Solutions IBM Client Security

Logiciel Client Security version 5.4
Guide d'installation

Solutions IBM Client Security

Logiciel Client Security version 5.4
Guide d'installation

Important

Avant d'utiliser le présent document et le produit associé, prenez connaissance des informations générales figurant dans l'Annexe A, «Réglementation américaine relative à l'exportation du logiciel Client Security», à la page 35 et dans l'Annexe C, «**Remarques**», à la page 43.

Première édition - octobre 2004

Ce document est mis à jour périodiquement. Chaque nouvelle édition inclut les mises à jour. Les informations qui y sont fournies sont susceptibles d'être modifiées avant que les produits décrits ne deviennent eux-mêmes disponibles. En outre, il peut contenir des informations ou des références concernant certains produits, logiciels ou services non annoncés dans ce pays. Cela ne signifie cependant pas qu'ils y seront annoncés.

Pour plus de détails, pour toute demande d'ordre technique, ou pour obtenir des exemplaires de documents IBM, référez-vous aux documents d'annonce disponibles dans votre pays, ou adressez-vous à votre partenaire commercial.

Vous pouvez également consulter les serveurs Internet suivants :

- http://www.fr.ibm.com (serveur IBM en France)
- http://www.can.ibm.com (serveur IBM au Canada)
- http://www.ibm.com (serveur IBM aux Etats-Unis)

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

Table des matières

Avis aux lecteurs canadiens v

Avant-propos vii
A propos de ce manuel vii
A qui est destiné ce manuel vii
Comment utiliser ce manuel viii
Références au manuel *Logiciel Client Security - Guide d'administration et d'utilisation* viii
Informations complémentaires viii

Chapitre 1. Introduction 1
Le sous-système de sécurité intégré IBM 1
La puce de sécurité intégrée IBM 1
Logiciel IBM Client Security 2
Les relations entre les mots de passe et les clés . . . 2
Le mot de passe administrateur 3
Les clés publique et privée matérielles 3
Les clés publique et privée administrateur . . . 4
Archive ESS 4
Clés publique et privée utilisateur 4
Hiérarchie de substitution de clés IBM 4
Fonctions PKI (Public Key Infrastructure) CSS . . . 6

Chapitre 2. Mise en route 9
Matériel requis 9
Sous-système de sécurité intégré IBM 9
Modèles d'ordinateurs IBM pris en charge . . . 9
Logiciels requis 9
Systèmes d'exploitation 9
Produits compatibles avec UVM 9
Navigateurs Web 10

Chapitre 3. Opérations préalables à l'installation du logiciel 13
Avant d'installer le logiciel 13
Installation en vue d'une utilisation avec Tivoli Access Manager 13
Remarques sur les fonctions de démarrage . . . 13
Informations sur la mise à jour du BIOS 14
Utilisation de la paire de clés administrateur pour l'archivage de clés 15

Chapitre 4. Téléchargement, installation et configuration du logiciel 17
Téléchargement du logiciel 17
Installation du logiciel 18
Sélection d'une option de configuration 18
Configuration classique 18
Configuration évoluée 20
Utilisation de l'assistant d'installation d'IBM Client Security 21
Utilisation de l'assistant d'installation pour l'exécution d'une configuration classique . . . 21
Utilisation de l'assistant d'installation pour l'exécution d'une configuration évoluée 22
Activation du sous-système de sécurité IBM . . . 25
Mise à niveau de votre version du logiciel Client Security 26
Mise à niveau en utilisant de nouvelles données de sécurité. 26
Mise à niveau de CSS version 5.0 ou suivante à l'aide des données de sécurité existantes. . . . 26
Désinstallation du logiciel Client Security 27
Réglementations régissant l'exportation 28

Chapitre 5. Identification des incidents 29
Fonctions d'administrateur 29
Autorisation d'utilisateurs 29
Définition d'un mot de passe administrateur BIOS (ThinkCentre). 29
Définition d'un mot de passe superviseur (ThinkPad) 30
Vidage du sous-système de sécurité intégré IBM (ThinkCentre). 31
Vidage du sous-système de sécurité intégré IBM (ThinkPad) 31
Incidents ou limitations connus concernant CSS version 5.4. 32
Réinstallation du logiciel d'empreinte digitale Targus 32
Mot de passe composé superviseur BIOS . . . 32
Limitations relatives aux cartes à puce 32
Tableaux d'identification des incidents 33
Identification des incidents liés à l'installation . . 33

Annexe A. Réglementation américaine relative à l'exportation du logiciel Client Security 35

Annexe B. Informations relatives aux mots de passe et mots de passe composés 37
Règles relatives aux mots de passe et aux mots de passe composés 37
Règles applicables au mot de passe administrateur 37
Règles relatives aux mots de passe composés UVM 38
Nombre d'échecs sur les systèmes utilisant le TPM national 39
Nombre d'échecs sur les systèmes utilisant le TPM Atmel 40
Réinitialisation d'un mot de passe composé . . . 41
Réinitialisation à distance d'un mot de passe composé 41
Réinitialisation manuelle d'un mot de passe composé 41

Annexe C. Remarques 43
Remarques 43
Marques 44

Avis aux lecteurs canadiens

Le présent document a été traduit en France. Voici les principales différences et particularités dont vous devez tenir compte.

Illustrations

Les illustrations sont fournies à titre d'exemple. Certaines peuvent contenir des données propres à la France.

Terminologie

La terminologie des titres IBM peut différer d'un pays à l'autre. Reportez-vous au tableau ci-dessous, au besoin.

IBM France	IBM Canada
ingénieur commercial	représentant
agence commerciale	succursale
ingénieur technico-commercial	informaticien
inspecteur	technicien du matériel

Claviers

Les lettres sont disposées différemment : le clavier français est de type AZERTY, et le clavier français-canadien de type QWERTY.

OS/2 et Windows - Paramètres canadiens

Au Canada, on utilise :

- les pages de codes 850 (multilingue) et 863 (français-canadien),
- le code pays 002,
- le code clavier CF.

Nomenclature

Les touches présentées dans le tableau d'équivalence suivant sont libellées différemment selon qu'il s'agit du clavier de la France, du clavier du Canada ou du clavier des États-Unis. Reportez-vous à ce tableau pour faire correspondre les touches françaises figurant dans le présent document aux touches de votre clavier.

France	Canada	Etats-Unis
(Pos1)		Home
Fin	Fin	End
(PgAr)		PgUp
(PgAv)		PgDn
Inser	Inser	Ins
Suppr	Suppr	Del
Echap	Echap	Esc
Attn	Intrp	Break
Impr écran	ImpEc	PrtSc
Verr num	Num	Num Lock
Arrêt défil	Défil	Scroll Lock
(Verr maj)	FixMaj	Caps Lock
AltGr	AltCar	Alt (à droite)

Brevets

Il est possible qu'IBM détienne des brevets ou qu'elle ait déposé des demandes de brevets portant sur certains sujets abordés dans ce document. Le fait qu'IBM vous fournisse le présent document ne signifie pas qu'elle vous accorde un permis d'utilisation de ces brevets. Vous pouvez envoyer, par écrit, vos demandes de renseignements relatives aux permis d'utilisation au directeur général des relations commerciales d'IBM, 3600 Steeles Avenue East, Markham, Ontario, L3R 9Z7.

Assistance téléphonique

Si vous avez besoin d'assistance ou si vous voulez commander du matériel, des logiciels et des publications IBM, contactez IBM direct au 1 800 465-1234.

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, «Téléchargement, installation et configuration 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. Il vient compléter le manuel *Logiciel Client Security - Guide d'administration et 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 et d'utilisation*

Le présent document contient des références au manuel *Logiciel Client Security - Guide d'administration et d'utilisation*. Le *Guide d'administration et d'utilisation* 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 et d'utilisation* pour configurer et gérer la stratégie de sécurité sur chaque client.

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

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 TCG (Trusted Computing Group) définies dans TCG Main Specification version 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. 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 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.
- **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 version 5.1**

  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 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 4.8 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);
- le support Lotus Notes par la protection améliorée de l'authentification de l'ouverture de session.

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.

Les utilisateurs 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 du BIOS 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 Entrée ou 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 ThinkCentre et *mot de passe superviseur* dans l'utilitaire de configuration du BIOS ThinkPad.

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 support externe 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. Téléchargement, installation et configuration 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 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. Dans la boîte Resources, cliquez sur **Support and downloads**.
3. Dans la section Embedded Security Subsystem and IBM Client Security Software de la page Web, cliquez sur **Software download**.
4. Dans la boîte Select a system, cliquez sur **Detect my system & continue** ou entrez le numéro de modèle/type de votre machine (à 7 chiffres) dans la zone appropriée.
5. Entrez votre adresse électronique dans la zone fournie et sélectionnez votre pays/zone géographique dans le menu déroulant.
6. Cochez la case appropriée si vous souhaitez recevoir des informations sur les autres offres.
7. Consultez le contrat de licence en cliquant sur **View Licence**, puis sur **Accept Licence**.

   Vous êtes alors automatiquement redirigé vers la page de téléchargement d'IBM Client Security.
8. Recherchez le lien correspondant à Client Security Software 5.4 et cliquez sur **Download Now**.

   Remarque : Consultez le fichier `css54readme.html` pour les informations spécifiques de mise à niveau et de limitation.
9. Cliquez sur **Save** pour sauvegarder une copie du fichier exécutable d'installation sur votre disque dur.

10. Indiquez l'emplacement de sauvegarde et cliquez sur **Save**. Pour commencer l'installation du logiciel, cliquez sur **Open** lorsque le téléchargement est terminé, ou cliquez deux fois sur l'icône du fichier exécutable.

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

Installation du logiciel

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

1. Cliquez deux fois sur le fichier exécutable.

   L'écran de bienvenue de l'assistant d'installation du logiciel IBM Client Security s'affiche.
2. Cliquez sur **Suivant**.

   Le contrat de licence du logiciel IBM Client Security s'affiche.
3. Prenez connaissance des dispositions du contrat de licence, sélectionnez le bouton d'option **J'accepte les dispositions du contrat de licence** et cliquez sur **Suivant**.

   L'écran de sélection du produit s'affiche.
4. Sélectionnez l'un des boutons d'option suivants et cliquez sur **Suivant**.
   - **Logiciel IBM Client Security et IBM Password Manager.** Cette option permet d'installer ou de mettre à niveau le logiciel IBM Client Security, IBM Password Manager et tous les pilotes de périphériques nécessaires.
   - **Logiciel IBM Client Security uniquement.** Cette option permet d'installer ou de mettre à niveau le logiciel IBM Client Security et tous les les pilotes de périphériques nécessaires.

   L'écran indiquant le dossier cible s'affiche.
5. Cliquez sur **Suivant** pour accepter l'emplacement d'installation par défaut, ou cliquez sur **Modifier** pour accéder au dossier cible souhaité.

   L'écran indiquant que le programme est prêt à être installé s'affiche.
6. Cliquez sur **Installer** pour commencer l'installation, ou cliquez sur **Retour** pour revoir ou modifier les paramètres d'installation.

   Une barre d'état affiche la progression de l'installation et l'écran de fin de l'assistant d'installation InstallShield s'affiche.
7. Cliquez sur **Fin** pour sortir de l'assistant.

Vous devez redémarrer votre ordinateur pour que les modifications apportées lors de l'installation soient prises en compte.

Sélection d'une option de configuration

Le premier écran de l'assistant d'installation du logiciel IBM Client Security vous permet de sélectionner une option de configuration. Il est très important de sélectionner l'option de configuration appropriée. Lisez attentivement les informations suivantes avant de sélectionner une option de configuration. Les utilisateurs débutants doivent sélectionner l'option de *configuration classique*.

Configuration classique

Lorsque vous sélectionnez la configuration classique du logiciel IBM Client Security à l'aide de l'assistant d'installation du logiciel Client Security, vous configurez les fonctions suivantes d'IBM Client Security :

- IBM Password Manager (s'il est sélectionné lors de l'installation)

- Chiffrement de fichiers en cliquant à l'aide du bouton droit de la souris
- Authentification du mot de passe composé et de l'empreinte digitale
- Support de signature numérique

L'utilisation de l'option de *configuration classique* conseillée dans l'assistant d'installation du logiciel Client Security simplifie le processus de configuration. Toutefois, certaines fonctions évoluées du logiciel Client Security sont désactivées lorsque cette configuration est sélectionnée, rendant ainsi certaines fonctions CSS non disponibles.

Paramètres de configuration classique par défaut

Les paramètres de configuration classique définis dans le code par défaut sont les suivants :

- **Emplacement de l'archive :** C:\documents and settings\all users\application data\ibm\security\archive
- **Emplacement de la paire de clés administrateur :** C:\documents and settings\all users\application data\ibm\security\keys

  La clé privée de l'administrateur n'est pas divisée et est chiffrée à l'aide du mot de passe composé de l'administrateur CSS.

Les autres paramètres sont les suivants :

- Le support IBM Password Manager est activé.
- La stratégie de sécurité est moyenne : chaque méthode d'authentification disponible est requise uniquement à la première utilisation d'une fonction CSS.
- L'authentification par mot de passe composé est toujours requise.
- L'authentification par empreinte digitale est requise lorsqu'un lecteur d'empreinte digitale intégré est détecté lors de l'installation.
- Le mot de passe composé UVM de l'utilisateur qui installe CSS tient également lieu de *mot de passe administrateur* CSS. Le fait de modifier le mot de passe composé UVM modifie également le mot de passe administrateur CSS. Le mot de passe composé administrateur CSS n'expire jamais.

Limitations relatives aux composants de la configuration classique

Certaines fonctions du logiciel Client Security qui sont activées à l'issue d'une configuration évoluée sont désactivées lorsqu'une configuration classique est sélectionnée. Ces fonctions ne peuvent pas être utilisées dans une configuration classique de CSS. Pour activer ces fonctions, vous devez convertir votre configuration en configuration évoluée. Les différences de fonctionnement à l'issue d'une configuration classique sont les suivantes :

- **Utilitaire d'administration**

  Les actions suivantes ne sont pas admises dans une configuration classique :

  – Réinitialisation d'un utilisateur
  – Suppression d'un utilisateur
  – Modification du mot de passe administrateur à l'aide du bouton Paramètres de puce
  – Fonctions de configuration de clé

  Si un utilisateur tente d'effectuer d'une des opérations ci-dessus, il sera invité à convertir la configuration en configuration CSS évoluée. Le processus de conversion déchiffre la clé privée administrateur et transfère la paire de clés administrateur vers un emplacement défini par l'utilisateur.

- **Console d'administration**

  Les différences d'utilisation suivantes s'appliquent dans une configuration classique :

  – Les valeurs de répertoire de l'archive, d'emplacement de clé privée et d'emplacement de clé publique sont figées dans le code et ne peuvent pas être modifiées. L'archive peut seulement être modifiée sur l'ordinateur local.

  – L'option de configuration de l'itinérance des accréditations n'est pas disponible dans la configuration classique. Si vous sélectionnez une configuration classique et que vous souhaitez configurer un réseau itinérant d'accréditation, vous devez d'abord convertir votre configuration classique en configuration évoluée.

  – L'opération de contournement de mot de passe composé UVM ne peut pas être effectuée pour l'administrateur CSS.

- **Utilitaire de configuration utilisateur**

  Les différences d'utilisation suivantes s'appliquent dans une configuration classique :

  – Le mot de passe composé UVM de l'utilisateur qui installe CSS tient également lieu de mot de passe administrateur. Le fait de modifier le mot de passe composé UVM modifie également le mot de passe administrateur.

  – L'utilisateur administrateur CSS ne peut pas être réinitialisé.

  – L'option de configuration de l'itinérance des accréditations n'est pas disponible dans la configuration classique.

Conversion d'une configuration classique en configuration évoluée

Pour convertir une configuration Client Security classique en configuration évoluée, procédez comme suit :

1. Démarrez l'utilitaire d'administration.
2. Entrez le mot de passe administrateur CSS.
3. Cliquez sur le bouton **Configuration de clé**.
4. Cliquez sur **OK** pour continuer.
5. Sélectionnez l'emplacement dans lequel vous souhaitez stocker la paire de clés administrateur déchiffrées. La paire de clés administrateur déchiffrées ne doit pas être stockée sur l'unité de disque dur locale. Le processus de conversion est maintenant terminé.
6. Modifiez l'emplacement de l'archive. L'archive ne doit pas être stockée sur l'unité de disque dur locale.

Une fois que vous avez converti la configuration Client Security en configuration évoluée, vous ne pouvez pas la reconvertir en configuration classique.

Configuration évoluée

La *configuration évoluée* du logiciel IBM Client Security configure les fonctions Client Security *supplémentaires* suivantes :

- **Protection de connexion UVM**
- **Sélection d'emplacement d'enregistrement de clé**
- **Prise en charge d'application :** Entrust, chiffrement des fichiers et dossiers (FFE), Lotus Notes

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

L'assistant d'installation d'IBM Client Security fournit une interface qui vous aide à installer le logiciel Client Security et à activer la puce de sécurité intégrée IBM. Procédez comme suit pour permettre à l'assistant d'installation d'IBM Client Security de vous guider tout au long de l'exécution des tâches nécessaires pour configurer une stratégie de sécurité sur un client IBM.

Les étapes générales au cours desquelles l'assistant d'installation d'IBM Client Security vous guide sont décrites ci-dessous. Les étapes spécifiques varient en fonction de l'option de configuration que vous choisissez.

- **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.

- **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.

- **Autorisation des 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.

Utilisation de l'assistant d'installation pour l'exécution d'une configuration classique

Pour utiliser l'assistant d'installation d'IBM Client Security pour exécuter une configuration classique, procédez comme suit :

1. 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 vous permet de sélectionner une option de configuration.

2. Sélectionnez le bouton d'option Configuration classique (recommandé) et cliquez sur **Suivant**.

Cette sélection active IBM Password Manager et nécessite uniquement la saisie de quelques paramètres. Lorsque vous sélectionnez la configuration classique, CSS stocke vos informations de sauvegarde et vos clés de sécurité sur le disque dur. Les utilisateurs débutants doivent utiliser l'option de configuration classique. Il s'agit du paramètre par défaut.

L'écran Saisie de mot de passe composé s'affiche.

3. Exécutez les tâches suivantes :
   a. Entrez un mot de passe composé dans la zone Saisie de mot de passe composé. Si nécessaire, cliquez sur le bouton **Affichage des conditions requises pour les mots de passe composés** pour vous aider à définir un mot de passe composé valide.

      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 composé dans la zone Confirmation du mot de passe composé. Vous pouvez également être invité à fournir votre mot de passe superviseur, le cas échéant.

   b. Tapez un mot ou une expression dans la zone d'indice de mot de passe composé.
   c. Cliquez sur **Suivant**.

   Si un lecteur d'empreinte digitale est détecté sur votre ordinateur, l'écran Enregistrement d'empreinte digitale s'affiche. La case **Oui, Je souhaite enregistrer maintenant des empreintes digitales** est cochée par défaut.
4. Exécutez l'une des opérations suivantes :
   - Désélectionnez la case **Oui, Je souhaite enregistrer maintenant des empreintes digitales** et cliquez sur **Suivant**.
   - Cliquez sur **Suivant** et suivez les instructions affichées pour commencer l'enregistrement de vos empreintes digitales maintenant.

   L'écran permettant d'autoriser des utilisateurs supplémentaires s'affiche.
5. Exécutez l'une des opérations suivantes :
   - Cochez la case **Sélectionner d'autres utilisateurs à autoriser (facultatif)** et cliquez sur **Suivant**.
   - Cliquez sur **Ignorer** pour ignorer cette tâche.

   L'écran Récapitulatif de vos paramètres et fonctions de sécurité s'affiche.
6. Cliquez sur **Fin** pour implémenter les paramètres de sécurité que vous avez sélectionnés. Ce processus peut prendre quelques minutes. Un message s'affiche pour indiquer que l'ordinateur est maintenant protégé par IBM Client Security.
7. Cliquez sur **OK**.

Utilisation de l'assistant d'installation pour l'exécution d'une configuration évoluée

Pour utiliser l'assistant d'installation d'IBM Client Security pour exécuter une configuration classique, procédez comme suit :

1. 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 vous permet de sélectionner une option de configuration.
2. Sélectionnez le bouton d'option **Configuration évoluée** et cliquez sur **Suivant**.

Cette option nécessite que vous indiquiez des informations de configuration, telles qu'un emplacement d'enregistrement de clé et un niveau de sécurité, et permet d'activer la protection de connexion CSS, la protection Lotus Notes et Password Manager.

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 l'emplacement d'archive de clés 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 système 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.

- **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 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.

L'écran indiquant que la configuration est terminée et permettant de vérifier les paramètres de sécurité s'affiche.

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**.

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. Si la puce n'a pas été activée, 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**.

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

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 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 la dernière version du logiciel Client Security et configurez-la à l'aide de l'assistant d'installation d'IBM Client Security.

Mise à niveau de CSS version 5.0 ou suivante à l'aide des données de sécurité existantes

Si vous voulez effectuer une mise à niveau de la version 5.0 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. Mettez à niveau 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.

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 35.

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'installation ou de la configuration du logiciel Client Security.

Fonctions d'administrateur

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.

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.

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 Security Feature** et appuyez sur Entrée.
5. Cliquez sur **Yes**.
6. Appuyez sur Entrée pour confirmer votre choix.
7. Appuyez sur F10 pour sauvegarder vos modifications et sortir du programme de configuration.
8. Sélectionnez **Yes** et 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 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 Security Chip** et appuyez sur Entrée.
5. Appuyez sur Entrée et sélectionnez **Disabled**.
6. Appuyez sur Entrée pour confirmer votre choix.
7. Appuyez sur Entrée pour continuer.
8. Appuyez sur F10 pour sauvegarder vos modifications et sortir du programme de configuration.
9. Sélectionnez **Yes** et appuyez sur Entrée. L'ordinateur redémarre.

Incidents ou limitations connus concernant CSS version 5.4

Les informations ci-après pourront vous être utiles lors de l'installation ou de la configuration du logiciel IBM Client Security version 5.4.

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 5.4 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.

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.

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** pour la supprimer. Redémarrez l'ordinateur et 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.
Un message d'erreur s'affiche lorsque vous tentez d'exécuter certaines fonctions 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 ou le mot de passe administrateur BIOS ThinkCentre doit être désactivé pour générer la paire de clés matérielles sur un système Crypto 1 (non TCG). Le processus d'installation CSS ne peut pas activer le sous-système de sécurité intégré IBM tant que le mot de passe approprié n'est pas désactivé.

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

Une interface de l'utilitaire d'administration permet aux administrateurs de sécurité de contrôler les critères de mot de passe administrateur via une interface simple. Cette interface permet à un administrateur de définir les règles de mot de passe administrateur suivantes :

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

- 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.

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

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

Caractères
Le mot de passe 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 administrateur 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 administrateur 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).

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 utilisant le TPM national

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

Tentatives	Période de suspension lors du prochain échec
7-13	4 secondes chacune
14-20	8 secondes chacune
21-27	16 secondes chacune
28-34	32 secondes chacune
35-41	64 secondes chacune (1,07 minute chacune)
42-48	128 secondes chacune (2,13 minutes chacune)
49-55	256 secondes chacune (4,27 minutes chacune)

Tentatives	Période de suspension lors du prochain échec
56-62	512 secondes chacune (8,53 minutes chacune)
63-69	1024 secondes chacune (17,07 minutes chacune)
70-76	2048 secondes chacune (34,13 minutes chacune)
77-83	68,26 minutes chacune (1,14 heure chacune)
84-90	136,52 minutes chacune (2,28 heures chacune)
91-97	273,04 minutes chacune (4,55 heures chacune)
98-104	546,08 minutes chacune (9,1 heures chacune)
105-111	1092,16 minutes chacune (18,2 heures chacune)
112-118	2184,32 minutes chacune (36,4 heures chacune)

Les systèmes TPM nationaux 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. Il n'existe pas de délai d'attente maximal. Chaque échec déclenche la période de suspension indiquée ci-dessus. Les périodes de suspension anti-martèlement ne prennent pas fin à la 118ème tentative ; elles continuent plutôt indéfiniment de la manière illustrée ci-dessus.

Nombre d'échecs sur les systèmes utilisant le TPM Atmel

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

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 TPM Atmel 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 TPM Atmel ne peuvent appliquer de suspension supérieure à 4,7 heures.

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.