est restauré sur le mot de passe de sécurité intégrée d'origine via F10 BIOS.	Ceci fonctionne comme conçu ; ces mots de passe peuvent être resynchronisés en modifiant le mot de passe utilisateur de base et en l'authentifiant à l'invite du mot de passe de sécurité intégrée du BIOS.
Un seul utilisateur peut se connecter au système une fois que l'authentification de préamorçage TPM est activée dans le BIOS.	Le numéro PIN du BIOS du module TPM est associé au premier utilisateur qui initialise le paramètre d'utilisateur. Si un ordinateur a plusieurs utilisateurs, le premier utilisateur est, par principe, l'administrateur. Le premier utilisateur devra donner son numéro PIN	Ceci fonctionne comme conçu ; HP recommande que le service informatique du client suive de bonnes stratégies de sécurité pour le déploiement de sa solution de sécurité et s'assure que le mot de passe administrateur du BIOS est configuré par des administrateurs informatiques pour une protection au niveau du système.

Logiciel affecté — Brève description	Détails	Solution
	d'utilisateur TPM aux autres utilisateurs afin de se connecter.	
L'utilisateur doit modifier son numéro PIN pour que le préamorçage TPM fonctionne après une réinitialisation usine du module TPM.	L'utilisateur doit modifier son numéro PIN ou créer un autre utilisateur pour initialiser ce paramètre utilisateur pour que l'authentification BIOS TPM fonctionne après une réinitialisation. Il n'existe aucune option qui permette de rendre l'authentification BIOS TPM fonctionnelle.	Le système est ainsi conçu et la réinitialisation usine efface la clé utilisateur de base. L'utilisateur doit modifier son numéro PIN ou créer un nouvel utilisateur pour réinitialiser la clé utilisateur de base.
La prise en charge d'authentification à la mise sous tension n'est pas définie pour utiliser par défaut l'option Reset to Factory Settings (Restaurer les paramètres usine) de la sécurité intégrée.	Dans Computer Setup, la prise en charge d'authentification à la mise sous tension n'est pas réinitialisée sur les paramètres usine lors de l'utilisation de l'option de périphérique de sécurité intégrée Reset to Factory Settings (Restaurer les paramètres usine). Par défaut, la prise en charge d'authentification à la mise sous tension est définie sur Disable (Désactiver).	L'option Reset to Factory Settings (Restaurer les paramètres usine) désactive le périphérique de sécurité intégrée, qui masque les autres options de sécurité intégrée (y compris la prise en charge d'authentification à la mise sous tension). Toutefois, suite à la réactivation du périphérique de sécurité intégrée, la prise en charge d'authentification à la mise sous tension restait activée. HP s'efforce de trouver une solution, qui sera fournie dans un prochain SoftPaq de ROM de type Web.
L'authentification à la mise sous tension de la sécurité chevauche le mot de passe BIOS durant la séquence d'amorçage.	L'authentification à la mise sous tension invite l'utilisateur à se connecter au système à l'aide du mot de passe TPM mais, si l'utilisateur appuie sur la touche F10 pour accéder au BIOS, seul un accès en lecture est octroyé.	Pour pouvoir écrire vers le BIOS, l'utilisateur doit entrer le mot de passe BIOS au lieu du mot de passe TPM dans la fenêtre de prise en charge d'authentification à la mise sous tension.
Le BIOS demande l'ancien et le nouveau mots de passe via Computer Setup après la modification du mot de passe propriétaire dans le logiciel Windows de sécurité intégrée.	Le BIOS demande l'ancien et le nouveau mots de passe via Computer Setup après la modification du mot de passe propriétaire dans le logiciel Windows de sécurité intégrée.	Le système est ainsi conçu. Ceci est dû à l'incapacité du BIOS à communiquer avec le module TPM, une fois le système d'exploitation démarré et exécuté, et à vérifier la phrase de passe TPM par rapport au blob de clé TPM.

Glossaire

Advanced Encryption Standard (AES) Technique symétrique de chiffrement des données par bloc de 128 bits.

Application Programming Interface (API) Série de fonctions internes du système d'exploitation qui peuvent être utilisées par des applications logicielles pour effectuer diverses tâches.

Archive de récupération d'urgence Zone de stockage protégée qui permet de réencrypter des clés utilisateur de base d'une clé de propriétaire de plate-forme vers une autre.

Authentification Processus permettant de vérifier si un utilisateur est autorisé à exécuter une tâche comme, par exemple, l'accès à un ordinateur, la modification de paramètres pour un programme donné, ou l'affichage de données sécurisées.

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

Autorité de certification Service qui émet les certificats requis pour exécuter 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.

Carte Java Petit composant matériel, ayant la taille et le format d'une carte de crédit, qui stocke des informations d'identification concernant son propriétaire. Utilisée pour authentifier le propriétaire d'un ordinateur.

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

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

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

Cryptage Procédure, telle que l'utilisation d'un algorithme, employée en cryptographie pour convertir un texte normal en un texte codé afin d'empêcher les destinataires non autorisés de lire ces données. Il existe plusieurs types de cryptage de données et ils forment la base de la sécurité d'un réseau. Les types courants incluent le mode Data Encryption Standard et le cryptage par clé publique.

Cryptographic Service Provider (CSP) Fournisseur ou bibliothèque d'algorithmes cryptographiques qui peut être utilisé dans une interface correctement définie dans le but d'exécuter des fonctions cryptographiques spécifiques. Composant logiciel assurant l'interface avec les fonctions MSAPI.

Cryptographie Méthode de cryptage et décryptage de données pouvant uniquement être décodées par des individus spécifiques.

Décryptage Procédure utilisée dans la cryptographie pour convertir en texte normal des données cryptées.

Domaine Groupe d'ordinateurs qui font partie d'un réseau et qui partagent une base de données commune de répertoires. Les domaines sont nommés de manière unique, et chaque domaine possède un ensemble de règles et procédures communes.

Encrypting File System (EFS) Système qui crypte tous les fichiers et sous-dossiers au sein du dossier sélectionné. Service transparent de cryptage de fichiers fourni par Microsoft pour Windows 2000 ou versions ultérieures.

Identité Dans ProtectTools Credential Manager, groupe d'informations d'authentification et de paramètres qui est géré comme le compte ou le profil d'un utilisateur donné.

Informations d'authentification Méthode par laquelle un utilisateur prouve qu'il est autorisé à exécuter une tâche donnée durant le processus d'authentification.

Jeton USB Périphérique de sécurité qui stocke des informations d'identification concernant un utilisateur. Similairement à une carte Java ou un lecteur biométrique, il permet d'authentifier le propriétaire d'un ordinateur.

Jeton virtuel Fonction de sécurité dont le fonctionnement est très semblable à une carte Java ou un lecteur. Le jeton est enregistré sur le disque dur de l'ordinateur ou dans le registre Windows. Lorsque vous connectez à l'aide d'un jeton virtuel, vous êtes invité à fournir le PIN d'un utilisateur pour terminer l'authentification.

Low Pin Count (LPC) Définit l'interface de connexion entre le périphérique de sécurité intégrée HP ProtectTools et le jeu de puces de la plate-forme. Le bus se compose de 4 bits pour les broches d'adresse et de données, d'une horloge de 33 Mhz et de plusieurs broches d'état et de commande.

Microsoft Cryptographic API, ou CryptoAPI (MSCAPI) Interface de programmation de Microsoft permettant aux applications de cryptographie d'accéder aux fonctions du système d'exploitation Windows.

Migration Tâche qui permet de gérer, de restaurer et de transférer des clés et certificats.

Mode de sécurité du BIOS Paramètre du module Java Card Security for ProtectTools qui, lorsqu'il est activé, requiert d'utiliser une carte Java et un PIN valide pour l'authentification de l'utilisateur.

Mot de passe administrateur de carte Java Mot de passe qui lie une carte Java d'administrateur à l'ordinateur dans Computer Setup pour une identification au démarrage ou redémarrage. Ce mot de passe peut être défini manuellement par l'administrateur ou généré de manière aléatoire.

Mot de passe utilisateur de carte Java Mot de passe qui lie une carte Java d'utilisateur à l'ordinateur dans Computer Setup pour une identification au démarrage ou redémarrage. Ce mot de passe peut être défini manuellement par l'administrateur ou généré de manière aléatoire.

Personal Secure Drive (PSD) Fournit une zone de stockage protégée pour des données confidentielles. Fonction offerte par HP ProtectTools Embedded Security. Cette application crée une unité de disque virtuelle sur laquelle l'ordinateur de l'utilisateur stocke automatiquement les fichiers et dossiers sous une forme chiffrée.

Profil BIOS Groupe de paramètres de configuration du BIOS qui peuvent être enregistrés et appliqués à d'autres comptes.

Public Key Cryptographic Standards (PKCS) Normes régissant la définition et l'utilisation des méthodes de cryptage et de décryptage par clé publique ou privée.

Public Key Infrastructure (PKI) Terme général définissant la mise en oeuvre des systèmes de sécurité utilisant le cryptage et le décryptage par clé publique ou privée.

Puce de sécurité intégrée du module TPM (Trusted Platform Module) (certains modèles) Puce de sécurité intégrée qui peut protéger des informations hautement confidentielles contre des attaques malveillantes. Il s'agit de la racine de confiance dans une plate-forme donnée. Le module TPM propose des opérations et des algorithmes cryptographiques conformes aux spécifications TCG (Trusted Computing Group). Le matériel et le logiciel TPM améliorent la sécurité du système de fichiers EFS et de l'unité de disque PSD en protégeant les clés de chiffrement

utilisées. Dans les systèmes sans puce TPM, les clés utilisées par le système de fichiers EFS et l'unité PSD sont normalement stockées sur le disque dur. Ces clés sont donc potentiellement vulnérables. Dans les systèmes équipés d'un module TPM, les clés privées du stockage racine (qui ne quittent jamais la puce TPM) sont utilisées pour protéger les clés de chiffrement EFS et PSD. L'intrusion dans le module TPM pour extraire les clés privées est beaucoup plus difficile que de fouiner sur le disque dur du système pour rechercher ces clés. Le module TPM renforce également la sécurité de la messagerie sécurisée S/MIME dans Microsoft Outlook et Outlook Express. Les fonctions TPM jouent le rôle de fournisseur de service cryptographique CSP (Cryptographic Service Provider). Des clés et des certificats sont générés ou pris en charge par le matériel TPM, ce qui améliore considérablement la sécurité par rapport aux mises en œuvre purement logicielles.

Réamorçage Processus de redémarrage de l'ordinateur.

Secure Multipurpose Internet Mail Extensions (S/MIME) Spécification pour la sécurisation des messages électroniques basée sur les normes PKCS. La spécification S/MIME permet l'authentification par signatures électroniques et assure le secret des données par cryptage.

Sécurité stricte Fonction de sécurité du module BIOS Configuration qui offre une protection renforcée pour les mots de passe de mise sous tension et d'administrateur, ainsi que d'autres formes d'authentification à la mise sous tension.

Signature numérique Données envoyées avec un fichier qui vérifient l'expéditeur du matériel, et que le fichier n'a pas été modifié après sa signature.

Single Sign On (Signature unique) Fonction qui stocke des données d'authentification et qui permet d'utiliser Credential Manager pour accéder à des applications Internet et Windows qui requièrent une authentification par mot de passe.

TCG Software Stack (TSS) Fournit des services permettant de tirer le meilleur parti du module TPM, mais ne requérant pas les mêmes protections. Fournit une interface logicielle standard pour l'accès aux fonctions du module TPM. Pour bénéficier intégralement des possibilités du module TPM, telles que la sauvegarde de clés, la migration de clés, l'authentification de plate-forme et l'attestation, les applications écrivent directement vers la pile TSS.

Trusted Computing Group (TCG) Association d'industriels fondée pour promouvoir le concept d'ordinateur de confiance (« Trusted PC »). Le TGC remplace le TCPA.

Trusted Computing Platform Alliance (TCPA) Cette alliance est actuellement remplacée par le TCG.

Index

A

- agent de récupération de sécurité, mot de passe 4
- assistant de sauvegarde d'identité, mot de passe 5
- attaque Dictionnaire 12
- authentification à la mise sous tension
 - sécurité intégrée 7
- authentification de jeton virtuel, mot de passe 5
- authentification multifacteur, session Credential Manager 5

B

- BIOS
 - définition du mot de passe administrateur 2
 - définition du mot de passe de carte d'administrateur 3
 - définition du mot de passe de carte d'utilisateur 3
 - modification de paramètres 13
- BIOS Configuration for ProtectTools 13

C

- carte Java
 - authentification à la mise sous tension 7
 - définition de PIN 3
 - définition du mot de passe administrateur 3
 - définition du mot de passe de fichier de récupération 3
 - définition du mot de passe utilisateur 3
 - Security for ProtectTools 19
- Client Manager 23

- Client Manager pour déploiement distant 23
- Computer Setup
 - définition du mot de passe administrateur 2, 10
 - gestion de mots de passe 8
 - modification du mot de passe administrateur 11
- Configuration F10, mot de passe 2
- Credential Manager
 - connexion 18
 - installation 17
 - mot de passe de fichier de récupération 4
 - mot de passe de session 4
 - résolution des problèmes 25
 - session 5

E

- Embedded Security for ProtectTools
 - authentification à la mise sous tension 7
 - configuration 16
 - mot de passe 3
 - résolution des problèmes 30
- empreinte digitale, connexion 5

I

- installation de Credential Manager 17

J

- jeton de réinitialisation de mot de passe 4
- jeton virtuel, PIN principal 5
- jeton virtuel, PIN utilisateur 5

L

- logiciels
 - ProtectTools Security Manager 1

M

- mise sous tension
 - attaque Dictionnaire 12
 - changement de mot de passe 9
 - définition de mot de passe 8
 - définition du mot de passe 3
- mise sous tension, authentification carte Java 7
- mot de passe de jeton de récupération d'urgence, définition 3
- mot de passe de préamorçage TPM 3
- mot de passe propriétaire, définition 4
- mots de passe
 - administrateur Computer Setup 2
 - administrateur de carte Java 3
 - agent de récupération de sécurité 4
 - alias d'authentification TPM 5
 - assistant de sauvegarde d'identité 5
 - authentification de jeton USB 5
 - authentification de jeton virtuel 5
 - connexion via empreinte digitale 5
 - définition pour administrateur Computer Setup 10

- définition pour mise sous tension 8
- définitions 2
- fichier de récupération
 - Credential Manager 4
- fichier de récupération de carte Java 3
- gestion dans ProtectTools 2
- gestion pour Computer Setup 8
- instructions 6
- jeton de récupération d'urgence 3
- jeton de réinitialisation de mot de passe 4
- mise sous tension 3
- modification du mot de passe de mise sous tension 9
- modification pour administrateur Computer Setup 11
- PIN de carte Java 3
- PIN principal de jeton virtuel 5
- PIN utilisateur de jeton virtuel 5
- PKCS #12 Import 4
- planificateur de sauvegarde 4
- propriétaire 4
- session Credential Manager 4
- session Windows 4
- utilisateur de base 3
- utilisateur de carte Java 3

P

- PKCS #12, mot de passe 4
- planificateur de sauvegarde, mot de passe 4
- ProtectTools
 - accès à Security Manager 1
 - Credential Manager 17
 - gestion de mots de passe 2
 - gestion de paramètres 7
 - Java Card Security 19
 - modules Security Manager 1
 - sécurité intégrée 15

R

- résolution des problèmes
 - Credential Manager for ProtectTools 25

- divers 38
- Embedded Security for ProtectTools 30

S

- sécurité
 - carte Java 19
 - intégrée pour ProtectTools 15
 - mot de passe de configuration 2
 - rôles 2
- Security Manager, ProtectTools 1
- solutions de partie tierce 21

T

- tâches avancées 7
- TCG Software Stack (TSS) 1, 21
- TPM, alias d'authentification 5

U

- USB, authentification de jeton 5
- utilisateur de base, définition du mot de passe 3

W

- Windows
 - mot de passe de session 4