Solutions IBM Client Security

Logiciel Client Security version 5.3 Guide d'installation

Solutions IBM Client Security

Logiciel Client Security version 5.3 Guide d'installation

Important

Avant d'utiliser le présent document et le produit associé, prenez connaissance des informations figurant dans l'Annexe A, «Réglementation américaine relative à l'exportation du logiciel Client Security», à la page 55 et dans l'Annexe C, «**Remarques**», à la page 61.

Première édition - mai 2004

Compagnie IBM France
Direction Qualité
Tour Descartes
92066 Paris-La Défense Cedex 50

Table des matières

Avant-propos

Cette section fournit des informations sur l'utilisation du présent manuel.

A propos de ce manuel

Le présent manuel contient des informations sur l'installation du logiciel IBM Client Security sur un ordinateur réseau IBM, également appelé client IBM, sur lequel se trouve le sous-système de sécurité intégré IBM. Il présente également des instructions concernant l'activation du sous-système de sécurité intégré IBM et la définition d'un mot de passe administrateur pour le sous-système de sécurité.

Ce manuel est constitué des sections suivantes :

Le Chapitre 1, «Introduction», contient une présentation générale des concepts de sécurité de base, une présentation des applications et composants inclus dans le logiciel et une description des fonctions PKI (Public Key Infrastructure).

Le Chapitre 2, «Mise en route», présente la configuration matérielle et logicielle requise de l'ordinateur, ainsi que les instructions de téléchargement du logiciel.

Le Chapitre 3, «Opérations préalables à l'installation du logiciel», fournit les instructions concernant les opérations prérequises pour l'installation du logiciel IBM Client Security.

Le Chapitre 4, «Installation, mise à jour et désinstallation du logiciel», présente les instructions d'installation, de mise à jour et de désinstallation du logiciel.

Le Chapitre 5, «Identification des incidents», contient les informations utiles pour la résolution des incidents que vous pouvez éventuellement rencontrer en suivant les instructions du présent manuel.

L'Annexe A, «Réglementation américaine relative à l'exportation du logiciel Client Security», contient des informations sur la réglementation américaine régissant l'exportation du logiciel.

L'Annexe B, «Informations relatives aux mots de passe et mots de passe composés», contient les critères en matière de mots de passe composés qui peuvent s'appliquer à un mot de passe composé UVM, ainsi que les règles de définition de mots de passe administrateur.

L'Annexe C, «**Remarques**», contient les remarques légales et les informations sur les marques.

A qui est destiné ce manuel

Ce manuel est destiné aux administrateurs de système ou de réseau qui configurent la sécurité informatique sur les clients IBM. Une bonne connaissance des concepts de sécurité, tels que l'infrastructure de clés publiques (PKI) et la gestion de certificats numériques dans un environnement de réseau, est requise.

Comment utiliser ce manuel

Utilisez ce manuel pour installer et configurer les options de sécurité informatique sur les clients IBM. Ce manuel est associé aux manuels *Logiciel Client Security - Guide d'administration*, *Utilisation du logiciel Client Security avec Tivoli Access Manager* et *Logiciel Client Security - Guide d'utilisation*.

Le présent manuel et tous les autres documents relatifs à Client Security peuvent être téléchargés à partir du site Web IBM http://www.pc.ibm.com/us/security/secdownload.html.

Références au manuel *Logiciel Client Security - Guide d'administration*

Le présent document contient des références au manuel *Logiciel Client Security - Guide d'administration*. Le *Guide d'administration* contient des informations relatives à l'utilisation du gestionnaire de vérification d'utilisateur (UVM) et à la gestion des stratégies UVM, ainsi que des informations sur l'utilisation des utilitaires d'administration et de configuration utilisateur.

Après avoir installé le logiciel, utilisez les instructions du *Guide d'administration* pour configurer et gérer la stratégie de sécurité sur chaque client.

Références au manuel *Logiciel Client Security - Guide d'utilisation*

Le *Guide d'utilisation*, qui est associé au manuel *Logiciel Client Security - Guide d'administration*, contient des informations utiles sur l'exécution des tâches utilisateur Client Security, telles que l'utilisation de la fonction de protection des connexions UVM, la création d'un certificat numérique et l'utilisation de l'utilitaire de configuration utilisateur.

Informations complémentaires

Vous pouvez obtenir des informations complémentaires, ainsi que les mises à jour des produits de sécurité, dès leur disponibilité, à partir du site Web IBM http://www.pc.ibm.com/us/security/index.html.

Chapitre 1. Introduction

Certains ordinateurs ThinkPad et ThinkCentre sont équipés de matériel de chiffrement associé à un logiciel téléchargeable, cette association permettant d'offrir à l'utilisateur un niveau de sécurité très élevé sur une plateforme PC client. Cette association est globalement appelée sous-système de sécurité intégré IBM (ESS). Le composant matériel est la puce de sécurité intégrée IBM et le composant logiciel est le logiciel IBM Client Security (CSS).

Le logiciel Client Security est conçu pour les ordinateurs IBM qui utilisent la puce de sécurité intégrée IBM pour chiffrer et stocker les clés de chiffrement. Il est constitué d'applications et de composants qui permettent aux système client IBM d'utiliser les fonctions de sécurité client à l'échelle d'un réseau local, d'une entreprise ou d'Internet.

Le sous-système de sécurité intégré IBM

Le sous-système IBM ESS prend en charge les solutions de gestion de clés, telles que la fonction PKI (Public Key Infrastructure) et se compose des applications locales suivantes :

- Utilitaire de chiffrement de fichiers et de dossiers (FFE - File and Folder Encryption)
- Password Manager
- Fonction de connexion Windows sécurisée
- Plusieurs méthodes d'authentification configurables, parmi lesquelles :
  - Le mot de passe composé
  - Les empreintes digitales
  - La carte à puce
  - La carte de proximité

Pour pouvoir utiliser de façon efficace les fonctions du sous-système IBM ESS, l'administrateur de la sécurité doit être familiarisé avec certains concepts de base qui sont décrits dans les sections suivantes.

La puce de sécurité intégrée IBM

Le sous-système de sécurité intégré IBM est un élément matériel de chiffrement intégré qui offre un niveau de sécurité intégré supplémentaire sur certaines plateformes PC IBM. Grâce à ce sous-système, les procédures de chiffrement et d'authentification sont transférées de logiciels plus vulnérables vers l'environnement sécurisé d'un matériel dédié. Il fournit une sécurité supplémentaire significative.

Le sous-système de sécurité intégré IBM prend en charge les opérations suivantes :

- Opérations PKI RSA3, telles que le chiffrement de signatures privées et numériques permettant l'authentification
- Génération de clés RSA
- Génération de pseudo nombres aléatoires
- Calcul de la fonction RSA en 200 millisecondes
- Mémoire EEPROM pour le stockage de la paire de clés RSA

- Toutes les fonctions TCPA définies dans la spécification 1.1
- Communication avec le processeur principal via le bus LPC (Low Pin Count)

Logiciel IBM Client Security

Le logiciel IBM Client Security se compose des applications et composants logiciels suivants :

- **Utilitaire d'administration :** Cet utilitaire est l'interface que l'administrateur utilise pour activer ou désactiver le sous-système de sécurité intégré et pour créer, archiver et régénérer les clés de chiffrement et les mots de passe composés. En outre, l'administrateur peut ajouter des utilisateurs dans la stratégie de sécurité fournie par le logiciel Client Security.
- **Console d'administration :** La console d'administration du logiciel Client Security permet à l'administrateur de configurer un réseau itinérant d'accréditation, de créer et de configurer des fichiers qui activent le déploiement, de créer une configuration non administrateur et de récupérer des profils.
- **Utilitaire de configuration utilisateur :** Cet utilitaire permet à l'utilisateur client de modifier le mot de passe composé UVM, d'autoriser la reconnaissance des mots de passe de connexion Windows par UVM, de mettre à jour les archives de clés et d'enregistrer des empreintes digitales. L'utilisateur peut également créer des certificats numériques générés à l'aide du sous-système de sécurité intégré IBM.
- **Gestionnaire de vérification d'utilisateur (UVM) :** Le logiciel Client Security utilise le gestionnaire UVM pour gérer les mots de passe composés et d'autres éléments d'authentification des utilisateurs du système. Par exemple, un lecteur d'empreintes digitales peut être utilisé par le gestionnaire UVM pour l'authentification à l'ouverture de session. Le logiciel Client Security offre les fonctions suivantes :
  - **Protection de stratégie client UVM :** Le logiciel Client Security permet à l'administrateur de la sécurité de définir la stratégie de sécurité client, qui régit le mode d'identification de l'utilisateur client sur le système.

    Si la stratégie indique que l'empreinte digitale est requise pour la connexion et que les empreintes digitales de l'utilisateur ne sont pas enregistrées, ce dernier peut choisir de les enregistrer lors de la connexion. De même, si la vérification d'empreinte digitale est requise et qu'aucun scanneur n'est connecté, UVM renvoie une erreur. Enfin, si le mot de passe Windows n'est pas enregistré ou est enregistré de façon incorrecte dans UVM, l'utilisateur a la possibilité de fournir le mot de passe Windows correct lors de la connexion.
  - **Protection de la connexion au système par UVM :** Le logiciel Client Security permet à l'administrateur de la sécurité de contrôler l'accès à l'ordinateur via une interface d'ouverture de session. La protection UVM garantit que seuls les utilisateurs reconnus par la stratégie de sécurité peuvent accéder au système d'exploitation.

Les relations entre les mots de passe et les clés

Les mots de passe et les clés interagissent, avec d'autres dispositifs d'authentification en option, pour permettre la vérification de l'identité des utilisateurs du système. Il est vital de comprendre les relations entre les mots de passe et les clés pour pouvoir comprendre le mode de fonctionnement du logiciel IBM Client Security.

Le mot de passe administrateur

Le mot de passe administrateur permet d'authentifier un administrateur auprès du sous-système de sécurité intégré IBM. Ce mot de passe, qui doit se composer de 8 caractères, est géré et authentifié dans l'environnement matériel sécurisé du sous-système de sécurité intégré. Une fois authentifié, l'administrateur peut exécuter les actions suivantes :

- Enregistrement d'utilisateurs
- Démarrage de l'interface de stratégie
- Modification du mot de passe administrateur

Le mot de passe administrateur peut être défini par les méthodes suivantes :

- Via l'assistant de configuration du logiciel IBM Client Security
- Via l'utilitaire d'administration
- En utilisant des scripts
- Via l'interface BIOS (ordinateurs ThinkCentre uniquement)

Il est important de définir une stratégie de création et de gestion du mot de passe administrateur. Ce dernier peut être modifié en cas d'oubli ou de divulgation.

Si vous êtes familiarisé avec les concepts et la terminologie TCG (Trusted Computing Group), sachez que le mot de passe administrateur équivaut à l'autorisation du propriétaire. Etant donné que le mot de passe administrateur est associé au sous-système de sécurité intégré IBM, il est parfois appelé *mot de passe matériel*.

Les clés publique et privée matérielles

Le principal intérêt du sous-système de sécurité intégré IBM est qu'il constitue un *point d'ancrage* de sécurité sur un système client. Ce point d'ancrage permet de sécuriser les autres applications et fonctions. Pour créer un point d'ancrage de sécurité, il faut créer une clé publique matérielle et une clé privée matérielle. Une clé publique et une clé privée, également appelées *paire de clés*, sont mathématiquement reliées comme suit :

- Toute donnée chiffrée avec la clé publique peut uniquement être déchiffrée avec la clé privée correspondante.
- Toute donnée chiffrée avec la clé privée peut uniquement être déchiffrée avec la clé publique correspondante.

La clé privée matérielle est créée, stockée et utilisée dans l'environnement matériel sécurisé du sous-système de sécurité. La clé publique matérielle est mise à disposition pour diverses raisons (ce qui explique qu'on la qualifie de publique) mais elle n'est jamais exposée hors de l'environnement matériel sécurisé du sous-système de sécurité. Les clés privée et publique matérielles constituent un élément de base de la hiérarchie de substitution de clés IBM décrite dans une section ultérieure.

Les clés publique et privée matérielles sont créées en utilisant les méthodes suivantes :

- Via l'assistant de configuration du logiciel IBM Client Security
- Via l'utilitaire d'administration
- En utilisant des scripts

Si vous êtes familiarisé avec les concepts et la terminologie TCG (Trusted Computing Group), sachez que les clés publique et privée matérielles sont appelées *clé racine de stockage* (SRK).

Les clés publique et privée administrateur

Les clés publique et privée administrateur font partie intégrante de la hiérarchie de substitution de clés IBM. Elles permettent également la sauvegarde et la restauration des données propres à l'utilisateur en cas de défaillance de la carte mère ou de l'unité de disque dur.

Les clés publique et privée administrateur peuvent être uniques pour chaque système ou être communes pour tous les systèmes ou groupes de systèmes. Il est important de noter que ces clés administrateur doivent faire l'objet d'une gestion. Il est donc primordial de disposer d'une stratégie adéquate.

Les clés publique et privée administrateur peuvent être créées en utilisant les méthodes suivantes :

- Via l'assistant de configuration du logiciel IBM Client Security
- Via l'utilitaire d'administration
- En utilisant des scripts

Archive ESS

Les clés publique et privée administrateur permettent la sauvegarde et la restauration des données propres à l'utilisateur en cas de défaillance de la carte mère ou de l'unité de disque dur.

Clés publique et privée utilisateur

Le sous-système de sécurité intégré IBM crée des clés publique et privée utilisateur pour protéger les données propres à l'utilisateur. Ces paires de clés sont créées lors de l'inscription d'un utilisateur dans le logiciel IBM Client Security. Leur création et leur gestion est effectuée de façon transparente par le composant UVM (User Verification Manager) du logiciel IBM Client Security. Les clés sont gérées en fonction de l'utilisateur Windows connecté au système d'exploitation.

Hiérarchie de substitution de clés IBM

La hiérarchie de substitution de clés IBM constitue un élément fondamental de l'architecture du sous-système de sécurité intégré IBM. La base (ou racine) de la hiérarchie de substitution de clés IBM est constituée par les clés publique et privée matérielles. Ces dernières, appelées *paire de clés matérielles*, sont créées par le logiciel IBM Client Security et sont statistiquement uniques sur chaque client.

Le "niveau" suivant de la hiérarchie (au-dessus de la racine) est constitué par les clés publique et privée administrateur, également appelées *paire de clés administrateur*. Cette paire de clés peut être unique sur chaque machine ou être commune à tous les clients ou sous-ensembles de clients. Le mode de gestion de cette paire de clés varie en fonction de la façon dont vous souhaitez gérer votre réseau. La clé privée administrateur est unique car elle réside sur le système client (protégé par la clé publique matérielle), dans un emplacement défini par l'administrateur.

Le logiciel IBM Client Security enregistre les utilisateurs Windows dans l'environnement du sous-système de sécurité intégré. Lorsqu'un utilisateur est enregistré, une clé publique et une clé privée (*paire de clés utilisateur*) sont créées,

ainsi qu'un nouveau ″niveau″ de clé. La clé privée utilisateur est chiffrée avec la clé publique administrateur. La clé privée administrateur est chiffrée avec la clé publique matérielle. Par conséquent, pour utiliser la clé privée utilisateur, vous devez charger la clé privée administrateur (chiffrée avec la clé publique matérielle) dans le sous-système de sécurité. Une fois ce chargement effectué, la clé privée matérielle déchiffre la clé privée administrateur. Cette dernière est alors prête à être utilisée dans le sous-système de sécurité pour la substitution des données chiffrées avec la clé publique administrateur, leur déchiffrement et leur utilisation. La clé privée utilisateur Windows en cours (chiffrée avec la clé publique administrateur) est transmise au sous-système de sécurité. Toutes les données nécessaires à une application qui déverrouille le sous-système de sécurité intégré sont également transmises à la puce, déchiffrées et déverrouillées dans l'environnement sécurisé du sous-système de sécurité. Cela se produit, par exemple, lorsqu'une clé privée est utilisée pour effectuer une authentification auprès d'un réseau sans fil.

Chaque fois qu'une clé est nécessaire, elle est substituée dans le sous-système de sécurité. Les clés privées chiffrées sont substituées dans le sous-système de sécurité afin de pouvoir ensuite être utilisées dans l'environnement protégé du sous-système. Les clés privées ne sont jamais exposées ou utilisées en dehors de cet environnement matériel. Cela permet de protéger une quantité presque illimitée de données via la puce de sécurité intégrée IBM.

Les clés privées sont chiffrées car elles doivent bénéficier d'une protection élevée et parce qu'il existe un espace de stockage disponible limité dans le sous-système de sécurité intégré IBM. Une seule paire de clés peut être stockée dans le sous-système de sécurité à un moment donné. Les clés publique et privée matérielles sont les seules qui restent stockées dans le sous-système de sécurité entre deux démarrages. Aussi, pour pouvoir faire intervenir plusieurs clés et plusieurs utilisateurs, le logiciel IBM Client Security met en oeuvre la hiérarchie de substitution de clés IBM. Chaque fois qu'une clé est nécessaire, elle est substituée dans le sous-système de sécurité intégré IBM. Les clés privées chiffrées connexes sont substituées dans le sous-système de sécurité afin de pouvoir ensuite être utilisées dans l'environnement protégé de ce dernier. Les clés privées ne sont jamais exposées ou utilisées en dehors de cet environnement matériel.

La clé privée administrateur est chiffrée avec la clé publique matérielle. La clé privée matérielle, qui est uniquement disponible dans le sous-système de sécurité, permet de déchiffrer la clé privée administrateur. Une fois cette clé déchiffrée dans le sous-système de sécurité, une clé privée utilisateur (chiffrée avec la clé publique administrateur) peut être transmise au sous-système de sécurité et déchiffrée avec la clé privée administrateur. Plusieurs clés privées utilisateur peuvent être chiffrées avec la clé publique administrateur. Cela permet la présence d'un nombre virtuellement illimité d'utilisateurs sur un système doté d'IBM ESS. Toutefois, il est bien connu que le fait de limiter le nombre d'utilisateurs inscrits à 25 par ordinateur permet de garantir une performance optimale.

L'IBM ESS utilise une hiérarchie de substitution de clés lorsque les clés privée et publique matérielles présentes dans le sous-système de sécurité sont utilisées pour sécuriser d'autres données stockées en dehors de la puce. La clé privée matérielle est générée dans le sous-système de sécurité et ne quitte jamais cet environnement sécurisé. La clé publique matérielle est disponible en dehors du sous-système de sécurité et est utilisée pour chiffrer ou sécuriser d'autres données telles qu'une clé privée. Une fois les données chiffrées avec la clé publique matérielle, elles peuvent uniquement être déchiffrées par la clé privée matérielle. Etant donné que la clé privée matérielle est uniquement disponible dans l'environnement sécurisé du sous-système de sécurité, les données chiffrées ne peuvent être déchiffrées et

utilisées que dans ce même environnement. Il est important de noter que chaque ordinateur possède une clé privée matérielle et une clé publique matérielle uniques. Le choix de nombres aléatoires dans le sous-système de sécurité intégré IBM assure l'unicité statistique de chaque paire de clés matérielles.

Fonctions PKI (Public Key Infrastructure) CSS

Le logiciel Client Security fournit tous les composants nécessaires à la création d'une infrastructure à clé publique (PKI) dans votre entreprise, tels que :

- **Contrôle de l'administrateur sur la stratégie de sécurité client.** Pour des raisons de stratégie de sécurité, il est essentiel d'authentifier les utilisateurs finals au niveau du client. Le logiciel Client Security offre l'interface requise pour gérer la stratégie de sécurité d'un client IBM. Cette interface fait partie du logiciel d'authentification UVM (Gestionnaire de vérification utilisateur), composant principal du logiciel Client Security.
- **Gestion des clés de chiffrement pour le chiffrement de clés publiques.** A l'aide du logiciel Client Security, les administrateurs créent des clés de chiffrement pour le matériel informatique et les utilisateurs clients. Une fois les clés de chiffrement créées, elles sont liées à la puce de sécurité intégrée IBM par l'intermédiaire d'une hiérarchie de clés, dans laquelle la clé matérielle de base permet de chiffrer les clés de niveau supérieur, y compris les clés utilisateur associées à chaque utilisateur client. Le chiffrement et le stockage des clés dans la puce de sécurité intégrée IBM ajoute un niveau supplémentaire de sécurité du client car les clés sont intimement liées au matériel informatique.
- **Création de certificats numériques et stockage protégé par la puce de sécurité intégrée IBM.** Lorsque vous faites une demande de certificat numérique à utiliser pour la signature et le chiffrement numérique d'un message électronique, le logiciel Client Security vous permet de choisir le sous-système de sécurité intégré IBM comme fournisseur de service pour les applications utilisant Microsoft CryptoAPI. Il peut s'agir des applications Internet Explorer et Microsoft Outlook Express. Ainsi, cela garantit que la clé privée du certificat numérique est chiffrée avec la clé publique utilisateur sur le sous-système de sécurité intégré IBM. De même, les utilisateurs de Netscape peuvent choisir le sous-système de sécurité intégré IBM comme générateur de clé privée pour les certificats numériques utilisés pour la sécurité. Les applications utilisant la norme PKCS (Public-Key Cryptography Standard) 11, telles que Netscape Messenger, peuvent bénéficier de la protection fournie par le sous-système de sécurité intégré IBM.
- **Possibilité de transférer des certificats numériques vers le sous-système de sécurité intégré IBM.** L'outil de transfert de certificats IBM Client Security permet de déplacer des certificats qui ont été créés avec le fournisseur de service cryptographique Microsoft par défaut vers le fournisseur de service cryptographique du sous-système de sécurité intégré IBM. La protection offerte aux clés privées associées aux certificats s'en trouve alors fortement accrue, car les clés sont désormais stockées en toute sécurité sur le sous-système de sécurité intégré IBM et non plus sur un logiciel vulnérable.

  Remarque : Les certificats numériques protégés par le fournisseur de service cryptographique du sous-système de sécurité intégré IBM ne peut pas être exporté vers un autre fournisseur de service cryptographique.

- **Archive de clés et solutions de reprise.** L'une des fonctions importantes de l'architecture PKI est de permettre la création d'une archive de clés, à partir de laquelle des clés peuvent être restaurées en cas de perte des clés d'origine ou si celles-ci sont endommagées. Le logiciel Client Security IBM offre une interface permettant de générer une archive pour les clés et les certificats numériques créés à l'aide du sous-système de sécurité intégré IBM et de les restaurer si nécessaire.
- **Chiffrement de fichiers et de dossiers.** La fonction de chiffrement de fichiers et de dossiers permet à l'utilisateur client de chiffrer ou de déchiffrer des fichiers ou des dossiers. Elle offre un niveau de sécurité des données accru qui vient s'ajouter aux mesures de sécurité système CSS.
- **Authentification d'empreinte digitale.** Le logiciel IBM Client Security prend en charge les lecteurs d'empreinte digitale de carte PC Targus et de port USB Targus pour l'authentification. Ce logiciel doit être installé avant les pilotes de périphériques d'empreinte digitale Targus pour un fonctionnement correct.
- **Authentification par carte à puce.** Le logiciel IBM Client Security prend en charge certaines cartes à puce comme dispositif d'authentification. Il permet d'utiliser des cartes à puce comme jeton d'authentification pour un seul utilisateur à la fois. Chaque carte à puce est reliée à un système sauf si l'itinérance des accréditations est utilisée. L'utilisation obligatoire d'une carte à puce renforce la sécurité de votre système car cette carte doit être fournie accompagnée d'un mot de passe qui, lui, peut être divulgué.
- **Itinérance des accréditations.** L'itinérance des accréditations permet à un utilisateur réseau autorisé d'utiliser tout ordinateur du réseau comme s'il s'agissait de son propre poste de travail. Une fois qu'un utilisateur est autorisé à utiliser UVM sur un client enregistré auprès du logiciel Client Security, il peut importer ses données personnelles sur n'importe quel autre poste client enregistré dans le réseau. Ses données personnelles sont alors automatiquement mises à jour et gérées dans l'archive CSS et sur tout ordinateur sur lequel elles ont été importées. Les mises à jour de ces données personnelles, telles que les nouveaux certificats ou les modifications de mot de passe composé, sont immédiatement disponibles sur tous les autres ordinateurs connectés au réseau itinérant.
- **Certification FIPS 140-1.** Le logiciel Client Security prend en charge les bibliothèques de chiffrement certifiées FIPS 140-1. Des bibliothèques RSA BSAFE certifiées FIPS sont utilisées sur les systèmes TCPA.
- **Péremption du mot de passe composé.** Le logiciel Client Security définit une stratégie de péremption de mot de passe composé et de mot de passe composé spécifique de l'utilisateur lors de l'ajout de chaque utilisateur à UVM.

Chapitre 2. Mise en route

La présente section contient les conditions requises en matière de compatibilité matérielle et logicielle pour une utilisation avec le logiciel IBM Client Security. Elle contient également des informations sur le téléchargement du logiciel IBM Client Security.

Matériel requis

Avant de télécharger et d'installer le logiciel, assurez-vous que votre matériel informatique est compatible avec le logiciel IBM Client Security.

Les informations les plus récentes concernant le matériel et les logiciels requis sont disponibles sur le site Web IBM http://www.pc.ibm.com/us/security/index.html.

Sous-système de sécurité intégré IBM

Le sous-système de sécurité intégré IBM est un microprocesseur de chiffrement intégré à la carte mère du client IBM. Ce composant essentiel du logiciel IBM Client Security transfère les fonctions de stratégie de sécurité des logiciels vulnérables vers un matériel sécurisé, ce qui améliore de façon radicale la sécurité du client local.

Seuls les ordinateurs et les stations de travail IBM qui contiennent le sous-système de sécurité intégré IBM prennent en charge le logiciel IBM Client Security. Si vous essayez de télécharger et d'installer le logiciel sur un ordinateur qui ne contient pas de sous-système de sécurité intégré IBM, le logiciel ne sera pas correctement installé ou il ne fonctionnera pas correctement.

Modèles d'ordinateurs IBM pris en charge

Le logiciel Client Security fourni sous licence prend en charge de nombreux ordinateurs de bureau et portables IBM. Pour obtenir la liste complète des modèles d'ordinateurs pris en charge, reportez-vous à la page Web http://www.pc.ibm.com/us/security/index.html.

Logiciels requis

Avant de télécharger et d'installer le logiciel, assurez-vous que vos logiciels informatiques et votre système d'exploitation sont compatibles avec le logiciel IBM Client Security.

Systèmes d'exploitation

Le logiciel IBM Client Security nécessite un des systèmes d'exploitation suivants :

- Windows XP
- Windows 2000 Professionnel

Produits compatibles avec UVM

IBM Client Security est fourni avec le logiciel Gestionnaire de vérification d'utilisateur (UVM), qui vous permet de personnaliser les règles d'authentification pour votre ordinateur de bureau. Ce premier niveau de contrôle basé sur des stratégies augmente la protection des ressources et l'efficacité de la gestion des

mots de passe. Le gestionnaire UVM, qui est compatible avec les programmes de stratégie de sécurité d'entreprise, vous permet d'utiliser des produits compatibles avec UVM, tels que les produits suivants :

- **Unités biométriques, telles que des lecteurs d'empreinte digitale**

  Le gestionnaire UVM fournit une interface prête à l'emploi pour les unités biométriques. Vous devez installer le logiciel IBM Client Security *avant* d'installer un capteur compatible avec UVM.

  Pour utiliser un capteur compatible avec UVM qui est déjà installé sur un client IBM, vous devez désinstaller ce capteur, installer le logiciel IBM Client Security, puis réinstaller le capteur compatible avec UVM.

- **Tivoli Access Manager versions 3.8 et 3.9**

  Le logiciel UVM simplifie et améliore la gestion des stratégies en s'intégrant parfaitement à une solution centralisée de contrôle d'accès basé sur des stratégies, telle que Tivoli Access Manager.

  Le logiciel UVM applique les stratégies localement, que le système soit en réseau (ordinateur de bureau) ou autonome, créant ainsi un modèle de stratégie unifiée unique.

- **Lotus Notes version 4.5 ou suivante**

  Le gestionnaire UVM s'associe au logiciel IBM Client Security pour améliorer la sécurité de votre connexion à Lotus Notes (Lotus Notes version 4.5 ou suivante).

- **Entrust Desktop Solutions versions 5.1, 6.0 et 6.1**

  Entrust Desktop Solutions améliore les fonctionnalités de sécurité d'Internet au point que des processus entreprise essentiels peuvent être placés sur Internet. Entrust Entelligence fournit un niveau de sécurité unique, qui peut comprendre l'ensemble des besoins en sécurité avancée d'une entreprise, y compris l'identification, la confidentialité, la vérification et la gestion de la sécurité.

- **RSA SecurID Software Token**

  RSA SecurID Software Token permet à l'enregistrement de départ qui est utilisé dans les marqueurs matériels RSA traditionnels d'être intégré aux plateformes utilisateur existantes. En conséquence, les utilisateurs peuvent s'authentifier auprès des ressources protégées en accédant au logiciel intégré au lieu de devoir disposer de périphériques d'authentification dédiés.

- **Lecteur d'empreinte digitale Targus**

  Le lecteur d'empreinte digitale Targus fournit une interface très simple qui permet à une stratégie de sécurité d'inclure l'authentification des empreintes digitales.

- **Badge de proximité Ensure**

  Le logiciel IBM Client Security version 5.2 et suivante nécessite que les utilisateurs d'un badge de proximité mettent à niveau leur logiciel Ensure sur la version 7.41. Lors de la mise à niveau à partir d'une version précédente du logiciel IBM Client Security, mettez à niveau votre logiciel Ensure *avant* le logiciel Client Security version 5.2 ou suivante.

- **Lecteur de carte à puce Gemplus GemPC400**

  Le lecteur de carte à puce Gemplus GemPC400 permet à une stratégie de sécurité d'inclure l'authentification des cartes à puce, en ajoutant ainsi un niveau de sécurité supplémentaire à la protection par mot de passe composé standard.

Navigateurs Web

Le logiciel IBM Client Security prend en charge les navigateurs Web suivants pour les demandes de certificats numériques :

- Internet Explorer version 5.0 ou suivante

- Netscape 4.51-4.7x et Netscape 7.1

Informations sur le chiffrement renforcé du navigateur

Si le dispositif de chiffrement renforcé est installé, utilisez la version 128 bits de votre navigateur Web. Pour vérifier si votre navigateur Web prend en charge le chiffrement renforcé, consultez le système d'aide fourni avec le navigateur.

Services cryptographiques

Le logiciel IBM Client Security prend en charge les services cryptographiques suivants :

- **Microsoft CryptoAPI :** CryptoAPI est le service cryptographique par défaut pour les systèmes d'exploitation et les applications Microsoft. Grâce à la prise en charge intégrée de CryptoAPI, le logiciel IBM Client Security vous permet d'utiliser les fonctions de chiffrement du sous-système de sécurité intégré IBM lorsque vous créez des certificats numériques pour des applications Microsoft.
- **PKCS#11 :** PKCS#11 est le service cryptographique standard pour Netscape, Entrust, RSA et d'autres produits. Après avoir installé le module PKCS#11 du sous-système de sécurité intégré IBM, vous pouvez utiliser le sous-système de sécurité intégré IBM pour générer des certificats numériques pour Netscape, Entrust, RSA et d'autres applications utilisant PKCS#11.

Applications de messagerie

Le logiciel IBM Client Security prend en charge les types d'application de messagerie électronique sécurisée suivants :

- les applications de messagerie qui utilisent le service Microsoft CryptoAPI pour les opérations cryptographiques, telles que Outlook Express et Outlook (lorsqu'il est utilisé avec une version prise en charge d'Internet Explorer) ;
- les applications de messagerie qui utilisent le service PKCS#11 (Public Key Cryptographic Standard #11) pour les opérations cryptographiques, telles que Netscape Messenger (lorsqu'il est utilisé avec une version prise en charge de Netscape).

Téléchargement du logiciel

Vous pouvez télécharger le logiciel Client Security à partir du site Web IBM http://www.pc.ibm.com/us/security/index.html.

Formulaire d'enregistrement

Lorsque vous téléchargez le logiciel, vous devez remplir un formulaire d'enregistrement et un questionnaire, et accepter les termes du contrat de licence. Suivez les instructions fournies sur le site Web IBM http://www.pc.ibm.com/us/security/index.html pour télécharger le logiciel.

Les fichiers d'installation du logiciel IBM Client Security sont inclus dans le fichier auto-extractible nommé `csec53.exe` .

Réglementations régissant l'exportation

Le logiciel IBM Client Security contient un code de chiffrement qui peut être téléchargé en Amérique du Nord et au niveau international. Si vous résidez dans un pays où le téléchargement d'un logiciel de chiffrement à partir d'un site Web basé aux Etats-Unis est interdit, vous ne pouvez pas télécharger le logiciel IBM Client Security. Pour plus d'informations sur les réglementations régissant l'exportation du logiciel IBM Client Security, reportez-vous à l'Annexe A, «Réglementation américaine relative à l'exportation du logiciel Client Security», à la page 55.

Chapitre 3. Opérations préalables à l'installation du logiciel

Cette section contient les instructions à suivre avant de lancer le programme d'installation et de configurer le logiciel IBM Client Security sur les clients IBM.

Tous les fichiers requis pour l'installation du logiciel Client Security sont fournis sur le site Web IBM http://www.pc.ibm.com/us/security/index.html. Ce site Web fournit des informations qui vous permettent de vous assurer que votre système est doté du sous-système de sécurité intégré IBM et de sélectionner l'offre IBM Client Security appropriée pour votre système.

Avant d'installer le logiciel

Le programme d'installation installe le logiciel IBM Client Security sur le client IBM et active le sous-système de sécurité intégré IBM. Cependant, l'installation spécifique varie en fonction d'un certain nombre de facteurs.

Installation sur des clients dotés de Windows XP ou Windows 2000

Les utilisateurs de Windows XP et Windows 2000 doivent se connecter avec des droits d'administrateur pour installer le logiciel IBM Client Security.

Installation en vue d'une utilisation avec Tivoli Access Manager

Si vous envisagez d'utiliser Tivoli Access Manager pour contrôler les règles d'authentification définies pour votre ordinateur, vous devez installer certains composants de Tivoli Access Manager *avant* d'installer le logiciel IBM Client Security. Pour plus de détails, reportez-vous au manuel *Utilisation du logiciel Client Security avec Tivoli Access Manager*.

Remarques sur les fonctions de démarrage

Deux fonctions de démarrage IBM peuvent affecter la façon dont vous activez le sous-système de sécurité intégré IBM et dont vous générez les clés de chiffrement. Ces fonctions sont le mot de passe administrateur et la sécurité avancée. Vous pouvez y accéder à partir du programme de configuration d'un ordinateur IBM. Le logiciel IBM Client Security est doté d'un mot de passe administrateur distinct. Pour éviter toute confusion, le mot de passe administrateur défini dans le programme de configuration est appelé *mot de passe administrateur BIOS* dans les manuels du logiciel Client Security.

Mot de passe administrateur BIOS

Un mot de passe administrateur BIOS empêche les personnes non autorisées de modifier les paramètres de configuration d'un ordinateur IBM. Ce mot de passe est défini à l'aide du programme de configuration sur un ordinateur NetVista ou ThinkCentre ou à l'aide de l'utilitaire de configuration du BIOS IBM sur un ThinkPad. Le programme approprié est accessible en appuyant sur la touche F1 lors de la séquence d'amorçage de l'ordinateur. Ce mot de passe est appelé mot de passe administrateur dans le programme de configuration et dans l'utilitaire de configuration du BIOS IBM.

Sécurité avancée

La sécurité avancée assure une protection supplémentaire du mot de passe administrateur BIOS et des paramètres de la séquence d'amorçage. Vous pouvez déterminer si la sécurité avancée est activée ou désactivée à l'aide du programme de configuration, qui est accessible en appuyant sur F1 pendant la séquence d'amorçage de l'ordinateur.

Pour plus d'informations sur les mots de passe et la sécurité avancée, reportez-vous à la documentation fournie avec l'ordinateur.

Sécurité avancée sur les ordinateurs NetVista modèles 6059, 6569, 6579, 6649 et sur tous les modèles Q1x : Si un mot de passe administrateur a été défini sur les ordinateurs NetVista modèles 6059, 6569, 6579, 6649, 6646 et tous les modèles Q1x, vous devez ouvrir l'utilitaire d'administration pour activer le sous-système de sécurité intégré IBM et générer les clés de chiffrement.

Lorsque la sécurité avancée est activée sur ces modèles, vous devez utiliser l'utilitaire d'administration pour activer le sous-système de sécurité intégré IBM et générer les clés de chiffrement *après* l'installation du logiciel IBM Client Security. Si le programme d'installation détecte que la sécurité avancée est activée, vous en êtes averti à la fin de la procédure d'installation. Redémarrez alors l'ordinateur et ouvrez l'utilitaire d'administration pour activer le sous-système de sécurité intégré IBM et générer les clés de chiffrement.

Sécurité avancée sur tous les autres modèles de NetVista (autres que les modèles 6059, 6569, 6579, 6649 et tous les modèles Q1x) : Si un mot de passe administrateur a été défini sur les autres modèles de NetVista, le système *ne* vous demande *pas* de saisir le mot de passe administrateur au cours de la procédure d'installation.

Lorsque la sécurité avancée est activée sur ces modèles de NetVista, vous pouvez utiliser le programme d'installation pour installer le logiciel, mais vous devez faire appel au programme de configuration pour activer le sous-système de sécurité intégré IBM. *Après* avoir activé le sous-système de sécurité intégré IBM, vous pouvez utiliser l'utilitaire d'administration pour générer les clés de chiffrement.

Informations sur la mise à jour du BIOS

Avant d'installer le logiciel, vous devrez peut-être télécharger la dernière version du code BIOS sur votre ordinateur. Pour déterminer le niveau de BIOS utilisé par votre ordinateur, redémarrez l'ordinateur et appuyez sur F1 pour lancer le programme de configuration. Lorsque le menu principal du programme de configuration s'affiche, sélectionnez Product Data pour afficher les informations relatives au code BIOS. Le niveau du code BIOS est également appelé niveau de révision de l'EEPROM.

Pour exécuter le logiciel IBM Client Security version 2.1 ou suivante sur les NetVista modèles 6059, 6569, 6579 et 6649, vous devez utiliser le niveau de BIOS xxxx22axx ou suivant. Pour exécuter le logiciel IBM Client Security version 2.1 ou suivante sur les NetVista modèles 6790, 6792, 6274 et 2283, vous devez utiliser le niveau de BIOS xxxx20axx ou suivant. Pour plus d'informations, consultez le fichier README inclus avec le téléchargement du logiciel.

Pour rechercher les dernières mises à jour du code BIOS disponibles pour votre ordinateur, allez sur le site Web IBM http://www.pc.ibm.com/support, tapez `bios` dans la zone de recherche, sélectionnez Downloadable Files dans la liste déroulante et appuyez sur Entrée. Une liste de mises à jour du code BIOS s'affiche. Cliquez sur le numéro de modèle approprié et suivez les instructions de la page Web.

Utilisation de la paire de clés administrateur pour l'archivage de clés

La paire de clés d'archive est simplement une copie de la paire de clés administrateur que vous stockez sur un système éloigné en vue d'une restauration. Etant donné que vous utilisez l'utilitaire d'administration pour créer la paire de clés d'archive, vous devez installer le logiciel IBM Client Security sur un client IBM initial, avant de pouvoir créer la paire de clés administrateur.

Chapitre 4. Installation, mise à jour et désinstallation du logiciel

Cette section contient les instructions de téléchargement, d'installation et de configuration du logiciel IBM Client Security sur les clients IBM. Elle contient également les instructions de désinstallation du logiciel. Veillez à installer le logiciel IBM Client Security avant d'installer un des divers utilitaires qui améliorent les fonctionnalités de Client Security.

Important : Si vous effectuez une mise à niveau à partir de versions antérieures à la version 5.0 du logiciel IBM Client Security, vous *devez* déchiffrer tous les fichiers chiffrés *avant* d'installer le logiciel Client Security version 5.1 ou suivante. En effet, le logiciel IBM Client Security version 5.1 ou suivante ne peut pas déchiffrer les fichiers qui ont été chiffrés à l'aide des versions de Client Security antérieures à la version 5.0 en raison des modifications apportées à la mise en oeuvre du chiffrement des fichiers.

Téléchargement et installation du logiciel

Tous les fichiers requis pour l'installation du logiciel Client Security sont fournis sur le site Web IBM http://www.pc.ibm.com/us/security/index.html. Ce site Web fournit des informations qui vous permettent de vous assurer que votre système est doté du sous-système de sécurité intégré IBM et de sélectionner l'offre IBM Client Security appropriée pour votre système.

Pour télécharger les fichiers appropriés pour votre système, procédez comme suit :

1. A l'aide d'un navigateur Web, accédez au site Web IBM http://www.pc.ibm.com/us/security/index.html.
2. Cliquez sur **Download instructions and links**.
3. Dans la zone de téléchargement des informations du logiciel IBM Client Security, cliquez sur le bouton **Continue**.
4. Cliquez sur **Detect my system & continue** ou entrez le numéro de modèle/type de votre machine (à 7 chiffres) dans la zone appropriée.
5. Créez un ID utilisateur, enregistrez-vous auprès d'IBM en complétant le formulaire en ligne et lisez le contrat de licence, puis cliquez sur **Accept Licence**.

   Vous êtes alors automatiquement redirigé vers la page de téléchargement d'IBM Client Security.
6. Suivez les étapes de la page de téléchargement pour télécharger les pilotes de périphérique nécessaires, les fichiers readme, le logiciel, les documents de référence et les utilitaires complémentaires du logiciel IBM Client Security. Respectez l'ordre de téléchargement indiqué sur le site Web.
7. A partir du bureau Windows, cliquez sur **Démarrer > Exécuter**.
8. Dans la zone Exécuter, tapez `d:\directory\csec53.exe` , où d:\répertoire\ correspond à l'unité et au répertoire où se trouve le fichier.
9. Cliquez sur **OK**.

   L'écran de bienvenue de l'assistant d'installation du logiciel IBM Client Security s'affiche.

10. Cliquez sur **Suivant**.

    L'assistant extrait les fichiers et installe le logiciel. Lorsque l'installation est terminée, vous avez le choix entre redémarrer l'ordinateur immédiatement ou ultérieurement.

11. Sélectionnez l'option de redémarrage immédiat de l'ordinateur et cliquez sur **OK**.

    L'assistant d'installation du logiciel IBM Client Security s'affiche au redémarrage de l'ordinateur.

Utilisation de l'assistant d'installation du logiciel IBM Client Security

L'assistant d'installation du logiciel IBM Client Security fournit une interface qui vous aide à installer le logiciel Client Security et à activer la puce de sécurité intégrée IBM. Il guide également les utilisateurs tout au long de l'exécution des tâches nécessaires pour configurer une stratégie de sécurité sur un client IBM.

Les étapes à suivre sont les suivantes :

- **Définition d'un mot de passe administrateur de sécurité**

  Le mot de passe administrateur de sécurité permet de contrôler l'accès à l'utilitaire d'administration d'IBM Client Security, qui est utilisé pour modifier les paramètres de sécurité de l'ordinateur. Ce mot de passe doit contenir exactement huit caractères.

- **Création des clés de sécurité administrateur**

  Les clés de sécurité administrateur sont un ensemble de clés numériques qui sont stockées dans un fichier informatique. Ces fichiers de clés sont également appelés clés administrateur, paires de clés administrateur ou paire de clés d'archive. Il est recommandé de sauvegarder ces clés de sécurité essentielles sur une unité ou un disque amovible. Lorsqu'une modification est apportée à la stratégie de sécurité dans l'utilitaire d'administration, le système vous demande de fournir une clé administrateur pour prouver que la modification de la stratégie est autorisée.

  Les informations de sécurité sont également sauvegardées au cas où vous devriez remplacer la carte mère ou l'unité de disque dur de votre ordinateur. Stockez ces informations de sauvegarde hors du système local.

- **Protection des applications à l'aide d'IBM Client Security**

  Sélectionnez les applications que vous voulez protéger à l'aide d'IBM Client Security. Il est possible que certaines options ne soient pas disponibles si vous n'avez pas installé les applications nécessaires.

- **Affectation d'autorisations aux utilisateurs**

  Les utilisateurs doivent disposer d'une autorisation pour pouvoir accéder à l'ordinateur. Lorsque vous affectez une autorisation à un utilisateur, vous devez indiquer le mot de passe composé de cet utilisateur. Les utilisateurs non autorisés ne peuvent pas utiliser l'ordinateur.

- **Sélection du niveau de sécurité du système**

  En sélectionnant un niveau de sécurité système, vous pouvez établir une stratégie de sécurité de base rapidement et facilement. Vous pouvez ultérieurement définir une stratégie de sécurité personnalisée à l'aide de l'utilitaire d'administration d'IBM Client Security.

Pour utiliser l'assistant d'installation du logiciel IBM Client Security, procédez comme suit :

1. Si l'assistant n'est pas encore ouvert, cliquez sur **Démarrer > Programmes > Access IBM > Logiciel IBM Client Security > Assistant d'installation d'IBM Client Security**.

   L'écran de bienvenue dans l'assistant d'installation d'IBM Client Security affiche la présentation générale des étapes à suivre.

   Remarque : Si vous envisagez d'utiliser la fonction d'authentification des empreintes digitales, vous devez installer le logiciel correspondant et le lecteur d'empreinte digitale avant de continuer.

2. Cliquez sur **Suivant** pour commencer à utiliser l'assistant.

   L'écran Définition du mot de passe administrateur de sécurité s'affiche.

3. Saisissez le mot de passe administrateur de sécurité dans la zone Saisie du mot de passe administrateur et cliquez sur **Suivant**.

   Remarque : Lors de l'installation initiale ou si la puce de sécurité intégrée IBM a été vidée, vous êtes invité à confirmer le mot de passe administrateur de sécurité dans la zone Confirmation du mot de passe administrateur. Vous pouvez également être invité à fournir votre mot de passe superviseur, le cas échéant.

   L'écran Création des clés de sécurité administrateur s'affiche.

4. Exécutez l'une des opérations suivantes :
   - **Création de nouvelles clés de sécurité**

     Pour créer de nouvelles clés de sécurité, procédez comme suit :

     a. Cliquez sur le bouton d'option **Création de nouvelles clés de sécurité**.
     b. Indiquez où vous voulez sauvegarder les clés de sécurité administrateur en saisissant le chemin d'accès dans la zone correspondante ou en cliquant sur le bouton **Parcourir** pour sélectionner le dossier approprié.
     c. Si vous voulez diviser la clé de sécurité pour obtenir une meilleure protection, cochez la case **Division de la clé de sécurité de sauvegarde pour une sécurité accrue**, puis utilisez les flèches pour sélectionner le nombre voulu dans la zone déroulante **Nombre de divisions**.

   - **Utilisation d'une clé de sécurité existante**

     Pour utiliser une clé de sécurité existante, procédez comme suit :

     a. Cliquez sur le bouton d'option **Utilisation d'une clé de sécurité existante**.
     b. Indiquez l'emplacement de la clé publique en saisissant le chemin d'accès dans la zone correspondante ou en cliquant sur le bouton **Parcourir** pour sélectionner le dossier approprié.
     c. Indiquez l'emplacement de la clé privée en saisissant le chemin d'accès dans la zone correspondante ou en cliquant sur le bouton **Parcourir** pour sélectionner le dossier approprié.

5. Indiquez où vous voulez sauvegarder les copies de sauvegarde de vos informations de sécurité en saisissant le chemin d'accès dans la zone correspondante ou en cliquant sur le bouton **Parcourir** pour sélectionner le dossier approprié.
6. Cliquez sur **Suivant**.

   L'écran Protection des applications à l'aide d'IBM Client Security s'affiche.

7. Activez la protection IBM Client Security en cochant les cases appropriées et en cliquant sur **Suivant**. Les options Client Security disponibles sont les suivantes :
   - **Protection de l'accès à votre ordinateur par le remplacement de la fenêtre de connexion Windows standard par la fenêtre de connexion sécurisée Client Security**

     Cochez cette case pour remplacer la fenêtre de connexion Windows normale par la fenêtre de connexion sécurisée Client Security. Cette option accroît la sécurité de votre système et ne permet la connexion qu'après l'authentification à l'aide de la puce de sécurité intégrée IBM et de périphériques en option, tels que des lecteurs d'empreinte digitale ou des cartes à puce.
   - **Activation du chiffrement de fichiers et de dossiers**

     Cochez cette case si vous voulez sécuriser les fichiers situés sur votre unité de disque dur à l'aide de la puce de sécurité intégrée IBM. (Cette option suppose que vous téléchargiez l'utilitaire de chiffrement des fichiers et dossiers IBM Client Security.)
   - **Activation de la prise en charge du gestionnaire de mots de passe IBM Client Security**

     Cochez cette case si vous voulez utiliser le gestionnaire de mots de passe IBM pour enregistrer de manière pratique et sûre les mots de passe définis pour les applications et les connexions aux sites Web. (Cette option suppose que vous téléchargiez l'application Gestionnaire de mots de passe IBM Client Security.)
   - **Remplacement de la connexion à Lotus Notes par la connexion à IBM Client Security**

     Cochez cette case si vous voulez que le logiciel Client Security authentifie les utilisateurs de Lotus Notes à l'aide de la puce de sécurité intégrée IBM.
   - **Activation de la prise en charge d'Entrust**

     Cochez cette case si vous voulez permettre l'intégration des produits logiciels de sécurité Entrust.
   - **Protection de Microsoft Internet Explorer**

     Cette protection vous permet de sécuriser vos communications électroniques et la navigation sur le Web avec Microsoft Internet Explorer (un certificat numérique est requis). La prise en charge de Microsoft Internet Explorer est activée par défaut.

   Une fois que vous avez coché les cases appropriées, l'écran Affectation d'autorisations aux utilisateurs s'affiche.
8. Renseignez cet écran en procédant comme suit :
   - Pour autoriser des utilisateurs à exécuter des fonctions d'IBM Client Security, procédez comme suit :
     a. Sélectionnez un utilisateur dans la zone Utilisateurs non autorisés.
     b. Cliquez sur **Autorisation utilisateur**.
     c. Saisissez et confirmez votre mot de passe composé IBM Client Security dans les zones appropriées et cliquez sur **Suivant**.

        L'écran Expiration du mot de passe composé UVM s'affiche.
     d. Définissez le délai d'expiration du mot de passe composé pour l'utilisateur et cliquez sur **Fin**.
     e. Cliquez sur **Suivant**.

- Pour interdire à des utilisateurs d'exécuter des fonctions d'IBM Client Security, procédez comme suit :
  a. Sélectionnez un utilisateur dans la zone Utilisateurs autorisés.
  b. Cliquez sur **Suppression d'autorisation utilisateur**.

     Un message vous demandant de confirmer l'opération s'affiche.
  c. Cliquez sur **Oui**.
  d. Cliquez sur **Suivant**.

  L'écran Sélection du niveau de sécurité du système s'affiche.

9. Sélectionnez un niveau de sécurité système en exécutant l'une des opérations suivantes :
   - Sélectionnez les règles d'authentification souhaitées en cochant les cases appropriées. Vous pouvez sélectionner plusieurs règles d'authentification. La case **Utiliser le mot de passe composé UVM** est cochée par défaut.
   - Le pilote du lecteur d'empreinte digitale et le pilote du lecteur de carte à puce doivent être installés avant de démarrer l'assistant d'installation d'IBM Client Security pour que ce dernier puisse accéder à ces périphériques.
   - Sélectionnez le niveau de sécurité du système en faisant glisser le sélecteur sur le niveau de sécurité voulu, puis cliquez sur **Suivant**.

     Remarque : Vous pouvez ultérieurement définir une stratégie de sécurité personnalisée à l'aide de l'éditeur de stratégie dans l'utilitaire d'administration.
10. Vérifiez vos paramètres de sécurité et effectuez une des actions suivantes :
    - Pour accepter les paramètres, cliquez sur **Fin**.
    - Pour modifier les paramètres, cliquez sur **Précédent**, faites les modifications appropriées, puis revenez à cet écran et cliquez sur **Fin**.

    Le logiciel IBM Client Security configure vos paramètres à l'aide de la puce de sécurité intégrée IBM. Un message s'affiche et confirme que l'ordinateur est maintenant protégé par IBM Client Security.
11. Cliquez sur **OK**.

    Vous pouvez maintenant installer et configurer le gestionnaire de mots de passe IBM Client Security et l'utilitaire de chiffrement des fichiers et dossiers IBM Client Security.

Activation du sous-système de sécurité IBM

Le sous-système de sécurité IBM doit être activé pour que vous puissiez utiliser le logiciel Client Security. S'il n'a pas été activé, vous pouvez le faire à l'aide de l'utilitaire d'administration. Les instructions d'utilisation de l'assistant d'installation sont fournies dans la section précédente.

Pour activer le sous-système de sécurité IBM à l'aide de l'utilitaire d'administration, procédez comme suit :

1. Cliquez sur **Démarrer > Paramètres > Panneau de configuration > Sous-système de sécurité intégré IBM**.

   Un écran affiche un message qui stipule que le sous-système de sécurité IBM n'a pas été activé et qui vous demande si vous voulez l'activer.
2. Cliquez sur **Oui**.

   Un message s'affiche et indique que si vous disposez d'un mot de passe superviseur activé, vous devez le désactiver dans l'utilitaire de configuration du BIOS avant de continuer.

3. Exécutez l'une des opérations suivantes :
   - Si vous disposez d'un mot de passe superviseur activé, cliquez sur **Annulation**, désactivez votre mot de passe superviseur, puis terminez cette procédure.
   - Si vous ne disposez d'aucun mot de passe superviseur activé, cliquez sur **OK** pour continuer.
4. Fermez toutes les applications ouvertes et cliquez sur **OK** pour redémarrer l'ordinateur.
5. Après le redémarrage du système, cliquez sur **Démarrer > Paramètres > Panneau de configuration > Sous-système de sécurité intégré IBM** pour ouvrir l'utilitaire d'administration.

   Un message s'affiche et indique que le sous-système de sécurité IBM n'a pas été configuré ou a été vidé. Un nouveau mot de passe est alors requis.
6. Saisissez et confirmez le nouveau mot de passe administrateur dans les zones appropriées, puis cliquez sur **OK**.

   Remarque : Le mot de passe doit contenir huit caractères.

   L'opération est terminée et l'écran principal de l'utilitaire d'administration s'affiche.

Installation du logiciel sur d'autres clients IBM lorsque la clé publique administrateur est disponible - installations automatiques uniquement

Si vous avez installé le logiciel sur le premier client IBM et créé une paire de clés administrateur, vous pouvez installer le logiciel et activer le sous-système de sécurité sur d'autres clients IBM à l'aide du programme d'installation.

Au cours de l'installation, vous devez choisir un emplacement pour la clé publique administrateur, la clé privée administrateur et l'archive de clés. Si vous voulez utiliser une clé publique administrateur qui se trouve dans un répertoire partagé, ou sauvegarder l'archive de clés dans un répertoire partagé, vous devez affecter un identificateur d'unité au répertoire cible avant de procéder à l'installation. Pour plus d'informations sur l'affectation d'un identificateur d'unité à une ressource réseau partagée, reportez-vous à la documentation du système d'exploitation Windows.

Exécution d'une installation automatisée

Une installation automatisée permet à un administrateur d'installer le logiciel Client Security sur un client IBM éloigné sans devoir accéder physiquement à cet ordinateur client.

Avant de commencer une installation automatisée, lisez le Chapitre 3, «Opérations préalables à l'installation du logiciel», à la page 13. Aucun message d'erreur n'est affiché au cours d'une installation automatisée. Si une installation automatisée s'arrête prématurément, vous devez effectuer une installation avec opérateur pour visualiser tous les messages d'erreur susceptibles de s'afficher.

Remarque : Les utilisateurs doivent se connecter avec des droits d'administrateur pour installer le logiciel Client Security.

Déploiement de masse

Le déploiement de masse permet aux administrateurs de la sécurité de mettre en oeuvre une stratégie de sécurité sur plusieurs ordinateurs simultanément. Cela facilite la gestion et le déploiement des mesures de sécurité, et permet de garantir la mise en oeuvre des stratégies de sécurité appropriées.

Vous devez installer les pilotes de périphérique suivants avant d'exécuter la procédure de déploiement de masse :

- le pilote de bus SM,
- le pilote de périphérique Atmel TPM (pour les systèmes TCPA).

Le déploiement de masse se décompose en deux étapes principales :

- Installation de masse
- Configuration de masse

Installation de masse

Vous devez effectuer une installation automatisée pour installer le logiciel IBM Client Security sur plusieurs clients simultanément. Vous devez utiliser le paramètre d'installation automatisée lors du lancement d'un déploiement de masse.

Pour lancer une installation de masse, procédez comme suit :

1. Créez le fichier `csec.ini`.

   Le fichier `csec.ini` est créé lorsque l'utilisateur sort de l'assistant d'installation d'IBM Client Security. Cette étape n'est requise que si vous avez l'intention d'effectuer une configuration de masse. Voir «Configuration de masse» à la page 24 pour plus de détails.
2. Extrayez le contenu du module d'installation CSS à l'aide de Winzip en utilisant les noms de dossier.
3. Dans le fichier `Setup.iss` , modifiez les entrées `szIniPath` et `szDir`, qui sont requises pour une configuration de masse.

   Le contenu intégral de ce fichier est répertorié ci-après. L'emplacement du dossier est défini par le paramètre `szIniPath` du fichier `csec.ini`. Le paramètre `szIniPath` n'est requis que si vous avez l'intention d'effectuer une configuration de masse.
4. Copiez les fichiers sur le système cible.
5. Créez l'instruction de ligne de commande `\setup -s`.

   Cette instruction de ligne de commande doit être exécutée à partir du bureau d'un utilisateur disposant des droits d'administrateur. Le groupe de programmes de démarrage ou le dossier Exécuter sont des emplacements adéquats pour ce faire.
6. Supprimez l'instruction de ligne de commande à l'amorçage suivant.

Vous trouverez ci-après le contenu complet du fichier `Setup.iss` , qui est inclus dans le module d'installation CSS extrait ci-dessus, ainsi que quelques descriptions.

```
[InstallShield Silent]
Version=v6.00.000
File=Response File
szIniPath=d:\csssetup.ini
```

(Le paramètre ci-dessus représente le nom et l'emplacement du fichier .ini qui est requis pour la configuration de masse. Si ce fichier se trouve sur une unité réseau,

un identificateur doit être affecté à celle-ci. Lorsque la configuration de masse n'est pas utilisée avec une installation automatique, supprimez cette entrée.)
[File Transfer]
OverwrittenReadOnly=NoToAll
[{7BD2CFF6-B037-47D6-A76B-D941EE13AD96}-DlgOrder]
Dlg0={7BD2CFF6-B037-47D6-A76B-D941EE13AD96}-SdLicense-0
Count=4
Dlg1={7BD2CFF6-B037-47D6-A76B-D941EE13AD96}-SdAskDestPath-0
Dlg2={7BD2CFF6-B037-47D6-A76B-D941EE13AD96}-SdSelectFolder-0
Dlg3={7BD2CFF6-B037-47D6-A76B-D941EE13AD96}-SdFinishReboot-0
[{7BD2CFF6-B037-47D6-A76B-D941EE13AD96}-SdLicense-0]
Result=1
[{7BD2CFF6-B037-47D6-A76B-D941EE13AD96}-SdAskDestPath-0]
szDir=C:\Program Files\IBM\Security
(Le paramètre ci-dessus représente le répertoire utilisé pour installer Client Security. Il doit s'agir d'un répertoire local de l'ordinateur.)
Result=1
[{7BD2CFF6-B037-47D6-A76B-D941EE13AD96}-SdSelectFolder-0]
szFolder=IBM Client Security Software
(Le paramètre ci-dessus représente le groupe de programmes Client Security.)
Result=1
[Application]
Name=Client Security
Version=5.00.002f
Company=IBM
Lang=0009
[{7BD2CFF6-B037-47D6-A76B-D941EE13AD96}-SdFinishReboot-0]
Result=6
BootOption=3

Configuration de masse

Le fichier suivant est également essentiel lors du lancement d'une configuration de masse. Ce fichier peut porter n'importe quel nom, pourvu qu'il ait l'extension .ini. Ci-après figure un exemple de fichier. Sur le côté figure une brève description qui ne doit pas être incluse dans le fichier. La commande suivante permet d'exécuter ce fichier à partir de la ligne de commande lorsque la configuration de masse n'est pas effectuée conjointement à une installation de masse :

```
<dossier d'installation de CSS>\acamucli /ccf:c:\csec.ini
```

Remarque : Si des chemins ou des fichiers se trouvent sur une unité réseau, un identificateur doit être affecté à cette unité.

[CSSSetup]	En-tête de section pour la configuration de CSS.
suppw=bootup	Mot de passe administrateur/superviseur BIOS. N'indiquez aucune valeur si aucun mot de passe n'est requis.
hwpw=11111111	Mot de passe administrateur pour le sous-système de sécurité intégré IBM. Il doit comporter huit caractères et est toujours requis. Vous devez indiquer la valeur correcte si le mot de passe administrateur a déjà été défini.
newkp=1	Indiquez la valeur 1 pour générer une nouvelle paire de clés administrateur, ou la valeur 0 pour utiliser une paire de clés administrateur existante.

keysplit=1	Lorsque `newkp` a pour valeur 1, ce paramètre détermine le nombre de composants de clé privée. **Remarque :** Si la paire de clés existante utilise plusieurs éléments de clé privée, tous les éléments de clé privée doivent être stockés dans le même répertoire.
kpl=c:\jgk	Emplacement de la paire de clés administrateur lorsque le paramètre `newkp` a pour valeur 1. S'il s'agit d'une unité réseau, un identificateur doit lui être affecté.
kal=c:\jgk\archive	Emplacement de l'archive de clés utilisateur. S'il s'agit d'une unité réseau, un identificateur doit lui être affecté.
pub=c:\jk\admin.key	Emplacement de la clé publique administrateur lorsque vous utilisez une paire de clés administrateur existante. S'il s'agit d'une unité réseau, un identificateur doit lui être affecté.
pri=c:\jk\private1.key	Emplacement de la clé privée administrateur lorsque vous utilisez une paire de clés administrateur existante. S'il s'agit d'une unité réseau, un identificateur doit lui être affecté.
wiz=0	Détermine si ce fichier a été généré par l'assistant d'installation de CSS. Cette entrée n'est pas nécessaire. Si vous l'incluez dans le fichier, sa valeur doit être 0.
clean=0	Indiquez la valeur 1 pour supprimer le fichier .ini après l'initialisation, ou la valeur 0 pour conserver le fichier .ini après l'initialisation.
enableroaming=1	Indiquez la valeur 1 pour activer l'itinérance pour le client, ou la valeur 0 pour désactiver l'itinérance pour le client.
username= [promptcurrent]	[promptcurrent] pour inviter l'utilisateur en cours à entrer le mot de passe d'enregistrement sur le client itinérant. [current] lorsque le mot de passe d'enregistrement sur le client itinérant de l'utilisateur en cours est fourni par l'entrée `sysregpwd` et que cet utilisateur a été autorisé à enregistrer le système sur le serveur itinérant. [<specific user account>] si l'utilisateur désigné a été autorisé à enregistrer le système sur le serveur itinérant et si le mot de passe d'enregistrement système de cet utilisateur est fourni par l'entrée `sysregpwd`. N'utilisez pas cette entrée si `enableroaming` a pour valeur 0 ou si l'entrée `enableroaming` est absente.
sysregpwd=12345678	Mot de passe d'enregistrement système. Définissez ce paramètre par le mot de passe correct afin de permettre au système d'être enregistré sur le serveur itinérant. N'utilisez pas cette entrée si `username` a pour valeur [promptcurrent] ou si l'entrée `username` est absente.
[UVMEnrollment]	En-tête de section pour l'inscription des utilisateurs.
enrollall=0	Indiquez la valeur 1 pour enregistrer tous les comptes utilisateur locaux dans UVM, ou la valeur 0 pour enregistrer des comptes utilisateur spécifiques dans UVM.
defaultuvmpw=top	Lorsque `enrollall` a pour valeur 1, ce paramètre représente le mot de passe composé UVM de tous les utilisateurs.
defaultwinpw=down	Lorsque `enrollall` a pour valeur 1, ce paramètre représente le mot de passe Windows enregistré dans UVM pour tous les utilisateurs.

defaultppchange=0	Lorsque `enrollall` a pour valeur 1, ce paramètre représente la stratégie de modification du mot de passe composé UVM de tous les utilisateurs. Indiquez la valeur 1 pour obliger l'utilisateur à modifier le mot de passe composé UVM lors de sa prochaine connexion, ou la valeur 0 pour ne pas obliger l'utilisateur à modifier le mot de passe composé UVM lors de sa prochaine connexion.
defaultppexppolicy=1	Lorsque `enrollall` a pour valeur 1, ce paramètre représente la stratégie d'expiration du mot de passe composé UVM pour tous les utilisateurs. Indiquez la valeur 0 pour indiquer que le mot de passe composé arrive à expiration, ou la valeur 1 pour indiquer que le mot de passe composé UVM n'arrive pas à expiration.
defaultppexpdays=0	Lorsque `enrollall` a pour valeur 1, ce paramètre représente le nombre de jours au terme duquel le mot de passe composé UVM expire pour tous les utilisateurs. Lorsque le paramètre `ppexppolicy` a pour valeur 0, définissez cette valeur pour établir le nombre de jours au terme duquel le mot de passe composé UVM expire.
enrollusers=2	Lorsque `enrollall` a pour valeur 0, ce paramètre indique le nombre d'utilisateurs qui seront enregistrés dans UVM.
user1=jknox	Enumérez les utilisateurs à enregistrer en commençant par l'utilisateur 1. Les noms d'utilisateur doivent correspondre aux noms de compte. Pour obtenir le nom de compte réel sous Windows 2000, procédez comme suit : 1. Lancez la Gestion de l'ordinateur (Gestionnaire de périphériques). 2. Développez le noeud Utilisateurs et groupes locaux. 3. Ouvrez le dossier Utilisateurs. Les éléments répertoriés dans la colonne Nom sont les noms de compte. Pour obtenir le nom de compte réel sous Windows XP à partir du Panneau de configuration Windows, cliquez sur l'icône **Compte d'utilisateur**. Les comptes d'utilisateur s'affichent.
user1uvmpw=chrome	Enumérez les mots de passe composés UVM des utilisateurs à enregistrer en commençant par celui de l'utilisateur 1.
user1winpw=spinning	Enumérez les mots de passe Windows enregistrés dans UVM des utilisateurs à enregistrer en commençant par celui de l'utilisateur 1.
user1domain=0	Indiquez la valeur 0 pour indiquer que ce compte est local, ou la valeur 1 pour indiquer que ce compte se trouve sur le domaine.
user1ppchange=0	Indiquez la valeur 1 pour obliger l'utilisateur à modifier le mot de passe composé UVM lors de sa prochaine connexion, ou la valeur 0 pour ne pas obliger l'utilisateur à modifier le mot de passe composé UVM lors de sa prochaine connexion.
user1ppexppolicy=1	Indiquez la valeur 0 pour indiquer que le mot de passe composé arrive à expiration, ou la valeur 1 pour indiquer que le mot de passe composé UVM n'arrive pas à expiration.
user1ppexpdays=0	Lorsque le paramètre ppexppolicy a pour valeur 0, définissez cette valeur pour indiquer le nombre de jours au terme duquel le mot de passe composé UVM expire.

user2=russell	
user2uvmpw=left	
user2winpw=right	
user2domain=0	
user2ppchange=1	
user2ppexppolicy=0	
user2ppexpdays=90	
[UVMAppConfig]	En-tête de section pour la configuration des modules et des applications compatibles UVM.
uvmlogon=0	Indiquez la valeur 1 pour utiliser la protection à la connexion UVM, ou la valeur 0 pour utiliser la connexion Windows.
entrust=0	Indiquez la valeur 1 pour utiliser UVM pour l'authentification Entrust, ou la valeur 0 pour utiliser l'authentification Entrust.
notes=1	Indiquez la valeur 1 pour activer le support Lotus Notes, ou la valeur 0 pour désactiver le support Lotus Notes.
netscape=0	Indiquez la valeur 1 pour signer et chiffrer les courriers électroniques avec le module IBM PKCS#11, ou la valeur 0 pour ne pas signer ni chiffrer les courriers électroniques avec le module IBM PKCS#11.
passman=0	Indiquez la valeur 1 pour utiliser Password Manager, ou la valeur 0 pour ne pas utiliser Password Manager
folderprotect=0	Indiquez la valeur 1 pour utiliser la fonction de chiffrement des fichiers et dossiers (FFE), ou la valeur 0 pour ne pas utiliser la fonction FFE.

Mise à niveau de votre version du logiciel Client Security

Vous devez mettre à jour les clients sur lesquels des versions antérieures de Client Security sont installées avec cette version du logiciel afin de pouvoir tirer parti des nouvelles fonctions de Client Security.

Important : sur les systèmes TCPA dotés de la version 4.0x du logiciel IBM Client Security, vous devez désinstaller le logiciel IBM Client Security version 4.0x et vider la puce de sécurité avant d'installer cette version du logiciel IBM Client Security. Si vous ne le faites pas, l'installation risque d'échouer ou le logiciel risque de ne pas répondre.

Mise à niveau en utilisant de nouvelles données de sécurité

Si vous voulez supprimer totalement le logiciel Client Security et repartir de zéro, procédez comme suit :

1. Désinstallez la version précédente du logiciel Client Security à l'aide de l'applet Ajout/Suppression de programmes du Panneau de configuration.
2. Redémarrez le système.
3. Videz la puce de sécurité intégrée IBM dans l'utilitaire de configuration du BIOS.
4. Redémarrez le système.
5. Installez Client Security version 5.1 et configurez-le à l'aide de l'assistant d'installation du logiciel IBM Client Security.

Mise à niveau de la version 5.1 vers une version ultérieure en utilisant les données de sécurité existantes

Si vous voulez effectuer une mise à niveau de la version 5.1 du logiciel Client Security vers une version ultérieure en utilisant vos données de sécurité existantes, procédez comme suit :

1. Mettez votre archive à jour en procédant comme suit :
   a. Cliquez sur **Démarrer > Programmes > Access IBM > Logiciel IBM Client Security > Modification des paramètres de sécurité**.
   b. Cliquez sur le bouton **Mettre à jour l'archive de clés** pour vous assurer que les informations de sauvegarde soient mises à jour.

      Notez le répertoire d'archivage.
   c. Quittez l'utilitaire de configuration utilisateur du logiciel IBM Client Security.
2. Supprimez la version existante du logiciel Client Security en procédant comme suit :
   a. A partir du bureau Windows, cliquez sur **Démarrer > Exécuter**.
   b. Dans la zone Exécuter, tapez `d:\répertoire\csec5xxus_00yy.exe` , où d:\répertoire\ correspond à l'unité et au répertoire où se trouve le fichier exécutable. `xx` et `yy` sont alphanumériques.
   c. Sélectionnez **Mise à niveau**.
   d. Redémarrez le système.

Désinstallation du logiciel Client Security

Veillez à désinstaller les divers utilitaires (IBM Client Security Password Manager, Chiffrement de fichiers et de dossiers (FFE) IBM Client Security) qui améliorent les fonctionnalités de Client Security avant de désinstaller le logiciel IBM Client Security. Les utilisateurs doivent se connecter avec des droits d'administrateur pour désinstaller le logiciel Client Security.

Remarque : Vous devez désinstaller tous les utilitaires du logiciel IBM Client Security et tous les capteurs compatibles avec UVM avant de désinstaller le logiciel IBM Client Security. Le mot de passe administrateur est requis pour la désinstallation du logiciel Client Security.

Pour désinstaller le logiciel Client Security, procédez comme suit :

1. Fermez tous les programmes Windows.
2. A partir du bureau Windows, cliquez sur **Démarrer > Paramètres > Panneau de configuration**.
3. Cliquez sur l'icône **Ajout/Suppression de programmes**.
4. Dans la liste des logiciels qui peuvent être automatiquement supprimés, sélectionnez **IBM Client Security**.
5. Cliquez sur **Ajout/Suppression**.
6. Sélectionnez le bouton d'option **Supprimer**.
7. Cliquez sur **Suivant** pour désinstaller le logiciel.
8. Cliquez sur **OK** pour confirmer cette opération.
9. Saisissez le mot de passe administrateur dans l'interface fournie et cliquez sur **OK**.

10. Exécutez l'une des opérations suivantes :
    - Si vous avez installé le module PKCS#11 de la puce de sécurité intégrée IBM pour Netscape, un message s'affiche et vous demande si vous voulez lancer le processus de désactivation du module PKCS#11 de la puce de sécurité intégrée IBM. Cliquez sur **Oui** pour continuer.

      Une série de messages va s'afficher. Cliquez sur **OK** à chaque message jusqu'à ce que le module PKCS#11 de la puce de sécurité intégrée IBM soit supprimé.
    - Si vous n'avez pas installé le module PKCS#11 de la puce de sécurité intégrée IBM pour Netscape, un message s'affiche et vous demande si vous voulez supprimer les fichiers DLL partagés qui ont été installés avec le logiciel Client Security.

      Cliquez sur **Oui** pour désinstaller ces fichiers, ou sur **Non** pour les conserver. Le fait de conserver ces fichiers n'a aucune incidence sur le fonctionnement de votre ordinateur.

    Un message vous demandant si vous souhaitez supprimer ces informations système du fichier s'affiche. Si vous sélectionnez **Non**, vous pouvez restaurer ces informations lorsque vous réinstallez une version plus récente du logiciel IBM Client Security.
11. Cliquez sur **Terminé** après la suppression du logiciel.

    Vous devez redémarrer l'ordinateur après avoir désinstallé le logiciel Client Security.

Lorsque vous désinstallez le logiciel Client Security, vous supprimez tous les composants logiciels Client Security installés, ainsi que toutes les clés utilisateur, les certificats numériques, les empreintes digitales enregistrées et les mots de passe.

Chapitre 5. Identification des incidents

La section suivante présente des informations qui peuvent s'avérer utiles pour éviter des difficultés ou identifier et corriger les incidents qui peuvent survenir lors de l'utilisation du logiciel Client Security.

Fonctions d'administrateur

La présente section contient des informations qui peuvent s'avérer utiles pour un administrateur lors de la configuration et de l'utilisation du logiciel Client Security.

Le logiciel IBM Client Security ne peut être utilisé qu'avec des ordinateurs IBM dotés du sous-système de sécurité intégré IBM. Il est constitué d'applications et de composants qui permettent aux clients IBM de sécuriser leurs informations confidentielles à l'aide de matériel sécurisé et non pas via des logiciels vulnérables.

Autorisation d'utilisateurs

Pour qu'il soit possible de protéger les informations utilisateur client,le logiciel IBM Client Security **doit** être installé sur le client et les utilisateurs **doivent** être autorisés à l'utiliser. Un assistant de configuration facile à utiliser est à votre disposition afin de vous guider lors de la procédure d'installation.

Important : Au moins un utilisateur client **doit** être autorisé à utiliser UVM lors de la configuration. Si aucun utilisateur n'est autorisé à utiliser UVM lors de la configuration initiale du logiciel IBM Client Security, vos paramètres de sécurité ne seront **pas** appliqués et vos informations ne seront **pas** protégées.

Si vous avez exécuté les étapes de l'assistant de configuration sans autoriser d'utilisateur, arrêtez, puis relancez votre ordinateur, puis exécutez l'assistant de configuration de Client Security à partir du menu Démarrer de Windows et autorisez un utilisateur Windows à utiliser UVM. Ainsi, vos paramètres de sécurité seront appliqués et vos informations confidentielles seront protégées par le logiciel IBM Client Security.

Suppression d'utilisateurs

Lorsque vous supprimez un utilisateur, le nom de l'utilisateur est supprimé de la liste des utilisateurs dans l'utilitaire d'administration.

Définition d'un mot de passe administrateur BIOS (ThinkCentre)

Les paramètres de sécurité disponibles dans l'utilitaire de configuration permettent aux administrateurs d'effectuer les opérations suivantes :

- Activation ou désactivation du sous-système de sécurité intégré IBM
- Vidage du sous-système de sécurité intégré IBM

Important :

- Lorsque le sous-système de sécurité intégré IBM est vidé, toutes les clés de chiffrement et tous les certificats stockés sur le sous-système sont perdus.

Vos paramètres de sécurité étant accessibles via le programme de configuration de l'ordinateur, définissez un mot de passe administrateur pour empêcher les utilisateurs non autorisés de les modifier.

Pour définir un mot de passe administrateur BIOS, procédez comme suit :

1. Arrêtez et redémarrez l'ordinateur.
2. Lorsque l'invite du programme de configuration s'affiche, appuyez sur **F1**.
   Le menu principal du programme de configuration s'affiche.
3. Sélectionnez **System Security**.
4. Sélectionnez **Administrator Password**.
5. Tapez votre mot de passe et appuyez sur la flèche de défilement vers le bas de votre clavier.
6. Retapez votre mot de passe et appuyez sur la flèche de défilement vers le bas.
7. Sélectionnez **Change Administrator password** et appuyez sur Entrée ; appuyez de nouveau sur Entrée.
8. Appuyez sur **Echap** pour sortir et sauvegarder les paramètres.

Une fois que vous avez défini un mot de passe administrateur BIOS, une invite s'affiche chaque fois que vous tentez d'accéder au programme de configuration.

Important : Conservez votre mot de passe administrateur BIOS en lieu sûr. Si vous le perdez ou l'oubliez, vous ne pourrez pas accéder au programme de configuration, ni modifier ou supprimer le mot de passe sans retirer le capot de l'ordinateur et déplacer un cavalier sur la carte mère. Pour plus de détails, consultez la documentation matérielle fournie avec l'ordinateur.

Définition d'un mot de passe superviseur (ThinkPad)

Les paramètres de sécurité disponibles dans l'utilitaire de configuration du BIOS IBM permettent aux administrateurs d'effectuer les opérations suivantes :

- Activation ou désactivation du sous-système de sécurité intégré IBM
- Vidage du sous-système de sécurité intégré IBM

Important :

- Il est nécessaire de désactiver temporairement le mot de passe superviseur sur certains modèles de ThinkPad avant d'installer ou de mettre à niveau le logiciel Client Security.

Après avoir configuré le logiciel Client Security, définissez un mot de passe superviseur pour empêcher les utilisateurs non autorisés de modifier ces paramètres.

Pour définir un mot de passe superviseur, exécutez l'une des procédures suivantes :

Exemple 1

1. Arrêtez et redémarrez l'ordinateur.
2. Lorsque l'invite du programme de configuration s'affiche, appuyez sur F1.
   Le menu principal du programme de configuration s'affiche.
3. Sélectionnez **Password**.
4. Sélectionnez **Supervisor Password**.
5. Tapez votre mot de passe et appuyez sur Entrée.

6. Retapez votre mot de passe et appuyez sur Entrée.
7. Cliquez sur **Continue**.
8. Appuyez sur F10 pour sauvegarder et sortir.

Exemple 2

1. Arrêtez et redémarrez l'ordinateur.
2. Lorsque le message ″Pour interrompre le démarrage normal, appuyez sur le bouton bleu Access IBM″ s'affiche, appuyez sur le bouton bleu Access IBM.

   La zone Access IBM Predesktop Area s'affiche.
3. Cliquez deux fois sur **Start setup utility**.
4. Sélectionnez **Security** à l'aide des touches directionnelles (vers le bas du menu).
5. Sélectionnez **Password**.
6. Sélectionnez **Supervisor Password**.
7. Tapez votre mot de passe et appuyez sur Entrée.
8. Retapez votre mot de passe et appuyez sur Entrée.
9. Cliquez sur **Continue**.
10. Appuyez sur F10 pour sauvegarder et sortir.

Une fois que vous avez défini un mot de passe superviseur, une invite s'affiche chaque fois que vous tentez d'accéder à l'utilitaire de configuration du BIOS.

Important : Conservez votre mot de passe superviseur en lieu sûr. Si vous le perdez ou l'oubliez, vous ne pourrez pas accéder à l'utilitaire de configuration du BIOS IBM, ni modifier ou supprimer le mot de passe. Pour plus de détails, consultez la documentation matérielle fournie avec l'ordinateur.

Protection du mot de passe administrateur

Le mot de passe administrateur protège l'accès à l'utilitaire d'administration. Protégez ce mot de passe afin d'empêcher les utilisateurs non autorisés de modifier les paramètres de l'utilitaire d'administration.

Vidage du sous-système de sécurité intégré IBM (ThinkCentre)

Si vous souhaitez effacer toutes les clés de chiffrement utilisateur du sous-système de sécurité intégré IBM et mettre à blanc le mot de passe administrateur pour le sous-système, vous devez vider ce dernier. Avant de vider le sous-système de sécurité intégré IBM, lisez les informations ci-après.

Important :

- Lorsque le sous-système de sécurité intégré IBM est vidé, toutes les clés de chiffrement et tous les certificats stockés sur le sous-système sont perdus.

Pour vider le sous-système de sécurité intégré IBM, procédez comme suit :

1. Arrêtez et redémarrez l'ordinateur.
2. Lorsque l'invite du programme de configuration s'affiche, appuyez sur F1.

   Le menu principal du programme de configuration s'affiche.
3. Sélectionnez **Security**.
4. Sélectionnez **IBM TCPA Feature Setup**.
5. Sélectionnez **Clear IBM TCPA Security Feature** et appuyez sur Entrée.
6. Cliquez sur **Yes**.

7. Appuyez sur F10 et sélectionnez **Yes**.
8. Appuyez sur Entrée. L'ordinateur redémarre.

Vidage du sous-système de sécurité intégré IBM (ThinkPad)

Si vous souhaitez effacer toutes les clés de chiffrement utilisateur du sous-système de sécurité intégré IBM et mettre à blanc le mot de passe administrateur, vous devez vider le sous-système. Avant de vider le sous-système de sécurité intégré IBM, lisez les informations ci-après.

Important :

- Lorsque le sous-système de sécurité intégré IBM est vidé, toutes les clés de chiffrement et tous les certificats stockés sur le sous-système sont perdus.

Pour vider le sous-système de sécurité intégré IBM, procédez comme suit :

1. Arrêtez l'ordinateur.
2. Maintenez enfoncée la touche Fn lors du redémarrage de l'ordinateur.
3. Lorsque l'invite du programme de configuration s'affiche, appuyez sur F1.
   Le menu principal du programme de configuration s'affiche.
4. Sélectionnez **Config**.
5. Sélectionnez **IBM Security Chip**.
6. Sélectionnez **Clear IBM Security Chip**.
7. Cliquez sur **Yes**.
8. Appuyez sur Entrée pour continuer.
9. Appuyez sur F10 pour sauvegarder et sortir.

Incidents ou limitations connus concernant CSS version 5.2

Les informations ci-après pourront vous être utiles lorsque vous utiliserez les fonctions du logiciel IBM Client Security version 5.2.

Limitations relatives à l'itinérance

Utilisation d'un serveur itinérant CSS

L'invite de mot de passe administrateur CSS s'affiche à chaque tentative de connexion au serveur itinérant CSS. Vous pouvez toutefois utiliser l'ordinateur normalement sans avoir à taper ce mot de passe.

Utilisation du gestionnaire de mots de passe d'IBM Client Security dans un environnement itinérant

Les mots de passe stockés sur un système à l'aide du gestionnaire de mots de passe d'IBM Client Security peuvent être utilisés sur d'autres systèmes au sein de l'environnement itinérant. De nouvelles entrées sont automatiquement extraites de l'archive lorsque l'utilisateur se connecte à un autre système (si l'archive est disponible) au sein du réseau itinérant. Par conséquent, si un utilisateur est déjà connecté à un système, il doit se déconnecter, puis se reconnecter pour que de nouvelles entrées soient disponibles sur le réseau itinérant.

Délais de régénération d'itinérance et certificats Internet Explorer

Les certificats Internet Explorer sont régénérés dans l'archive toutes les 20 secondes. Lorsqu'un nouveau certificat Internet Explorer est généré par un utilisateur itinérant, celui-ci doit attendre au moins 20 secondes avant d'importer, de restaurer ou de modifier sa configuration CSS sur un autre système. S'il tente

d'exécuter l'une ou l'autre de ces opérations avant le délai de 20 secondes, l'intervalle de régénération entraîne la perte du certificat. En outre, si l'utilisateur n'était pas connecté à l'archive au moment de la création du certificat, il doit attendre 20 secondes après s'être connecté à l'archive afin d'être certain que le certificat est mis à jour dans l'archive.

Mot de passe Lotus Notes et itinérance d'accréditation

Si Lotus Notes est activé, le mot de passe correspondant est stocké par UVM. Les utilisateurs n'ont pas besoin d'entrer leur mot de passe Notes pour se connecter à Lotus Notes. Le système les invite à entrer leur mot de passe composé UVM, leurs empreintes digitales, leur carte à puce, etc. (selon les paramètres de stratégie de sécurité définis) afin de pouvoir accéder à Lotus Notes.

Si un utilisateur modifie son mot de passe Notes à partir de Lotus Notes, le nouveau mot de passe est mis à jour dans le fichier ID Lotus Notes et la copie UVM de ce nouveau mot de passe est également mise à jour. Dans un environnement itinérant, les accréditations UVM de l'utilisateur seront disponibles sur d'autres systèmes du réseau itinérant auquel l'utilisateur peut accéder. Il se peut que la copie UVM du mot de passe Notes ne corresponde pas au mot de passe Notes indiqué dans le fichier ID figurant sur d'autres systèmes du réseau itinérant si le fichier ID Notes contenant le mot de passe mis à jour n'est pas disponible sur les autres systèmes. Lorsque cela se produit, l'utilisateur ne peut pas accéder à Lotus Notes.

Si le fichier ID Notes de l'utilisateur contenant le mot de passe mis à jour n'est pas disponible sur les autres systèmes du réseau itinérant, il doit être copié sur ces systèmes de sorte que le mot de passe mis à jour corresponde à la copie stockée par UVM. Ou bien, les utilisateurs peuvent exécuter l'option de modification des paramètres de sécurité à partir du menu Démarrer et restaurer leur ancien mot de passe Notes. Le mot de passe Notes peut alors être de nouveau mis à jour via Lotus Notes.

Disponibilité des accréditations lors de la connexion dans un environnement itinérant

Lorsqu'une archive est stockée sur un partage de réseau, les derniers jeux d'accréditations utilisateur sont téléchargés à partir de cette archive dès que l'utilisateur y accède. Lors de la connexion, les utilisateurs n'ont pas encore accès aux partages de réseau. Par conséquent, il se peut que les dernières accréditations ne soient pas téléchargées tant que le processus de connexion n'est pas terminé. Par exemple, si le mot de passe composé UVM a été modifié sur un autre système du réseau itinérant ou que de nouvelles empreintes digitales ont été enregistrées sur un autre système, ces mises à jour ne sont pas disponibles tant que le processus de connexion n'est pas terminé. Si les accréditations utilisateur mises à jour ne sont pas disponibles, les utilisateurs peuvent tenter d'utiliser leur ancien mot de passe composé ou d'autres empreintes digitales enregistrées afin de se connecter au système. Une fois le processus de connexion terminé, les accréditations utilisateur mises à jour sont disponibles et les nouveaux mot de passe composé et empreintes digitales sont enregistrés avec UVM.

Limitations relatives aux badges de proximité

Activation d'une protection de connexion UVM sécurisée via des badges de proximité Xyloc

Pour activer une protection de connexion UVM sécurisée avec des badges de proximité CSS, vous devez installer les composants dans l'ordre indiqué ci-après.

1. Installez le logiciel IBM Client Security.

2. Activez la protection de connexion UVM sécurisée à l'aide de l'utilitaire d'administration CSS.
3. Redémarrez l'ordinateur.
4. Installez le logiciel Xyloc pour assurer la prise en charge des badges de proximité.

Remarque : Si vous installez en premier le logiciel de prise en charge des badges de proximité Xyloc, l'interface de connexion du logiciel Client Security ne s'affiche pas. Dans ce cas, vous devez désinstaller le logiciel Client Security et le logiciel Xyloc, puis les réinstaller dans l'ordre décrit précédemment afin de restaurer la protection de connexion UVM sécurisée.

Badge de proximité et fonction Cisco LEAP

Le fait d'activer simultanément la protection par badge de proximité et la fonction Cisco LEAP peut provoquer des résultats inattendus. Il est recommandé de ne pas installer ni utiliser ces composants sur le même système.

Prise en charge du logiciel Ensure

Le logiciel Client Security version 5.2 impose aux utilisateurs de badge de proximité de procéder à une mise à niveau de leur logiciel Ensure vers Ensure version 7.41. Lors d'une mise à niveau à partir d'une version antérieure du logiciel Client Security, vous devez mettre à niveau votre logiciel Ensure avant de procéder à la mise à niveau vers le logiciel Client Security version 5.2.

Restauration de clés

Lorsque vous avez exécuté une opération de restauration de clé, vous devez redémarrer l'ordinateur de manière à pouvoir continuer à utiliser le logiciel Client Security.

Noms d'utilisateurs de domaine et locaux

Si des noms d'utilisateurs de domaine et locaux sont identiques, vous devez utiliser le même mot de passe Windows pour les deux comptes. L'outil IBM User Verification Manager ne stocke qu'un seul mot de passe Windows par ID. Ainsi, les utilisateurs doivent utiliser le même mot de passe pour la connexion à un domaine et au réseau local. Si tel n'est pas le cas, ils ne sont pas invités à mettre à jour le mot de passe Windows UVM d'IBM lorsqu'ils passent d'un domaine à un réseau local et vice-versa si la fonction de remplacement de connexion Windows sécurisée UVM d'IBM est activée.

CSS ne permet pas d'enregistrer des utilisateurs de domaine et de réseau local distincts sous le même nom de compte. Si vous tentez d'enregistrer des utilisateurs de domaine et de réseau local avec le même ID, le message suivant s'affiche : The selected user ID has already been configured. CSS ne permet pas d'enregistrer de manière distincte un ID utilisateur de domaine et de réseau local commun sur un seul système de sorte que l'ID utilisateur commun peut accéder au même jeu d'accréditations tels que des certificats, des empreintes digitales stockées, etc.

Réinstallation du logiciel d'empreinte digitale Targus

Si le logiciel d'empreinte digitale Targus est enlevé et réinstallé, les entrées de registre nécessaires pour l'activation de la fonction d'empreinte digitale dans le logiciel Client Security doivent être ajoutées manuellement. Téléchargez le fichier de registre contenant les entrées nécessaires (atplugin.reg) et cliquez deux fois dessus de sorte que ces entrées soient fusionnées dans le registre. Cliquez sur Yes

lorsque le système vous invite à confirmer cette opération. Vous devez relancer le système pour que le logiciel Client Security reconnaisse ces modifications et active la fonction d'empreinte digitale.

Remarque : Vous devez disposer de privilèges administrateur sur le système de façon à pouvoir ajouter ces entrées de registre.

Mot de passe composé superviseur BIOS

La version 5.2 et les versions antérieures du logiciel IBM Client Security ne prennent pas en charge la fonction de mot de passe composé superviseur BIOS disponible sur certains systèmes ThinkPad. Si vous activez l'utilisation du mot de passe composé superviseur BIOS, toute opération d'activation ou de désactivation du sous-système de sécurité doit être effectuée à partir du programme de configuration BIOS.

Utilisation de Netscape 7.x

Netscape 7.x se comporte différemment de Netscape 4.x. L'invite de mot de passe composé ne s'affiche pas dès que Netscape est lancé. Le module PKCS 11 est chargé uniquement lorsqu'il est nécessaire de sorte que l'invite de mot de passe composé ne s'affiche que pour une opération nécessitant le module PKCS 11.

Utilisation d'une disquette pour l'archivage

Si vous spécifiez une disquette pour votre archivage lorsque vous configurez le logiciel de sécurité, vous devez prévoir des temps d'attente assez longs lors de l'écriture des données sur cette disquette. Le choix d'autres supports tels qu'un partage de réseau ou une clé USB peut s'avérer plus judicieux.

Limitations relatives aux cartes à puce

Enregistrement de cartes à puce

Les cartes à puce doivent être enregistrées avec UVM avant de pouvoir être utilisées pour authentifier un utilisateur. Si une carte est attribuée à plusieurs utilisateurs, seul le dernier d'entre eux à avoir enregistré la carte pourra l'utiliser. Par conséquent, il est recommandé d'enregistrer une carte à puce pour un seul compte utilisateur.

Authentification des cartes à puce

Si une carte à puce est requise pour l'authentification, UVM affiche une boîte de dialogue invitant à insérer la carte à puce. Lorsque vous insérez la carte à puce dans le lecteur, une boîte de dialogue s'affiche pour vous inviter à taper le code PIN de la carte. Si vous entrez un code PIN incorrect, UVM vous invite à insérer de nouveau la carte à puce. Vous devez retirer, puis réinsérer la carte à puce avant d'entrer de nouveau le code PIN. Vous devez continuer de retirer puis de réinsérer la carte à puce jusqu'à ce que le code PIN soit correct.

Affichage du caractère + devant les dossiers après le chiffrement

Une fois les fichiers ou les dossiers chiffrés, il se peut que Windows Explorer affiche un caractère + devant l'icône de dossier. Ce caractère disparaît lorsque la fenêtre de Windows Explorer est régénérée.

Limites relatives aux utilisateurs limités de Windows XP

Les utilisateurs limités de Windows XP ne peuvent pas mettre à jour leur mot de passe composé UVM ou leur mot de passe Windows ni mettre à jour leur archive de clé à l'aide de l'utilitaire de configuration utilisateur.

Autres limites

La présente section contient des informations sur d'autres questions et limites connues concernant le logiciel Client Security.

Utilisation du logiciel Client Security avec des systèmes d'exploitation Windows

Tous les systèmes d'exploitation Windows présentent la limite connue suivante : Si un utilisateur client enregistré dans UVM modifie son nom d'utilisateur Windows, toutes les fonctions du logiciel Client Security sont perdues. L'utilisateur devra ré-enregistrer le nouveau nom d'utilisateur dans UVM et demander de nouvelles autorisations d'accès.

Les systèmes d'exploitation Windows XP présentent la limite connue suivante : Les utilisateurs enregistrés dans UVM dont le nom d'utilisateur Windows a été modifié auparavant ne sont pas reconnus par UVM. UVM ne pointera pas vers le nom d'utilisateur précédent, tandis que Windows ne reconnaîtra que le nouveau nom d'utilisateur. Cette limite est valable même si le nom d'utilisateur Windows a été modifié avant l'installation du logiciel Client Security.

Utilisation du logiciel Client Security avec des applications Netscape

Netscape s'ouvre après un échec d'autorisation : Si la fenêtre de mot de passe composé UVM s'affiche, vous devez taper le mot de passe composé UVM et cliquer sur **OK** pour pouvoir continuer. Si vous tapez un mot de passe composé UVM incorrect (ou que vous fournissez une empreinte digitale incorrecte pour un scannage), un message d'erreur s'affiche. Si vous cliquez sur **OK**, Netscape se lance mais vous ne pouvez pas utiliser le certificat numérique généré par le sous-système de sécurité imbriqué IBM. Vous devez fermer, puis ouvrir à nouveau Netscape et taper le mot de passe composé UVM correct avant de pouvoir utiliser le certificat de sous-système de sécurité intégré IBM.

Les algorithmes ne s'affichent pas : Tous les algorithmes de hachage pris en charge par le module PKCS 11 du sous-système de sécurité intégré IBM ne sont pas sélectionnés si le module est affiché. Les algorithmes suivants sont pris en charge par le module PKCS 11 du sous-système de sécurité intégré IBM, mais ne sont pas identifiés comme tels lorsqu'ils sont affichés dans Netscape :

- SHA-1
- MD5

Certificat du sous-système de sécurité intégré IBM et algorithmes de chiffrement

Les informations suivantes vous aident à identifier les incidents relatifs aux algorithmes de chiffrement qui peuvent être utilisés avec le certificat du sous-système de sécurité intégré IBM. Consultez la documentation Microsoft ou Netscape pour obtenir des informations à jour sur les algorithmes de chiffrement utilisés avec leurs applications de messagerie électronique.

Lors de l'envoi de courrier électronique entre deux clients Outlook Express (128 bits) : Si vous utilisez Outlook Express avec la version 128 bits d'Internet Explorer 4.0 ou 5.0 pour envoyer du courrier électronique chiffré à d'autres clients utilisant Outlook Express (128 bits), les messages électroniques chiffrés à l'aide du certificat du sous-système de sécurité intégré IBM peuvent uniquement utiliser l'algorithme 3DES.

Lors de l'envoi de courrier électronique entre un client Outlook Express (128 bits) et un client Netscape : Une demande de chiffrement RC2(40), RC2(64) ou RC2(128) d'un client Netscape vers un client Outlook Express (128 bits) est toujours renvoyée au client Netscape avec l'algorithme RC2(40).

Certains algorithmes risquent de ne pas être disponibles pour la sélection dans le client Outlook Express (128 bits) : En fonction de la façon dont votre version d'Outlook Express (128 bits) a été configurée ou mise à jour, certains algorithmes RC2 et d'autres algorithmes risquent de ne pas pouvoir être utilisés avec le certificat du sous-système de sécurité intégré IBM. Consultez la documentation Microsoft pour obtenir des informations à jour sur les algorithmes de chiffrement utilisés avec votre version d'Outlook Express.

Utilisation de la protection UVM pour un ID utilisateur Lotus Notes

La protection UVM ne fonctionne pas si vous changez d'ID utilisateur dans une session Notes : Vous pouvez configurer la protection UVM uniquement pour l'ID utilisateur en cours d'une session Notes. Pour passer d'un ID utilisateur disposant d'une protection UVM à un autre ID utilisateur, procédez comme suit :

1. Quittez Notes.
2. Désactivez la protection UVM pour l'ID utilisateur en cours.
3. Ouvrez Notes et changez d'ID utilisateur. Consultez la documentation Lotus Notes pour plus d'informations sur le changement d'ID utilisateur.

   Pour configurer la protection UVM pour le nouvel ID utilisateur choisi, passez à l'étape 4.
4. Ouvrez l'outil de configuration Lotus Notes fourni par le logiciel Client Security et configurez la protection UVM.

Limites de l'utilitaire de configuration utilisateur

Windows XP impose des restrictions d'accès qui limitent les fonctions disponibles pour un utilisateur client dans certaines circonstances.

Windows XP Professionnel

Sous Windows XP Professionnel, les restrictions pour l'utilisateur client peuvent s'appliquer dans les situations suivantes :

- Le logiciel Client Security est installé sur une partition qui sera ensuite convertie au format NTFS.
- Le dossier Windows se trouve sur une partition qui sera ensuite convertie au format NTFS.
- Le dossier d'archive se trouve sur une partition qui sera ensuite convertie au format NTFS.

Dans les situations ci-avant, les utilisateurs limités de Windows XP Professionnel risquent de ne pas pouvoir exécuter les tâches suivantes de l'utilitaire de configuration utilisateur :

- Modifier leur mot de passe composé UVM
- Mettre à jour le mot de passe Windows enregistré à l'aide d'UVM
- Mettre à jour l'archive de clés

Windows XP Edition familiale

Les utilisateurs limités de Windows XP Edition familiale ne pourront pas utiliser l'utilitaire de configuration utilisateur dans l'une des situations suivantes :

- Le logiciel Client Security est installé sur une partition au format NTFS.
- Le dossier Windows se trouve sur une partition au format NTFS.
- Le dossier d'archive se trouve sur une partition au format NTFS.

Limites relatives à Tivoli Access Manager

La case à cocher **Refuser tout accès à l'objet sélectionné** n'est pas désactivée lorsque le contrôle Tivoli Access Manager est sélectionné. Dans l'éditeur de stratégie UVM, si vous cochez la case **Access Manager contrôle l'objet sélectionné** pour permettre à Tivoli Access Manager de contrôler un objet d'authentification, la case **Refuser tout accès à l'objet sélectionné** n'est pas désélectionnée. Bien que la case **Refuser tout accès à l'objet sélectionné** reste active, elle ne peut pas être cochée pour remplacer le contrôle Tivoli Access Manager.

Messages d'erreur

Des messages d'erreur relatifs au logiciel Client Security sont générés dans le journal des événements : Le logiciel Client Security utilise un pilote de périphérique qui risque de générer des messages d'erreur dans le journal des événements. Les erreurs associées à ces messages n'affectent pas le fonctionnement normal de l'ordinateur.

UVM appelle des messages d'erreur qui sont générés par le programme associé en cas de refus d'accès à un objet d'authentification : Si la stratégie UVM est définie de sorte que l'accès à un objet d'authentification (déchiffrement de courrier électronique, par exemple) soit refusé, le message indiquant le refus d'accès varie en fonction du logiciel utilisé. Par exemple, un message d'erreur Outlook Express signalant le refus d'accès à un objet d'authentification est différent d'un message d'erreur Netscape indiquant le refus d'accès.

Tableaux d'identification des incidents

La section suivante contient des tableaux d'identification des incidents qui peuvent s'avérer utiles en cas d'incident avec le logiciel Client Security.

Identification des incidents liés à l'installation

Les informations suivantes peuvent s'avérer utiles en cas d'incident lors de l'installation du logiciel Client Security.

Incident	Solution possible
Un message d'erreur s'affiche lors de l'installation du logiciel	**Action**
Un message vous demandant si vous souhaitez retirer l'application sélectionnée et tous ses composants s'affiche lors de l'installation du logiciel.	Cliquez sur **OK** pour sortir de la fenêtre. Relancez le processus d'installation pour installer la nouvelle version du logiciel Client Security.
Un message s'affiche pendant l'installation pour signaler qu'une mise à niveau ou un retrait du programme est nécessaire.	Exécutez l'une des opérations suivantes : • Si une version antérieure à la version 5.0 du logiciel Client Security est installée, sélectionnez **Remove**, puis videz le sous-système de sécurité à l'aide de l'utilitaire de configuration BIOS d'IBM. • Sinon, sélectionnez **Upgrade** et poursuivez l'installation.
L'accès à l'installation est refusé car le mot de passe administrateur est inconnu	**Action**
Lorsque vous installez le logiciel sur un client IBM sur lequel un sous-système de sécurité intégré IBM est activé, le mot de passe administrateur pour ce dernier est inconnu.	Videz le sous-système de sécurité afin de poursuivre l'installation.

Identification des incidents liés à l'utilitaire d'administration

Les informations suivantes peuvent s'avérer utiles en cas d'incident lors de l'utilisation de l'utilitaire d'administration.

Incident	Solution possible
Le bouton Suivant n'est pas disponible une fois que vous avez entré et confirmé votre mot de passe composé UVM dans l'utilitaire d'administration	**Action**
Lorsque vous ajoutez des utilisateurs à UVM, le bouton **Suivant** risque de ne pas être disponible, une fois que vous avez entré et confirmé votre mot de passe composé UVM dans l'utilitaire d'administration.	Cliquez sur l'option **Information** dans la Barre des tâches Windows et continuez la procédure.
Un message d'erreur s'affiche lorsque vous modifiez la clé publique administrateur	**Action**
Lorsque vous videz le sous-système de sécurité intégré et que vous restaurez ensuite l'archive de clés, un message d'erreur peut s'afficher si vous modifiez la clé publique administrateur.	Ajoutez les utilisateurs à UVM et demandez de nouveaux certificats, le cas échéant.
Un message d'erreur s'affiche lorsque vous tentez de récupérer un mot de passe composé UVM	**Action**
Lorsque vous modifiez la clé publique administrateur et que vous tentez ensuite de récupérer un mot de passe composé UVM pour un utilisateur, un message d'erreur peut s'afficher.	Exécutez l'une des opérations suivantes : • Si le mot de passe composé UVM pour l'utilisateur n'est pas nécessaire, aucune action n'est requise. • Si le mot de passe composé UVM pour l'utilisateur est requis, vous devez ajouter l'utilisateur à UVM et demander de nouveaux certificats, le cas échéant.
Un message d'erreur s'affiche lorsque vous tentez de sauvegarder le fichier de stratégie UVM	**Action**
Lorsque vous tentez de sauvegarder un fichier de stratégie UVM (globalpolicy.gvm) en cliquant sur **Validation** ou **Sauvegarde**, un message d'erreur s'affiche.	Sortez du message d'erreur, éditez à nouveau le fichier de stratégie UVM pour apporter les modifications souhaitées, puis sauvegardez le fichier.
Un message d'erreur s'affiche lorsque vous tentez d'ouvrir l'éditeur de stratégie UVM	**Action**
Lorsque l'utilisateur en cours (connecté au système d'exploitation) n'a pas été ajouté à UVM, l'éditeur de stratégie UVM ne s'ouvre pas.	Ajoutez l'utilisateur à UVM et ouvrez l'éditeur de stratégie UVM.

Incident	Solution possible
Un message d'erreur s'affiche lorsque vous utilisez l'utilitaire d'administration	**Action**
Lorsque vous utilisez l'utilitaire d'administration, le message d'erreur suivant peut s'afficher : Une erreur d'E-S en mémoire tampon s'est produite lors de la tentative d'accès au sous-système de sécurité intégré IBM. Cet incident peut être résolu par un réamorçage.	Sortez du message d'erreur et redémarrez l'ordinateur.
Un message de désactivation de la puce s'affiche lors de la modification du mot de passe administrateur	**Action**
Lorsque vous tentez de modifier le mot de passe administrateur et que vous appuyez sur Entrée ou Tabulation > Entrée après avoir tapé le mot de passe de confirmation, le bouton **Désactivation de la puce** est activé et un message confirmant la désactivation de la puce s'affiche.	Exécutez les opérations suivantes : 1. Sortez de la fenêtre de confirmation de la désactivation de la puce. 2. Pour modifier le mot de passe administrateur, tapez le nouveau mot de passe, tapez le mot de passe de confirmation, puis cliquez sur **Modification**. N'appuyez ni sur Entrée, ni sur la touche de tabulation > Entrée après avoir tapé les informations dans la fenêtre de confirmation.

Identification des incidents relatifs à l'utilitaire de configuration utilisateur

Les informations suivantes peuvent s'avérer utiles en cas d'incident lors de l'utilisation de l'utilitaire de configuration utilisateur.

Incident	Solution possible
Les utilisateurs limités ne peuvent pas exécuter certaines fonctions de l'utilitaire de configuration utilisateur sous Windows XP Professionnel	**Action**
Les utilisateurs limités de Windows XP Professionnel risquent de ne pas pouvoir exécuter les tâches suivantes de l'utilitaire de configuration utilisateur : • Modifier leur mot de passe composé UVM • Mettre à jour le mot de passe Windows enregistré à l'aide d'UVM • Mettre à jour l'archive de clés	Il s'agit d'une limite connue de Windows XP Professional. Il n'existe pas de solution à cet incident.
Les utilisateurs limités ne peuvent pas utiliser l'utilitaire de configuration utilisateur sous Windows XP Edition familiale	**Action**
Les utilisateurs limités de Windows XP Edition familiale ne pourront pas utiliser l'utilitaire de configuration utilisateur dans l'une des situations suivantes : • Le logiciel Client Security est installé sur une partition au format NTFS. • Le dossier Windows se trouve sur une partition au format NTFS. • Le dossier d'archive se trouve sur une partition au format NTFS.	Il s'agit d'une limite connue de Windows XP Edition familiale. Il n'existe pas de solution à cet incident.

Identification des incidents liés aux ThinkPad

Les informations suivantes peuvent s'avérer utiles en cas d'incident lors de l'utilisation du logiciel Client Security sur des ThinkPad.

Incident	**Solution possible**
Un message d'erreur s'affiche lorsque vous tentez d'exécuter une fonction d'administration Client Security	**Action**
Un message d'erreur s'affiche après que vous avez tenté d'exécuter une fonction d'administration Client Security.	Le mot de passe superviseur ThinkPad doit être désactivé pour exécuter certaines fonctions d'administration Client Security. Pour désactiver le mot de passe superviseur, procédez comme suit : 1. Appuyez sur F1 pour accéder à l'utilitaire de configuration du BIOS IBM. 2. Entrez le mot de passe superviseur en cours. 3. Entrez un nouveau mot de passe superviseur vierge, puis confirmez un mot de passe vierge. 4. Appuyez sur Entrée. 5. Appuyez sur F10 pour sauvegarder et sortir.
Un autre détecteur d'empreinte digitale compatible UVM ne fonctionne pas correctement	**Action**
L'ordinateur ThinkPad IBM ne prend pas en charge l'interchangeabilité de plusieurs détecteurs d'empreinte digitale compatibles UVM.	Ne changez pas de modèle de détecteur d'empreinte digitale. Utilisez le même modèle pour un travail à distance et un travail à partir d'une station d'accueil.

Identification des incidents liés aux applications Microsoft

Les tableaux d'identification des incidents suivants contiennent des informations qui peuvent s'avérer utiles en cas d'incident lors de l'utilisation du logiciel Client Security avec des applications ou des systèmes d'exploitation Microsoft.

Incident	**Solution possible**
L'écran de veille ne s'affiche que sur l'écran local	**Action**
Lors de l'utilisation de la fonction Bureau étendu de Windows, l'écran de veille du logiciel Client Security s'affiche uniquement sur l'écran local, même si l'accès à votre système et à son clavier est protégé.	Si des informations sensibles sont affichées, réduisez les fenêtres de votre Bureau étendu avant d'appeler l'écran de veille Client Security.
Client Security ne fonctionne pas correctement pour un utilisateur enregistré dans UVM	**Action**
L'utilisateur client enregistré a peut-être changé son nom d'utilisateur Windows. Dans ce cas, toutes les fonctions Client Security sont perdues.	Ré-enregistrez le nouveau nom d'utilisateur dans UVM et demandez de nouvelles autorisations d'accès.
Remarque : Sous Windows XP, les utilisateurs enregistrés dans UVM qui avaient modifié précédemment leur nom d'utilisateur Windows ne seront pas reconnus par UVM. Cette limite est valable même si le nom d'utilisateur Windows a été modifié avant l'installation du logiciel Client Security.	
Incidents lors de la lecture du courrier électronique chiffré à l'aide d'Outlook Express	**Action**
Le courrier électronique chiffré ne peut pas être déchiffré en raison des différences de chiffrement renforcé existant entre les navigateurs Web utilisés par l'expéditeur et le destinataire.	Vérifiez les points suivants : 1. Le chiffrement renforcé pour le navigateur Web utilisé par l'expéditeur est compatible avec celui utilisé par le destinataire. 2. Le chiffrement renforcé pour le navigateur Web est compatible avec celui fourni par le microcode du logiciel Client Security.
Incidents lors de l'utilisation d'un certificat à partir d'une adresse à laquelle sont associés plusieurs certificats	**Action**
Outlook Express peut répertorier plusieurs certificats associés à une seule adresse électronique et certains de ces certificats peuvent ne plus être valables. Un certificat peut ne plus être valable si la clé privée qui lui est associée n'existe plus sur le sous-système de sécurité intégré IBM de l'ordinateur de l'expéditeur sur lequel le certificat a été généré.	Demandez au destinataire de renvoyer son certificat numérique, puis sélectionnez ce certificat dans le carnet d'adresses d'Outlook Express.

Incident	Solution possible
Message d'échec lors de la tentative de signature numérique d'un message électronique	**Action**
Si l'auteur d'un message électronique tente de le signer numériquement alors qu'aucun certificat n'est encore associé à son compte de messagerie électronique, un message d'erreur s'affiche.	Utilisez les paramètres de sécurité d'Outlook Express pour indiquer un certificat à associer au compte de l'utilisateur. Pour plus de détails, consultez la documentation fournie pour Outlook Express.
Outlook Express (128 bits) chiffre uniquement les messages électroniques avec l'algorithme 3DES	**Action**
Lors de l'envoi de courrier électronique chiffré entre des clients utilisant Outlook Express avec la version 128 bits d'Internet Explorer 4.0 ou 5.0, seul l'algorithme 3DES peut être utilisé.	Consultez la documentation Microsoft pour obtenir des informations à jour sur les algorithmes de chiffrement utilisés avec Outlook Express.
Les clients Outlook Express renvoient des messages électroniques avec un algorithme différent	**Action**
Un message électronique chiffré avec l'algorithme RC2(40), RC2(64) ou RC2(128) est envoyé d'un client utilisant Netscape Messenger à un client utilisant Outlook Express (128 bits). Un message électronique renvoyé par le client Outlook Express est chiffré avec l'algorithme RC2(40).	Aucune action n'est requise. Une demande de chiffrement RC2(40), RC2(64) ou RC2(128) d'un client Netscape vers un client Outlook Express (128 bits) est toujours renvoyée au client Netscape avec l'algorithme RC2(40). Consultez la documentation Microsoft pour obtenir des informations à jour sur les algorithmes de chiffrement utilisés avec votre version d'Outlook Express.
Message d'erreur lors de l'utilisation d'un certificat dans Outlook Express après une défaillance de l'unité de disque dur	**Action**
Les certificats peuvent être restaurés à l'aide de la fonction de restauration des clés de l'utilitaire d'administration. Certains certificats, tels que les certificats gratuits fournis par VeriSign, risquent de ne pas être restaurés après une restauration des clés.	Après la restauration des clés, exécutez l'une des opérations suivantes : • Obtenez de nouveaux certificats. • Enregistrez à nouveau l'autorité de certification dans Outlook Express.
Outlook Express ne met pas à jour le chiffrement renforcé associé à un certificat	**Action**
Lorsqu'un expéditeur sélectionne le chiffrement renforcé dans Netscape et envoie un message électronique signé à un client en utilisant Outlook Express avec Internet Explorer 4.0 (128 bits), le chiffrement renforcé du courrier électronique renvoyé risque de ne pas correspondre.	Supprimez le certificat associé dans le carnet d'adresses d'Outlook Express. Ouvrez à nouveau le courrier électronique signé et ajoutez le certificat au carnet d'adresses d'Outlook Express.
Un message d'erreur de déchiffrement s'affiche dans Outlook Express	**Action**
Vous pouvez ouvrir un message dans Outlook Express en cliquant deux fois dessus. Dans certains cas, lorsque vous effectuez cette opération trop rapidement, un message d'erreur de déchiffrement s'affiche.	Fermez le message et ouvrez à nouveau le message électronique chiffré.

Incident	Solution possible
Un message d'erreur de déchiffrement peut également s'afficher dans le volet de prévisualisation lorsque vous sélectionnez un message chiffré.	Si un message d'erreur s'affiche dans le volet de prévisualisation, aucune action n'est requise.
Un message d'erreur s'affiche lorsque vous cliquez deux fois sur le bouton Envoyer dans des courriers électroniques chiffrés	**Action**
Lorsque vous utilisez Outlook Express, si vous cliquez deux fois sur le bouton d'envoi pour envoyer un message électronique chiffré, un message d'erreur s'affiche pour indiquer que le message n'a pas pu être envoyé.	Fermez le message d'erreur et cliquez sur le bouton **Envoyer**.
Un message d'erreur s'affiche lorsque vous demandez un certificat	**Action**
Lorsque vous utilisez Internet Explorer, vous risquez de recevoir un message d'erreur si vous demandez un certificat qui utilise le fournisseur de service cryptographique du sous-système de sécurité intégré IBM.	Redemandez le certificat numérique.

Identification des incidents relatifs aux applications Netscape

Les tableaux d'identification des incidents suivants contiennent des informations qui peuvent s'avérer utiles en cas d'incident lors de l'utilisation du logiciel Client Security avec des applications Netscape.

Incident	Solution possible
Incidents lors de la lecture du courrier électronique chiffré	**Action**
Le courrier électronique chiffré ne peut pas être déchiffré en raison des différences de chiffrement renforcé existant entre les navigateurs Web utilisés par l'expéditeur et le destinataire.	Vérifiez les points suivants : 1. Le chiffrement renforcé pour le navigateur Web utilisé par l'expéditeur est compatible avec celui utilisé par le destinataire. 2. Le chiffrement renforcé pour le navigateur Web est compatible avec celui fourni par le microcode du logiciel Client Security.
Message d'échec lors de la tentative de signature numérique d'un message électronique	**Action**
Lorsque le certificat de sous-système de sécurité intégré IBM n'a pas été sélectionné dans Netscape Messenger et que l'auteur d'un message électronique tente de signer celui-ci avec le certificat, un message d'erreur s'affiche.	Utilisez les paramètres de sécurité de Netscape Messenger pour sélectionner le certificat. Lorsque Netscape Messenger est ouvert, cliquez sur l'icône de sécurité de la barre d'outils. La fenêtre relative aux informations de sécurité s'ouvre. Cliquez sur **Messenger** dans le panneau de gauche, puis sélectionnez le **certificat de la puce de sécurité intégrée IBM**. Pour plus de détails, consultez la documentation fournie par Netscape.

Incident	Solution possible
Un message électronique est renvoyé au client avec un algorithme différent	**Action**
Un message électronique chiffré avec l'algorithme RC2(40), RC2(64) ou RC2(128) est envoyé d'un client utilisant Netscape Messenger à un client utilisant Outlook Express (128 bits). Un message électronique renvoyé par le client Outlook Express est chiffré avec l'algorithme RC2(40).	Aucune action n'est requise. Une demande de chiffrement RC2(40), RC2(64) ou RC2(128) d'un client Netscape vers un client Outlook Express (128 bits) est toujours renvoyée au client Netscape avec l'algorithme RC2(40). Consultez la documentation Microsoft pour obtenir des informations à jour sur les algorithmes de chiffrement utilisés avec votre version d'Outlook Express.
Impossible d'utiliser un certificat numérique généré par le sous-système de sécurité intégré IBM	**Action**
Le certificat numérique généré par le sous-système de sécurité intégré IBM n'est pas disponible pour l'utilisation.	Vérifiez que le mot de passe composé UVM a été tapé correctement lors de l'ouverture de Netscape. Si le mot de passe composé UVM est incorrect, un message d'erreur signalant un échec d'authentification s'affiche. Si vous cliquez sur **OK**, Netscape se lance mais vous ne pouvez pas utiliser le certificat généré par le sous-système de sécurité intégré IBM. Vous devez sortir de Netscape, puis l'ouvrir à nouveau et taper le mot de passe composé UVM correct.
De nouveaux certificats numériques provenant du même expéditeur ne sont pas remplacés dans Netscape	**Action**
Lorsqu'un courrier électronique signé numériquement est reçu plusieurs fois par le même expéditeur, le premier certificat numérique associé au courrier électronique n'est pas remplacé.	Si vous recevez plusieurs certificats de courrier électronique, un seul fait office de certificat par défaut. Utilisez les fonctions de sécurité de Netscape pour supprimer le premier certificat, puis ouvrez à nouveau le deuxième certificat ou demandez à l'expéditeur d'envoyer un autre courrier électronique signé.
Impossible d'exporter le certificat du sous-système de sécurité intégré IBM	**Action**
Le certificat du sous-système de sécurité intégré IBM ne peut pas être exporté dans Netscape. La fonction d'exportation de Netscape peut être utilisée pour effectuer des copies de sauvegarde des certificats.	Accédez à l'utilitaire d'administration ou à l'utilitaire de configuration utilisateur pour mettre à jour l'archive de clés. Lorsque vous mettez à jour l'archive de clés, des copies de tous les certificats associés au sous-système de sécurité intégré IBM sont créées.
Message d'erreur lors de la tentative d'utilisation d'un certificat restauré après une défaillance de l'unité de disque dur	**Action**
Les certificats peuvent être restaurés à l'aide de la fonction de restauration des clés de l'utilitaire d'administration. Certains certificats, tels que les certificats gratuits fournis par VeriSign, risquent de ne pas être restaurés après une restauration des clés.	Après la restauration des clés, obtenez un nouveau certificat.

Incident	Solution possible
L'agent Netscape s'ouvre et provoque l'échec de Netscape	**Action**
L'agent Netscape s'ouvre et provoque la fermeture de Netscape.	Mettez l'agent Netscape hors tension.
Un délai s'écoule lors de la tentative d'ouverture de Netscape	**Action**
Si vous ajoutez le module PKCS 11 du sous-système de sécurité intégré IBM, puis que vous ouvrez Netscape, un petit délai s'écoule avant l'ouverture de Netscape.	Aucune action n'est requise. Ces informations sont fournies uniquement à titre d'information.

Identification des incidents relatifs à un certificat numérique

Les informations suivantes peuvent s'avérer utiles en cas d'incident lors de l'obtention d'un certificat numérique.

Incident	Solution possible
La fenêtre de mot de passe composé UVM ou la fenêtre d'authentification d'empreinte digitale s'affiche plusieurs fois lors de la demande d'un certificat numérique	**Action**
La stratégie de sécurité UVM impose qu'un utilisateur fournisse le mot de passe composé UVM ou l'authentification d'empreinte digitale avant de pouvoir acquérir un certificat numérique. Si l'utilisateur tente d'acquérir un certificat, la fenêtre d'authentification demandant le mot de passe composé UVM ou le scannage d'empreinte digitale peut s'afficher plusieurs fois.	Tapez votre mot de passe composé UVM ou scannez votre empreinte digitale chaque fois que la fenêtre d'authentification s'ouvre.
Un message d'erreur VBScript ou JavaScript s'affiche	**Action**
Lorsque vous demandez un certificat numérique, un message d'erreur relatif à VBScript ou JavaScript peut s'afficher.	Redémarrez l'ordinateur et redemandez le certificat.

Identification des incidents relatifs à Tivoli Access Manager

Les informations suivantes peuvent s'avérer utiles en cas d'incident lors de l'utilisation de Tivoli Access Manager avec le logiciel Client Security.

Incident	Solution possible
Les paramètres de stratégie locaux ne correspondent pas à ceux du serveur	**Action**
Tivoli Access Manager autorise certaines configurations de bit qui ne sont pas prises en charge par UVM. Les exigences de stratégie locales peuvent donc remplacer les paramètres définis par un administrateur lors de la configuration du serveur Tivoli Access Manager.	Il s'agit d'une limite connue.
Les paramètres de configuration de Tivoli Access Manager ne sont pas accessibles	**Action**
Les paramètres de configuration de Tivoli Access Manager et de la mémoire cache locale ne sont pas accessibles sur la page Définition de stratégie de l'utilitaire d'administration.	Installez l'environnement d'exécution de Tivoli Access Manager. Si l'environnement d'exécution n'est pas installé sur le client IBM, les paramètres de Tivoli Access Manager sur la page Définition de stratégie ne seront pas disponibles.
Une commande utilisateur est valide à la fois pour l'utilisateur et le groupe	**Action**
Lors de la configuration du serveur Tivoli Access Manager, si vous définissez un utilisateur par rapport à un groupe, la commande utilisateur est valide à la fois pour l'utilisateur et le groupe si l'option **Traverse bit** est activée.	Aucune action n'est requise.

Identification des incidents relatifs à Lotus Notes

Les informations suivantes peuvent s'avérer utiles en cas d'incident lors de l'utilisation de Lotus Notes avec le logiciel Client Security.

Incident	Solution possible
Une fois que la fonction de protection UVM pour Lotus Notes a été activée, Notes ne peut pas finir sa configuration	**Action**
Lotus Notes ne peut pas finir sa configuration une fois que la fonction de protection UVM a été activée à l'aide de l'utilitaire d'administration.	Il s'agit d'une limite connue. Lotus Notes doit être configuré et en cours d'exécution avant que le support Lotus Notes ne soit activé dans l'utilitaire d'administration.
Un message d'erreur s'affiche lorsque vous tentez de modifier le mot de passe Notes	**Action**
La modification du mot de passe Notes lors de l'utilisation du logiciel Client Security risque de provoquer l'affichage d'un message d'erreur.	Essayez de modifier à nouveau le mot de passe. Si l'opération n'aboutit pas, redémarrez le client.
Un message d'erreur s'affiche une fois que vous avez généré un mot de passe de façon aléatoire	**Action**
Un message d'erreur risque de s'afficher lorsque vous exécutez les opérations suivantes : • Utilisation de l'outil de configuration de Lotus Notes pour définir la protection UVM pour un ID Notes • Ouverture de Notes et utilisation de la fonction fournie par Notes pour modifier le mot de passe pour un fichier d'ID Notes • Fermeture immédiate de Notes après la modification du mot de passe	Cliquez sur **OK** pour faire disparaître le message d'erreur. Aucune autre action n'est requise. Contrairement aux indications du message d'erreur, le mot de passe a été modifié. Le nouveau mot de passe est généré de façon aléatoire par le logiciel Client Security. Le fichier d'ID Notes est désormais chiffré à l'aide du mot de passe généré de façon aléatoire et l'utilisateur n'a pas besoin d'un nouveau fichier d'ID utilisateur. Si l'utilisateur final modifie à nouveau le mot de passe, UVM génère un nouveau mot de passe de façon aléatoire pour l'ID Notes.

Identification des incidents relatifs au chiffrement

Les informations suivantes peuvent s'avérer utiles en cas d'incident lors du chiffrement de fichiers à l'aide du logiciel Client Security version 3.0 ou suivante.

Incident	Solution possible
Les fichiers précédemment chiffrés ne sont pas déchiffrés	**Action**
Les fichiers chiffrés à l'aide de versions précédentes du logiciel Client Security ne peuvent pas être déchiffrés après la mise à niveau vers Client Security version 3.0 ou suivante.	Il s'agit d'une limite connue. Vous devez déchiffrer tous les fichiers qui ont été chiffrés à l'aide de versions précédentes du logiciel Client Security *avant* d'installer Client Security version 3.0 ou suivante. Le logiciel Client Security 3.0 ne peut pas déchiffrer des fichiers qui ont été chiffrés à l'aide de versions précédentes du logiciel Client Security en raison de modifications effectuées dans l'implémentation du chiffrement de fichiers.

Identification des incidents relatifs aux périphériques compatibles UVM

Les informations suivantes peuvent s'avérer utiles en cas d'incident lors de l'utilisation de périphériques compatibles UVM.

Incident	Solution possible
Un périphérique compatible UVM cesse de fonctionner correctement	**Action**
Un dispositif de sécurité compatible UVM, tel qu'une carte à puce, un lecteur de carte à puce ou un scanneur d'empreinte digitale, ne fonctionne pas correctement.	Vérifiez que le dispositif est correctement configuré par le système. Une fois le dispositif configuré, il peut s'avérer nécessaire de redémarrer le système pour démarrer correctement le service. Pour plus d'informations sur la résolution des incidents liés à un dispositif, reportez-vous à la documentation fournie avec ce dernier ou prenez contact avec le fournisseur.
Un périphérique compatible UVM cesse de fonctionner correctement	**Action**
Lorsque vous déconnectez un périphérique compatible UVM d'un port USB, puis que vous le reconnectez au port USB, le périphérique risque de ne pas fonctionner correctement.	Redémarrez l'ordinateur une fois que le périphérique a été reconnecté au port USB.

Annexe A. Réglementation américaine relative à l'exportation du logiciel Client Security

Le progiciel IBM Client Security a été examiné par le bureau IBM Export Regulation Office (ERO) et, comme l'exigent les réglementations du gouvernement américain relatives à l'exportation, IBM a soumis la documentation appropriée et reçu l'approbation dans la catégorie "vente au détail" de l'U.S. Department of Commerce pour la distribution internationale du support de chiffrement 256 bits, excepté dans les pays sous embargo américain. La réglementation peut faire l'objet de modifications par le gouvernement américain ou par un autre gouvernement national.

Si vous ne parvenez pas à télécharger le logiciel Client Security, veuillez prendre contact avec votre revendeur IBM local pour vérifier auprès du coordinateur de la réglementation sur les exportations IBM de votre pays que vous pouvez le télécharger.

Annexe B. Informations relatives aux mots de passe et mots de passe composés

Cette annexe contient des informations relatives aux mots de passe et mots de passe composés.

Règles relatives aux mots de passe et aux mots de passe composés

Un système sécurisé comporte de nombreux mots de passe et mots de passe composés différents. Or, ces différents mots de passe répondent à des règles différentes. Cette section contient des informations sur le mot de passe administrateur et le mot de passe composé UVM.

Règles applicables au mot de passe administrateur

Les règles qui régissent le mot de passe administrateur ne peuvent pas être modifiées par l'administrateur de la sécurité.

Les règles ci-après s'appliquent au mot de passe administrateur.

Longueur
Le mot de passe doit contenir exactement huit caractères.

Caractères
Le mot de passe ne doit contenir que des caractères alphanumériques. Toute combinaison de lettres et de chiffres est admise. En revanche, les caractères spéciaux, tels que l'espace, le point d'exclamation (!), le point d'interrogation (?) ou le signe pourcentage (%), ne sont pas admis.

Propriétés
Définissez le mot de passe administrateur pour activer la puce de sécurité intégrée IBM sur l'ordinateur. Ce mot de passe doit être entré lors de chaque accès à l'utilitaire d'administration et à la console d'administration.

Tentatives infructueuses
Si vous indiquez un mot de passe incorrect dix fois, l'ordinateur se verrouille pendant 1 heure 17 minutes. Si, une fois ce délai écoulé, vous tapez encore dix fois un mot de passe incorrect, l'ordinateur se verrouille pendant 2 heures 34 minutes. Le temps de verrouillage de l'ordinateur double à chaque fois qu'un mot de passe incorrect est tapé dix fois de suite.

Règles relatives aux mots de passe composés UVM

Le logiciel IBM Client Security permet aux administrateurs de la sécurité de définir les règles qui régissent le mot de passe composé UVM d'un utilisateur. Pour améliorer la sécurité, le mot de passe composé UVM est plus long qu'un mot de passe traditionnel. La stratégie de mot de passe composé UVM est contrôlée par l'utilitaire d'administration.

L'interface de stratégie de mot de passe composé UVM de l'utilitaire d'administration permet aux administrateurs de sécurité de contrôler les critères de mot de passe composé via une interface simple. Cette interface donne à l'administrateur la possibilité d'établir les règles relatives aux mots de passe composés suivantes :

Remarque : Le paramètre par défaut pour chaque critère de mot de passe composé est indiqué ci-dessous entre parenthèses.

- Définir ou non un nombre minimal de caractères alphanumériques autorisé (oui, 6)

  Par exemple, lorsque ″6″ caractères sont autorisés, `1234567xxx` est un mot de passe incorrect.
- Définir ou non un nombre minimal de chiffres autorisé (oui, 1)

  Par exemple, lorsque ce nombre est défini à ″1″, `voicimonmotdepasse` est un mot de passe incorrect.
- Définir ou non le nombre minimal d'espaces autorisé (pas de minimum)

  Par exemple, lorsque ce nombre est défini à ″2″, `je suis absent` est un mot de passe incorrect.
- Autoriser ou non le mot de passe composé à commencer par un chiffre (non)

  Par exemple, par défaut, `1motdepasse` est un mot de passe incorrect.
- Autoriser ou non le mot de passe composé à se terminer par un chiffre (non)

  Par exemple, par défaut, `motdepasse8` est un mot de passe incorrect.
- Autoriser ou non le mot de passe composé à contenir un ID utilisateur (non)

  Par exemple, par défaut, `NomUtilisateur` est un mot de passe incorrect, où `NomUtilisateur` est un ID utilisateur.
- Vérifier ou non que le nouveau mot de passe composé est différent des x derniers mots de passe composés, où x correspond à une zone modifiable (oui, 3)

  Par exemple, par défaut, `monmotdepasse` est un mot de passe incorrect si l'un de vos trois derniers mots de passe était `monmotdepasse`.
- Autoriser ou non le mot de passe composé à contenir plus de trois caractères consécutifs, quel que soit leur emplacement, identiques au mot de passe précédent (non)

  Par exemple, par défaut, `motdep` est un mot de passe incorrect si votre mot de passe précédent était `motde` ou `mdepasse`.

L'interface Stratégie de mot de passe composé UVM de l'utilitaire d'administration permet aux administrateurs de sécurité de contrôler la péremption des mots de passe composés. Cette interface donne à l'administrateur la possibilité de choisir les règles de péremption de mots de passe composés suivantes :

- Indiquer si le mot de passe composé expire au bout d'un nombre de jours défini (oui, 184)

  Par exemple, par défaut, le mot de passe composé expire au bout de 184 jours. Le nouveau mot de passe composé doit respecter la stratégie de mot de passe composé établie.
- Indiquer si le mot de passe composé doit expirer (oui).

  Lorsque cette option est sélectionnée, le mot de passe composé n'expire jamais.

La stratégie de mot de passe composé est vérifiée dans l'utilitaire d'administration lors de l'inscription de l'utilisateur et également lorsque ce dernier modifie le mot de passe composé à partir de l'utilitaire client. Les deux paramètres utilisateur relatifs au mot de passe précédent sont redéfinis et l'historique du mot de passe composé est supprimé.

Les règles générales suivantes s'appliquent au mot de passe composé UVM :

Longueur
Le mot de passe composé peut contenir jusqu'à 256 caractères.

Caractères
Le mot de passe composé peut contenir toute combinaison des caractères que le clavier permet de taper, y compris les espaces et les caractères non alphanumériques.

Propriétés
Le mot de passe composé UVM est différent du mot de passe que vous pouvez utiliser pour ouvrir une session sur un système d'exploitation. Il peut être utilisé avec d'autres dispositifs d'authentification, tels que les capteurs à empreintes digitales UVM.

Tentatives infructueuses
Si vous tapez plusieurs fois un mot de passe composé UVM incorrect durant une session, l'ordinateur met à exécution une série de périodes de suspension anti-martèlement (qui vous empêchent de tenter de vous connecter de façon incessante). Ces périodes sont indiquées dans la section suivante.

Nombre d'échecs sur les systèmes TCPA et non-TCPA

Le tableau suivant indique la durée des périodes anti-martèlement définies pour un système TCPA :

Tentatives	Période de suspension lors du prochain échec
15	1,1 minute
31	2,2 minutes
47	4,4 minutes
63	8,8 minutes
79	17,6 minutes
95	35,2 minutes
111	1,2 heure
127	2,3 heures
143	4,7 heures

Les systèmes TCPA ne font pas de distinction entre les mots de passe composés utilisateur et le mot de passe administrateur. Toute authentification par le biais de la puce de sécurité intégrée IBM répond à la même stratégie. La période de suspension maximale est de 4,7 heures. Les systèmes TCPA ne peuvent appliquer de suspension supérieure à 4,7 heures.

Les systèmes non-TCPA font une distinction entre le mot de passe administrateur et les mots de passe composés utilisateur. Sur les systèmes non-TCPA, le mot de passe administrateur est suspendu pendant 77 minutes au bout de 10 tentatives infructueuses. Par contre, les mots de passe utilisateur ne sont suspendus que pendant une minute au bout de 32 tentatives infructueuses et ce temps de verrouillage est doublé au bout de chaque 32ème tentative infructueuse.

Réinitialisation d'un mot de passe composé

Si un utilisateur oublie son mot de passe composé, l'administrateur peut l'autoriser à réinitialiser son mot de passe.

Réinitialisation à distance d'un mot de passe composé

Pour réinitialiser un mot de passe à distance, procédez comme suit :

- **Administrateurs**

  Un administrateur distant doit exécuter la procédure suivante :

  1. Créer un nouveau mot de passe unique et le communiquer à l'utilisateur.
  2. Envoyer un fichier de données à l'utilisateur.

     Le fichier de données peut être envoyé à l'utilisateur par courrier électronique, copié sur un support amovible tel qu'une disquette ou copié directement dans le fichier d'archive de l'utilisateur (en supposant que l'utilisateur puisse accéder à ce système). Ce fichier chiffré permet d'effectuer une vérification par comparaison avec le nouveau mot de passe unique.

- **Utilisateurs**

  L'utilisateur doit exécuter la procédure suivante :

  1. Ouvrir une session sur l'ordinateur.
  2. Lorsqu'il est invité à entrer son mot de passe composé, cocher la case ″J'ai oublié mon mot de passe composé″.
  3. Entrer le mot de passe unique communiqué par l'administrateur distant et fournir l'emplacement du fichier envoyé par l'administrateur.

     Une fois qu'UVM a vérifié que les informations contenues dans le fichier correspondaient au mot de passe fourni, l'utilisateur se voit accorder l'accès. Il est alors immédiatement invité à modifier son mot de passe composé.

Voici la méthode recommandée pour réinitialiser un mot de passe composé en cas d'oubli.

Réinitialisation manuelle d'un mot de passe composé

Si l'administrateur peut utiliser directement le système de l'utilisateur ayant oublié son mot de passe, il peut ouvrir une session sur ce système en tant qu'administrateur, fournir la clé privée administrateur à l'utilitaire d'administration et modifier manuellement le mot de passe composé de l'utilisateur. Il n'est pas nécessaire que l'administrateur connaisse l'ancien mot de passe composé de l'utilisateur pour effectuer une modification de ce mot de passe.

Annexe C. Remarques

La présente annexe comporte les informations juridiques relatives aux produits IBM, ainsi qu'aux marques.

Remarques

Le présent document peut contenir des informations ou des références concernant certains produits, logiciels ou services IBM non annoncés dans ce pays. Pour plus de détails, référez-vous aux documents d'annonce disponibles dans votre pays, ou adressez-vous à votre partenaire commercial IBM. Toute référence à un produit, logiciel ou service IBM n'implique pas que seul ce produit, logiciel ou service puisse être utilisé. Tout autre élément fonctionnellement équivalent peut être utilisé, s'il n'enfreint aucun droit d'IBM. Il est de la responsabilité de l'utilisateur d'évaluer et de vérifier lui-même les installations et applications réalisées avec des produits, logiciels ou services non expressément référencés par IBM.

IBM peut détenir des brevets ou des demandes de brevet couvrant les produits mentionnés dans le présent document. La remise de ce document ne vous donne aucun droit de licence sur ces brevets ou demandes de brevet. Si vous désirez recevoir des informations concernant l'acquisition de licences, veuillez en faire la demande par écrit à l'adresse suivante :

IBM EMEA Director of Licensing
IBM Europe Middle-East Africa
Tour Descartes
92066 Paris-La Défense Cedex 50
France

Pour le Canada, veuillez adresser votre courrier à :

IBM Director of Commercial Relations
IBM Canada Ltd
3600 Steeles Avenue East
Markham, Ontario
L3R 9Z7
Canada

Le paragraphe suivant ne s'applique ni au Royaume-Uni, ni dans aucun pays dans lequel il serait contraire aux lois locales. LE PRESENT DOCUMENT EST LIVRE ″EN L'ETAT″. IBM DECLINE TOUTE RESPONSABILITE, EXPLICITE OU IMPLICITE, RELATIVE AUX INFORMATIONS QUI Y SONT CONTENUES, Y COMPRIS EN CE QUI CONCERNE LES GARANTIES DE VALEUR MARCHANDE OU D'ADAPTATION A VOS BESOINS. Certaines juridictions n'autorisent pas l'exclusion des garanties implicites, auquel cas l'exclusion ci-dessus ne vous sera pas applicable.

Le présent document peut contenir des inexactitudes ou des coquilles. Il est mis à jour périodiquement. Chaque nouvelle édition inclut les mises à jour. IBM peut modifier sans préavis les produits et logiciels décrits dans ce document.

Les licenciés souhaitant obtenir des informations permettant : (i) l'échange des données entre des logiciels créés de façon indépendante et d'autres logiciels (dont celui-ci), et (ii) l'utilisation mutuelle des données ainsi échangées, doivent adresser leur demande à : IBM Corporation, Department 80D, P.O. Box 12195, 3039 Cornwallis, Research Triangle Park, NC 27709, U.S.A. Ces informations peuvent être soumises à des conditions particulières, prévoyant notamment le paiement d'une redevance.

Le logiciel sous licence décrit dans ce document et tous les éléments sous licence disponibles s'y rapportant sont fournis par IBM conformément aux dispositions de l'ICA, des Conditions internationales d'utilisation des logiciels IBM ou de tout autre accord équivalent.

Marques

IBM et SecureWay sont des marques d'IBM Corporation aux Etats-Unis et/ou dans certains autres pays.

Tivoli est une marque de Tivoli Systems Inc. aux Etats-Unis et/ou dans certains autres pays.

Microsoft, Windows et Windows NT sont des marques de Microsoft Corporation aux Etats-Unis et/ou dans certains autres pays.

D'autres sociétés sont propriétaires des autres marques, noms de produits ou logos qui pourraient apparaître dans ce document.