Solutions IBM Client Security

Logiciel Client Security version 5.1
Guide d'installation

Solutions IBM Client Security

Logiciel Client Security version 5.1
Guide d'installation

Première édition - avril 2003

Réf. US : 59P7666

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

Table des matières

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

Ce manuel contient des informations relatives à l'installation du logiciel Client Security sur des ordinateurs de réseau IBM, également appelés clients IBM, qui renferment des puces de sécurité intégrées IBM. Il présente également des instructions concernant l'activation de la puce de sécurité intégrée IBM et la définition d'un mot de passe matériel de sécurité.

Ce manuel est constitué des sections suivantes :

Le Chapitre 1, «**Introduction au logiciel IBM Client Security**», contient une présentation générale des applications et des composants qui sont inclus dans le logiciel, ainsi qu'une description des fonctions PKI (infrastructure de clés publiques).

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 Client Security.

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

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

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

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

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

A qui est destiné ce manuel

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

Comment utiliser ce manuel

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

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/ww/security/secdownload.html.

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

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

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

Références au manuel *Logiciel Client Security - Guide de l'utilisateur*

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

Informations complémentaires

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

Chapitre 1. Introduction au logiciel IBM Client Security

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 clients IBM d'utiliser la sécurité client à l'échelle d'un réseau, d'une entreprise ou de l'internet.

Applications et composants du logiciel Client Security

Lorsque vous installez le logiciel Client Security, les applications et composants suivants sont installés :

- **Utilitaire d'administration :** Cet utilitaire est l'interface que l'administrateur utilise pour activer ou désactiver la puce de sécurité intégrée 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.
- **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 UVM offre les fonctions suivantes :
  - **Protection de stratégie client UVM :** Le logiciel UVM permet à l'administrateur de définir la stratégie de sécurité du client, qui régit le mode d'identification de l'utilisateur client sur le système.

    Si la stratégie indique qu'une empreinte digitale est requise pour établir la connexion et que l'utilisateur n'a encore enregistré aucune empreinte digitale, il a la possibilité de le faire au moment de la connexion. Si la vérification des empreintes digitales est requise et qu'aucun scanneur n'est connecté, UVM signale une erreur. Si le mot de passe Windows n'est pas enregistré ou s'il n'est pas correctement enregistré, sous UVM, l'utilisateur aura la possibilité de fournir le mot de passe Windows correct lors de la connexion.
  - **Protection de l'ouverture de session sur le système par UVM :** Le logiciel UVM permet à l'administrateur de contrôler l'accès à l'ordinateur à l'aide d'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.
  - **Protection par économiseur d'écran UVM Client Security :** Le logiciel UVM permet aux utilisateurs de contrôler l'accès à l'ordinateur à l'aide d'une interface d'économiseur d'écran Client Security.
- **Console d'administration :** la console d'administration du logiciel Client Security permet à l'administrateur de la sécurité d'exécuter à distance des tâches d'administration spécifiques.
- **Utilitaire de configuration utilisateur :** Cet utilitaire permet à un utilisateur client de modifier le mot de passe composé UVM. Sous Windows 2000 ou Windows XP, l'utilitaire de configuration utilisateur permet également aux utilisateurs de modifier les mots de passe de connexion Windows afin d'être reconnus par UVM et de mettre à jour les archives de clés. Les utilisateurs peuvent également créer des copies de sauvegarde des certificats numériques créés à l'aide de la puce de sécurité intégrée IBM.

Fonctions PKI (Public Key Infrastructure)

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 la cryptographie 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 matériel 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 la puce de sécurité intégrée IBM comme fournisseur de service pour les applications utilisant Microsoft CryptoAPI. Il peut s'agir des applications Internet Explorer et Microsoft Outlook Express. Ainsi, la clé privée du certificat numérique est stockée sur la puce de sécurité. De même, les utilisateurs de Netscape peuvent choisir la puce de sécurité intégrée IBM comme générateur de clé privée pour les certificats numériques utilisés pour la sécurité. Les applications utilisant la norme PKCS (Public-Key Cryptography Standard) n° 11, telles que Netscape Messenger, peuvent bénéficier de la protection fournie par la puce de sécurité intégrée IBM.
- **Possibilité de transférer les certificats numériques à la puce de sécurité intégrée IBM.** L'outil de transfert de certificats du logiciel IBM Client Security vous permet de déplacer les certificats qui ont été créés avec le fournisseur de service cryptographique Microsoft par défaut vers le fournisseur de service cryptographique de la puce de sécurité intégrée IBM. Cela augmente fortement le niveau de protection des clés privées associées aux certificats car elles sont maintenant stockées en toute sécurité sur la puce de sécurité intégrée IBM plutôt que dans un logiciel vulnérable.
- **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 offre une interface permettant de générer une archive pour les clés et les certificats numériques créés à l'aide de la puce de sécurité intégrée IBM et de les restaurer si nécessaire.
- **Chiffrement des fichiers et des dossiers.** La fonction de chiffrement des fichiers et des dossiers permet à l'utilisateur client de chiffrer ou de déchiffrer rapidement et simplement des fichiers ou des dossiers. Cette fonction s'ajoute aux mesures de sécurité du système CSS pour améliorer le niveau de sécurité des données.
- **Authentification des empreintes digitales.** Le logiciel IBM Client Security prend en charge les lecteurs d'empreintes digitales Targus PC Card et Targus

USB pour l'authentification. Pour garantir un fonctionnement correct, vous devez installer le logiciel Client Security avant les lecteurs d'empreintes digitales Targus.

- **Authentification des cartes à puce.** Le logiciel IBM Client Security prend désormais en charge certaines cartes à puce en tant que périphérique d'authentification. Client Security permet aux cartes à puce d'être utilisées en tant que jeton d'authentification pour un seul utilisateur à la fois. Chaque carte à puce est liée à un système, sauf si la fonction d'itinérance des données d'identification est utilisée. L'exigence d'une carte à puce rend votre système plus sûr car cette carte doit être fournie en plus d'un mot de passe, ce dernier pouvant être compromis.
- **Itinérance des données d'identification.**La fonction d'itinérance des données d'identification permet à un utilisateur réseau reconnu par UVM d'utiliser n'importe quel système 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 CSS enregistré, il peut importer ses données personnelles sur n'importe quel autre client enregistré du réseau. Ses données personnelles seront automatiquement mises à jour et gérées dans l'archive CSS et sur tout système sur lequel elles ont été importées. Les mises à jour des données personnelles, telles que les nouveaux certificats ou les changements de mot de passe composé, seront automatiquement disponibles sur tous les autres systèmes.
- **Certification FIPS 140-1.** Le logiciel Client Security prend en charge les bandothèques cryptographiques certifiées FIPS 140-1. Les bandothèques RSA BSAFE certifiées FIPS sont utilisées sur les systèmes TCPA.
- **Expiration du mot de passe composé.** Le logiciel Client Security établit un mot de passe composé propre à l'utilisateur et une stratégie d'expiration de ce mot de passe composé lorsque chaque utilisateur est ajouté à UVM.
- **Protection automatique des dossiers sélectionnés.** La fonction de protection automatique des dossiers permet à l'administrateur du logiciel Client Security de définir que le dossier Mes documents de chaque utilisateur reconnu par UVM doit être automatiquement protégé, sans requérir aucune action de l'utilisateur.

Chapitre 2. Mise en route

Cette section présente le matériel et les logiciels compatibles requis pour l'utilisation du logiciel Client Security. Elle contient également des informations sur le téléchargement du logiciel Client Security.

Matériel requis

Avant de télécharger et d'installer le logiciel, assurez-vous que votre matériel informatique est compatible avec le logiciel 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/ww/security/secdownload.html.

Puce de sécurité intégrée IBM

La puce de sécurité intégrée IBM est un microprocesseur cryptographique qui est intégré à la carte système 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 des puces de sécurité intégrées IBM prennent en charge le logiciel Client Security. Si vous essayez de télécharger et d'installer le logiciel sur un ordinateur qui ne contient pas de puce de sécurité intégrée 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/ww/resources/security/secdownload.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 Client Security.

Systèmes d'exploitation

Le logiciel 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 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 Client Security, puis réinstaller le capteur compatible avec UVM.

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

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

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

- **Lotus Notes version 4.5 ou suivante**

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

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

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

- **RSA SecurID Software Token**

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

- **Lecteur d'empreinte digitale Targus**

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

- **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 Client Security prend en charge les navigateurs Web suivants pour les demandes de certificats numériques :

- Internet Explorer version 5.0 ou suivante
- Netscape versions 4.51 à 7

Informations sur le chiffrement renforcé du navigateur Web

Si le dispositif de chiffrement renforcé est installé, utilisez la version 128 bits de votre navigateur Web. Sinon, utilisez la version 40 bits du 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 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 Client Security vous permet d'utiliser les opérations cryptographiques de la puce de sécurité intégrée 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 de la puce de sécurité intégrée IBM, vous pouvez utiliser la puce de sécurité intégrée IBM pour générer des certificats numériques pour Netscape, Entrust, RSA et d'autres applications utilisant PKCS#11.

Applications de messagerie

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

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

Téléchargement du logiciel

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

Formulaire d'enregistrement

Lorsque vous téléchargez le logiciel, vous devez remplir un formulaire d'enregistrement et un questionnaire, et accepter les termes du contrat de licence. Suivez les instructions qui sont fournies sur le site Web pour télécharger le logiciel.

Les fichiers d'installation du logiciel Client Security sont inclus dans le fichier auto-extractible nommé csec51.exe.

Réglementations régissant l'exportation

Le logiciel 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 Client Security. Pour plus d'informations sur les réglementations régissant l'exportation du logiciel Client Security, reportez-vous à l'Annexe A, «Réglementation américaine relative à l'exportation du logiciel Client Security», à la page 47.

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 Client Security sur les clients IBM. Tous les fichiers requis pour l'installation sont inclus dans le fichier csec51.exe que vous téléchargez à partir du site Web IBM.

Avant d'installer le logiciel

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

Installation sur des clients dotés de Windows XP ou Windows 2000

Les utilisateurs de Windows XP et Windows 2000 doivent se connecter avec des droits d'administrateur pour installer le logiciel 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 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 (la puce de sécurité intégrée) et dont vous générez les clés de chiffrement matérielles. Ces fonctions sont le mot de passe administrateur et la sécurité avancée.

Mot de passe administrateur (NetVista)

Les mots de passe administrateur empêchent les personnes non autorisées de modifier les paramètres de configuration d'un ordinateur IBM. Ces mots de passe sont définis à l'aide du programme de configuration, qui est accessible en appuyant sur F1 pendant la séquence d'amorçage du système.

Mot de passe superviseur (ThinkPad)

Les mots de passe superviseur empêchent les personnes non autorisées de modifier les paramètres de configuration d'un ordinateur ThinkPad IBM. Ces mots de passe sont définis à l'aide de l'utilitaire de configuration du BIOS IBM, qui est accessible en appuyant sur F1 pendant la séquence d'amorçage du système.

Sécurité avancée

La sécurité avancée assure une protection supplémentaire du mot de passe administrateur et des paramètres de la séquence d'amorçage. Vous pouvez vérifier 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 du système.

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 la puce et générer les clés matérielles.

Lorsque la sécurité avancée est activée sur ces modèles de NetVista, vous devez utiliser l'utilitaire d'administration pour activer la puce de sécurité intégrée et générer les clés de chiffrement matérielles après l'installation du logiciel 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 la puce et générer les clés matérielles.

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 la puce de sécurité intégrée. Après avoir activé la puce, vous pouvez utiliser l'utilitaire d'administration pour générer les clés matérielles.

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 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 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 de NetVista approprié et suivez les instructions de la page Web.

Utilisation de la paire de clés d'archive

La paire de clés d'archive, qui comprend la clé publique d'administrateur et la clé privée d'administrateur, vous permet de générer des clés de chiffrement matérielles pour un client IBM et de conserver des copies des données de clé à un autre endroit en vue d'une éventuelle restauration.

Etant donné que vous utilisez l'utilitaire d'administration de Client Security pour créer la paire de clés d'archive, vous devez installer le logiciel Client Security sur un client IBM initial, puis créer la paire de clés d'archive. Les instructions d'installation et de configuration du logiciel sur le premier client IBM sont fournies ci-après.

Remarque : Si vous envisagez d'utiliser une stratégie UVM applicable à des clients éloignés, vous devez faire appel à la même paire de clés d'archive lorsque vous installez le logiciel sur ces clients.

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

Cette section contient les instructions de téléchargement, d'installation et de configuration du logiciel 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 d'une version antérieure à la version 5.0 du logiciel Client Security, vous devez déchiffrer tous les fichiers chiffrés avant d'installer le logiciel Client Security version 5.1. En effet, le logiciel Client Security version 5.1 ne peut pas déchiffrer les fichiers qui ont été chiffrés à l'aide des versions de Client Security antérieures à la version 5.0 en raison des modifications apportées à la mise en oeuvre du chiffrement des fichiers.

Téléchargement et installation du logiciel

Tous les fichiers requis pour l'installation du logiciel Client Security sont inclus dans le fichier csec51.exe que vous téléchargez à partir du site Web IBM http://www.pc.ibm.com/ww/security/secdownload.html. Ce site Web fournit des informations qui vous permettent de vous assurer que votre système est doté de la puce de sécurité intégrée IBM et de sélectionner l'offre 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/ww/security/secdownload.html.
2. Conformément aux informations du site Web, vérifiez que la puce de sécurité intégrée IBM est installée sur votre système en comparant votre numéro de modèle avec ceux indiqués dans le tableau des systèmes requis, puis cliquez sur **Continue**.
3. Sélectionnez le bouton d'option qui correspond à votre type de machine et cliquez sur **Continue**.
4. Créez un ID utilisateur, enregistrez-vous auprès d'IBM en complétant le formulaire en ligne et lisez le contrat de licence, puis cliquez sur **Accept Licence**.

   Vous êtes alors automatiquement redirigé vers la page de téléchargement de Client Security.
5. Suivez les étapes de la page de téléchargement pour télécharger les pilotes de périphérique nécessaires, les fichiers readme, le logiciel, les documents de référence et les utilitaires complémentaires du logiciel IBM Client Security. Respectez l'ordre de téléchargement indiqué sur le site Web.
6. A partir du bureau Windows, cliquez sur **Démarrer > Exécuter**.
7. Dans la zone Exécuter, tapez `d:\répertoire\csec51.exe`, où d:\répertoire\ correspond à l'unité et au répertoire où se trouve le fichier.
8. Cliquez sur **OK**.

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

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

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

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

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

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

Les étapes à suivre sont les suivantes :

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

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

- **Création des clés de sécurité administrateur**

  Les clés de sécurité administrateur sont un ensemble de clés numériques qui sont stockées dans un fichier informatique. Il est recommandé de sauvegarder ces clés de sécurité sur une unité ou un disque amovible. Lorsqu'une modification est apportée à la stratégie de sécurité dans l'utilitaire d'administration d'IBM Client Security, le système vous demande de fournir ce fichier 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 système ou l'unité de disque dur de votre ordinateur. Ces informations de sauvegarde doivent être stockées en-dehors du système.

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

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

- **Affectation d'autorisations aux utilisateurs**

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

7. Activez la protection IBM Client Security en cochant les cases appropriées et en cliquant sur **Suivant**. Les options Client Security disponibles sont les suivantes :
   - **Protection de l'accès à votre 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.

- **Activation du chiffrement de fichiers et de dossiers**

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

- **Activation de la prise en charge du gestionnaire de mots de passe IBM Client Security**

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

- **Remplacement de la connexion à Lotus Notes par la connexion à IBM Client Security**

  Cochez cette case si vous voulez que le logiciel Client Security authentifie les utilisateurs de Lotus Notes à l'aide de la puce de sécurité intégrée IBM.

- **Activation de la prise en charge d'Entrust**

  Cochez cette case si vous voulez permettre l'intégration des produits logiciels de sécurité Entrust.

- **Protection de Microsoft Internet Explorer**

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

Une fois que vous avez coché les cases appropriées, l'écran Affectation d'autorisations aux utilisateurs s'affiche.

8. Renseignez cet écran en procédant comme suit :
   - Pour autoriser des utilisateurs à exécuter des fonctions d'IBM Client Security, procédez comme suit :
     a. Sélectionnez un utilisateur dans la zone Utilisateurs non autorisés.
     b. Cliquez sur **Autorisation utilisateur**.
     c. Saisissez et confirmez votre mot de passe composé IBM Client Security dans les zones appropriées et cliquez sur **Fin**.
     d. 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**.
     c. Saisissez et confirmez votre mot de passe composé IBM Client Security dans les zones appropriées et cliquez sur **Fin**.
     d. Cliquez sur **Suivant**.

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

9. Sélectionnez le niveau de sécurité du système en procédant comme suit :
   a. Sélectionnez les règles d'authentification que vous voulez utiliser en cochant les cases appropriées. Vous pouvez sélectionner plusieurs règles d'authentification.
   b. 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 IBM Client Security.
10. Vérifiez vos paramètres de sécurité et effectuez une des actions suivantes :
    - Pour accepter les paramètres, cliquez sur **Fin**.
    - Pour modifier les paramètres, cliquez sur **Précédent**, faites les modifications appropriées, puis revenez à cet écran et cliquez sur **Fin**.

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

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

Activation de la puce de sécurité IBM

La puce de sécurité IBM doit être activée 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 la puce 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 client IBM**.

   Un écran affiche un message qui stipule que la puce de sécurité IBM n'a pas été activée 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. Effectuez 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 client IBM** pour ouvrir l'utilitaire d'administration.

   Un message s'affiche et indique que la puce de sécurité IBM n'a pas été configurée ou a été vidée. Un nouveau mot de passe est alors requis.

6. Saisissez et confirmez le nouveau mot de passe de la puce de sécurité IBM dans les zones appropriées, puis cliquez sur **OK**.

   Remarque : Le mot de passe doit contenir huit caractères.

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

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

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

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

Exécution d'une installation automatisée

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

Avant de commencer une installation automatisée, lisez le Chapitre 3, «Opérations préalables à l'installation du logiciel», à la page 9. Aucun message d'erreur n'est affiché au cours d'une installation automatisée. Si une installation automatisée s'arrête prématurément, vous devez effectuer une installation avec opérateur pour visualiser tous les messages d'erreur susceptibles de s'afficher.

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

Pour plus d'informations sur l'exécution d'une installation automatisée, reportez-vous à la procédure suivante et consultez le fichier css51readme qui est disponible sur le site Web IBM http://www.pc.ibm.com/ww/security/secdownload.html.

Déploiement de masse

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

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

- le pilote de bus SM,
- le pilote de bus LPC (pour les systèmes TCPA).

Le déploiement de masse se décompose en deux étapes principales :

- Installation de masse
- Configuration de masse

Installation de masse

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

Pour lancer une installation de masse, procédez comme suit :

1. Créez le fichier CSS.ini.

   Cette étape n'est requise que si vous avez l'intention d'effectuer une configuration de masse.
2. Extrayez le contenu du module d'installation CSS à l'aide de Winzip en utilisant les noms de dossier.
3. Dans le fichier setup.iss, modifiez les entrées `szIniPath` et `szDir`, qui sont requises pour une configuration de masse.

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

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

Le contenu intégral du fichier setup.iss est répertorié ci-après avec quelques descriptions : [InstallShield Silent] Version=v6.00.000 File=Response File szIniPath=d:\csssetup.ini (Le paramètre ci-dessus a pour valeur le chemin et le nom du fichier .ini qui est requis pour la configuration de masse. Si ce fichier se trouve sur une unité réseau, un identificateur doit être affecté à celle-ci. Lorsque la configuration de masse n'est pas utilisée avec une installation automatique, supprimez cette entrée.) [File Transfer] OverwrittenReadOnly=NoToAll [{7BD2CFF6-B037-47D6-A76B-D941EE13AD96}-DlgOrder] Dlg0={7BD2CFF6-B037-47D6-A76B-D941EE13AD96}-SdLicense-0 Count=4 Dlg1={7BD2CFF6-B037-47D6-A76B-D941EE13AD96}-SdAskDestPath-0 Dlg2={7BD2CFF6-B037-47D6-A76B-D941EE13AD96}-SdSelectFolder-0 Dlg3={7BD2CFF6-B037-47D6-A76B-D941EE13AD96}-SdFinishReboot-0 [{7BD2CFF6-B037-47D6-A76B-D941EE13AD96}-SdLicense-0] Result=1 [{7BD2CFF6-B037-47D6-A76B-

D941EE13AD96}-SdAskDestPath-0] szDir=C:\Program Files\IBM\Security (Le paramètre ci-dessus a pour valeur le répertoire utilisé pour installer Client Security. Il doit s'agir d'un répertoire local de l'ordinateur.) Result=1 [{7BD2CFF6-B037-47D6-A76B-D941EE13AD96}-SdSelectFolder-0] szFolder=IBM Client Security Software (Le paramètre ci-dessus a pour valeur le groupe de programmes Client Security.) Result=1 [Application] Name=Client Security Version=5.00.002f Company=IBM Lang=0009 [{7BD2CFF6-B037-47D6-A76B-D941EE13AD96}-SdFinishReboot-0] Result=6 BootOption=3

Configuration de masse

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

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

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

[CSSSetup]	En-tête de section pour la configuration de CSS.
suppw=bootup	Mot de passe administrateur/superviseur. N'indiquez aucune valeur si aucun mot de passe n'est requis.
hwpw=11111111	Mot de passe matériel CSS. Il doit comporter huit caractères et est toujours requis. Vous devez indiquer la valeur correcte si le mot de passe matériel a déjà été défini.
newkp=1	Indiquez la valeur 1 pour générer une nouvelle paire de clés d'administrateur, ou la valeur 0 pour utiliser une paire de clés d'administrateur existante.
keysplit=1	Lorsque le paramètre newkp a pour valeur 1, ce paramètre détermine le nombre de composants de clé privée. **Remarque :** Si la paire de clés existante utilise plusieurs éléments de clé privée, tous les éléments de clé privée doivent être stockés dans le même répertoire.
kpl=c:\jgk	Emplacement de la paire de clés d'administrateur lorsque le paramètre newkp a pour valeur 1. S'il s'agit d'une unité réseau, un identificateur doit lui être affecté.
kal=c:\jgk\archive	Emplacement de l'archive de clés utilisateur. S'il s'agit d'une unité réseau, un identificateur doit lui être affecté.
pub=c:\jk\admin.key	Emplacement de la clé publique d'administrateur lorsque vous utilisez une paire de clés d'administrateur existante. S'il s'agit d'une unité réseau, un identificateur doit lui être affecté.
pri=c:\jk\private1.key	Emplacement de la clé privée d'administrateur lorsque vous utilisez une paire de clés d'administrateur existante. S'il s'agit d'une unité réseau, un identificateur doit lui être affecté.
clean=0	Indiquez la valeur 1 pour supprimer le fichier .ini après l'initialisation, ou la valeur 0 pour conserver le fichier .ini après l'initialisation.
[UVMEnrollment]	En-tête de section pour l'inscription des utilisateurs.
enrollall=0	Indiquez la valeur 1 pour enregistrer tous les comptes utilisateur locaux dans UVM, ou la valeur 0 pour enregistrer des comptes utilisateur spécifiques dans UVM.
defaultuvmpw=top	Lorsque le paramètre enrollall a pour valeur 1, cette valeur est le mot de passe composé UVM de tous les utilisateurs.

defaultwinpw=down	Lorsque le paramètre enrollall a pour valeur 1, cette valeur est le mot de passe Windows enregistré dans UVM pour tous les utilisateurs.
enrollusers=2	Lorsque le paramètre enrollall a pour valeur 0, cette valeur indique le nombre d'utilisateurs qui seront enregistrés dans UVM.
user1=joseph	Enumérez les utilisateurs à enregistrer en commençant par l'utilisateur 1. Les noms d'utilisateur doivent correspondre aux noms de compte. Pour obtenir le nom de compte réel sous Windows XP, procédez comme suit : 1. Lancez la Gestion de l'ordinateur (Gestionnaire de périphériques). 2. Développez le noeud Utilisateurs et groupes locaux. 3. Ouvrez le dossier Utilisateurs. Les éléments répertoriés dans la colonne Nom sont les noms de compte.
user1uvmpw=chrome	Enumérez les mots de passe composés UVM des utilisateurs à enregistrer en commençant par celui de l'utilisateur 1.
user1winpw=spinning	Enumérez les mots de passe Windows enregistrés dans UVM des utilisateurs à enregistrer en commençant par celui de l'utilisateur 1.
user1domain=0	Indiquez la valeur 0 pour indiquer que ce compte est local, ou la valeur 1 pour indiquer que ce compte se trouve sur le domaine.
user2=hallie user2uvmpw=left user2winpw=right user2domain=0	
[UVMAppConfig]	En-tête de section pour la configuration des modules et des applications compatibles avec UVM.
uvmlogon=0	Indiquez la valeur 1 pour utiliser la protection à la connexion UVM, ou la valeur 0 pour utiliser la connexion Windows.
entrust=0	Indiquez la valeur 1 pour utiliser UVM pour l'authentification Entrust, ou la valeur 0 pour utiliser l'authentification Entrust.
notes=0	Indiquez la valeur 1 pour utiliser la protection UVM pour Lotus Notes, ou la valeur 0 pour utiliser la protection par mot de passe Lotus Notes.
passman=0	Indiquez la valeur 1 pour utiliser le gestionnaire de mots de passe, ou la valeur 0 pour ne pas utiliser le gestionnaire de mots de passe.
folderprotect=0	Indiquez la valeur 1 pour utiliser l'utilitaire de chiffrement des fichiers et dossiers, ou la valeur 0 pour ne pas utiliser l'utilitaire de chiffrement des fichiers et dossiers.

Mise à niveau de votre version du logiciel Client Security

Vous devez mettre à jour les clients sur lesquels des versions de Client Security antérieures à la version 5.0 sont installées avec la version 5.1 du logiciel afin de pouvoir tirer parti des nouvelles fonctions de Client Security.

Important : sur les systèmes TCPA dotés de la version 4.0x du logiciel IBM Client Security, vous devez vider la puce de sécurité avant d'installer IBM Client Security version 5.1. Si vous ne le faites pas, l'installation risque d'échouer ou le logiciel risque de ne pas répondre.

Mise à niveau en utilisant de nouvelles données de sécurité

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

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

Mise à niveau vers Client Security version 5.1 en utilisant les données de sécurité existantes

Si vous voulez effectuer une mise à niveau à partir d'une version du logiciel Client Security antérieure à la version 5.0 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 **Mise à jour de l'archive** pour vous assurer que les informations de sauvegarde soient mises à jour.

      Notez le répertoire d'archivage.
   c. Quittez l'utilitaire client du logiciel IBM Client Security.
2. Supprimez la version existante du logiciel Client Security en procédant comme suit :
   a. Localisez les clés publique et privée d'administrateur qui ont été créées lorsque vous avez configuré la version précédente du logiciel Client Security.
   b. Cliquez sur **Démarrer > Paramètres > Panneau de configuration > Ajout/Suppression de programmes** et sélectionnez l'option de suppression du logiciel IBM Client Security.
   c. Sélectionnez **Non** lorsque vous êtes invité à redémarrer le système.
   d. Arrêtez le système.
3. Videz la puce de sécurité intégrée en procédant comme suit :
   a. Mettez le système sous tension.
   b. Appuyez sur F1 pour accéder à l'utilitaire de configuration du BIOS.
   c. Affichez les paramètres de configuration de la puce de sécurité et videz cette dernière.
   d. Quittez l'utilitaire de configuration du BIOS.

Le système va poursuivre son réamorçage.

4. Lancez le programme d'installation du logiciel Client Security version 5.0.
5. Redémarrez le système lorsque vous y êtes invité.

   Après le redémarrage, l'assistant d'installation du logiciel Client Security est automatiquement lancé. N'exécutez PAS l'assistant d'installation.
6. Cliquez sur **Annulation** pour quitter l'assistant d'installation.
7. Faites une copie de sauvegarde temporaire de la stratégie de sécurité par défaut en procédant comme suit :
   a. A l'aide de l'Explorateur Windows, allez dans le répertoire d'installation du logiciel IBM Client Security (par défaut, le répertoire c:\program files\ibm\security).
   b. Cliquez avec le bouton droit de la souris sur le dossier UVM_Policy, puis sélectionnez **Copier**.
   c. Cliquez avec le bouton droit de la souris sur le bureau Windows, puis cliquez sur **Coller**.

      Une copie de sauvegarde temporaire est alors créée sur le bureau Windows.

      Remarque : Vos paramètres de stratégie de sécurité existants vont être remplacés par les nouveaux paramètres par défaut.
8. Restaurez les paramètres du logiciel IBM Client Security version 4.0x en procédant comme suit :
   a. Cliquez sur **Démarrer > Paramètres > Panneau de configuration > Sous-système de sécurité client IBM**.

      L'écran principal de l'utilitaire d'administration du logiciel IBM Client Security s'affiche alors.
   b. Cliquez sur le bouton **Configuration de clé**.
   c. Sélectionnez **Oui** pour restaurer les clés de l'archive de clés.
9. Indiquez l'emplacement du répertoire d'archivage précédent.
10. Indiquez l'emplacement des fichiers de clés publique et privée d'administrateur que vous avez créés dans la version précédente.

    Le système vous informe que votre archive va être mise à jour pour la nouvelle version.
11. Cliquez sur **OK**.
12. Indiquez l'emplacement où vous voulez créer les nouvelles clés d'administrateur. Veillez à créer ces clés à un emplacement différent de celui des clés d'administrateur existantes. Si vous disposez de clés d'administrateur que vous avez déjà créées pour la version 5.0 sur un autre système, vous pouvez sélectionner l'option **Utilisation d'une paire de clés d'archive CSS existante** et indiquer l'emplacement des clés existantes.
13. Cliquez sur **Suivant**.

    Votre archive va être convertie et restaurée.
14. Quittez l'application lorsque la procédure est terminée.
15. Restaurez les paramètres de stratégie en procédant comme suit :
    a. A l'aide de l'Explorateur Windows, allez dans le répertoire d'installation du logiciel IBM Client Security (par défaut, le répertoire c:\program files\ibm\security).
    b. A l'aide du bouton gauche de la souris, faites glisser le dossier UVM_Policy du bureau vers le répertoire d'installation du logiciel IBM Client Security.

c. Cliquez sur **Oui** en réponse à tous les messages d'avertissement.

Vos données de sécurité ont maintenant été migrées vers la version 5.0 du logiciel Client Security.

Remarque : Si vous aviez auparavant modifié votre stratégie de sécurité dans la version 4.0x du logiciel Client Security, vous pouvez éventuellement ressoumettre vos paramètres de stratégie de sécurité en procédant comme suit :

1. Cliquez sur **Démarrer > Paramètres > Panneau de configuration > Sous-système de sécurité client IBM**.
2. Cliquez sur le bouton **Configuration du support d'application et des stratégies**.
3. Cliquez sur le bouton **Stratégie d'application**.
4. Cliquez sur le bouton **Edition de la stratégie**.

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

Si vous voulez effectuer une mise à niveau de la version 5.0 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 **Mise à jour de l'archive** pour vous assurer que les informations de sauvegarde soient mises à jour.

      Notez le répertoire d'archivage.
   c. Quittez l'utilitaire de configuration utilisateur du logiciel IBM Client Security.
2. Supprimez la version existante du logiciel Client Security en procédant comme suit :
   a. Localisez les clés publique et privée d'administrateur qui ont été créées lorsque vous avez configuré la version précédente du logiciel Client Security.
   b. Exécutez le fichier csec51.exe.
   c. Sélectionnez **Mise à niveau**.
   d. Redémarrez le système.

Désinstallation du logiciel Client Security

Veillez à désinstaller les divers utilitaires 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.

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 **Oui** pour désinstaller le logiciel.
8. Effectuez 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 normal de votre ordinateur.
9. Cliquez sur **OK** 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. Cependant, l'archive de clés n'est pas affectée lorsque le logiciel Client Security est désinstallé.

Chapitre 5. Identification des incidents

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

Fonctions d'administrateur

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

Définition d'un mot de passe administrateur (ThinkCentre)

Les paramètres de sécurité disponibles dans le programme Configuration/Setup Utility permettent aux administrateurs d'effectuer les opérations suivantes :

- Modifier le mot de passe matériel pour la puce de sécurité intégrée IBM
- Activer ou désactiver la puce de sécurité intégrée IBM
- Vider la puce de sécurité intégrée IBM

Important :

- Ne videz pas ou ne désactivez pas la puce de sécurité intégrée IBM lorsque la fonction de protection à la connexion UVM est activée. Sinon, le contenu du disque dur risque de devenir inutilisable et vous devrez reformater l'unité de disque dur et réinstaller tous les logiciels.

  Pour désactiver la fonction de protection UVM, ouvrez l'utilitaire d'administration, cliquez sur **Configuration du support d'application et des stratégies** et désélectionnez la case **Remplacement de la fenêtre de connexion standard de Windows par la fenêtre de connexion sécurisée UVM**. Vous devez redémarrer l'ordinateur pour que la fonction de protection UVM soit désactivée.
- Ne videz pas ou ne désactivez pas la puce de sécurité intégrée IBM si la fonction de protection UVM est activée. Sinon, vous serez éjecté du système.
- Lorsque la puce de sécurité intégrée IBM est vidée, toutes les clés de chiffrement et tous les certificats stockés sur la puce sont perdus.

Vos paramètres de sécurité étant accessibles via le programme Configuration/Setup Utility 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, procédez comme suit :

1. Arrêtez et redémarrez l'ordinateur.
2. Lorsque l'invite du programme Configuration/Setup Utility s'affiche, appuyez sur **F1**.

   Le menu principal du programme Configuration/Setup Utility 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, une invite s'affiche chaque fois que vous tentez d'accéder au programme Configuration/Setup Utility.

Important : Conservez votre mot de passe administrateur en lieu sûr. Si vous le perdez ou l'oubliez, vous ne pourrez pas accéder au programme Configuration/Setup Utility, 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 :

- Activer ou désactiver la puce de sécurité intégrée IBM
- Vider la puce de sécurité intégrée IBM

Important :

- Ne videz pas ou ne désactivez pas la puce de sécurité intégrée IBM lorsque la fonction de protection à la connexion UVM est activée. Sinon, vous serez éjecté du système.

  Pour désactiver la fonction de protection UVM, ouvrez l'utilitaire d'administration, cliquez sur **Configuration du support d'application et des stratégies** et désélectionnez la case **Remplacement de la fenêtre de connexion standard de Windows par la fenêtre de connexion sécurisée UVM**. Vous devez redémarrer l'ordinateur pour que la fonction de protection UVM soit désactivée.

  Lorsque la puce de sécurité intégrée IBM est vidée, toutes les clés de chiffrement et tous les certificats stockés sur la puce sont perdus.
- 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 la procédure suivante :

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

   Le menu principal de l'utilitaire de configuration du BIOS IBM 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.

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 IBM.

Important : Conservez votre mot de passe superviseur en lieu sûr. Si vous le perdez ou l'oubliez, vous ne pourrez pas accéder à l'utilitaire de configuration du

BIOS IBM, ni modifier ou supprimer le mot de passe. Pour plus de détails, consultez la documentation matérielle fournie avec l'ordinateur.

Protection du mot de passe matériel

Définissez un mot de passe pour la puce de sécurité afin d'activer la puce de sécurité intégrée IBM pour un client. Une fois que vous avez défini un mot de passe pour la puce de sécurité, l'accès à l'utilitaire d'administration est protégé par ce mot de passe. Vous devez protéger le mot de passe de la puce de sécurité pour empêcher les utilisateurs non autorisés de modifier des paramètres de l'utilitaire d'administration.

Vidage de la puce de sécurité intégrée IBM (ThinkCentre)

Si vous souhaitez effacer toutes les clés de chiffrement utilisateur de la puce de sécurité intégrée IBM et mettre à blanc le mot de passe matériel pour la puce, vous devez vider la puce. Lisez les informations de la section Important ci-dessous avant de vider la puce de sécurité intégrée IBM.

Important :

- Ne videz pas ou ne désactivez pas la puce de sécurité intégrée IBM si la fonction de protection UVM est activée. Sinon, vous serez éjecté du système.

  Pour désactiver la fonction de protection UVM, ouvrez l'utilitaire d'administration, cliquez sur **Configuration du support d'application et des stratégies** et désélectionnez la case **Remplacement de la fenêtre de connexion standard de Windows par la fenêtre de connexion sécurisée UVM**. Vous devez redémarrer l'ordinateur pour que la fonction de protection UVM soit désactivée.
- Lorsque la puce de sécurité intégrée IBM est vidée, toutes les clés de chiffrement et tous les certificats stockés sur la puce sont perdus.

Pour vider la puce de sécurité intégrée IBM, procédez comme suit :

1. Arrêtez et redémarrez l'ordinateur.
2. Lorsque l'invite du programme Configuration/Setup Utility s'affiche, appuyez sur F1.

   Le menu principal du programme Configuration/Setup Utility s'affiche.
3. Sélectionnez **Security**.
4. Sélectionnez **IBM TCPA Feature Setup**.
5. Sélectionnez **Clear IBM TCPA Security Feature**.
6. Cliquez sur **Yes**.
7. Appuyez sur Echap pour continuer.
8. Appuyez sur Echap pour sortir et sauvegarder les paramètres.

Vidage de la puce de sécurité intégrée IBM (ThinkPad)

Si vous souhaitez effacer toutes les clés de chiffrement utilisateur de la puce de sécurité intégrée IBM et mettre à blanc le mot de passe matériel pour la puce, vous devez vider la puce. Lisez les informations de la section Important ci-dessous avant de vider la puce de sécurité intégrée IBM.

Important :

- Ne videz pas ou ne désactivez pas la puce de sécurité intégrée IBM si la fonction de protection UVM est activée. Sinon, le contenu du disque dur risque de devenir inutilisable et vous devrez reformater l'unité de disque dur et réinstaller tous les logiciels.

Pour désactiver la fonction de protection UVM, ouvrez l'utilitaire d'administration, cliquez sur **Configuration du support d'application et des stratégies** et désélectionnez la case **Remplacement de la fenêtre de connexion standard de Windows par la fenêtre de connexion sécurisée UVM**. Vous devez redémarrer l'ordinateur pour que la fonction de protection UVM soit désactivée.

- Lorsque la puce de sécurité intégrée IBM est vidée, toutes les clés de chiffrement et tous les certificats stockés sur la puce sont perdus.

Pour vider la puce de sécurité intégrée IBM, procédez comme suit :

1. Arrêtez et redémarrez l'ordinateur.
2. Lorsque l'invite de l'utilitaire de configuration du BIOS IBM s'affiche, appuyez sur Fn.

   Remarque : Sur certains modèles de ThinkPad, vous pouvez avoir besoin d'appuyer sur la touche F1 lors de la mise sous tension pour accéder à l'utilitaire de configuration du BIOS IBM. Pour plus de détails, consultez le message d'aide de l'utilitaire de configuration du BIOS IBM.

   Le menu principal de l'utilitaire de configuration du BIOS IBM s'affiche.
3. Sélectionnez **Config**.
4. Sélectionnez **IBM Security Chip**.
5. Sélectionnez **Clear IBM Security Chip**.
6. Cliquez sur **Yes**.
7. Appuyez sur Entrée pour continuer.
8. Appuyez sur F10 pour sauvegarder et sortir.

Utilitaire d'administration

La section suivante contient des informations à conserver à l'esprit lors de l'utilisation de l'utilitaire d'administration.

Suppression d'utilisateurs

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

Suppression de l'accès à des objets sélectionnés à l'aide du contrôle Tivoli Access Manager

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

Limites connues

La présente section contient des informations sur les limites connues relatives au logiciel Client Security.

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

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

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

Utilisation du logiciel Client Security avec des applications Netscape

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

Les algorithmes ne s'affichent pas : Tous les algorithmes de hachage pris en charge par le module PKCS n° 11 de la puce de sécurité intégrée IBM ne sont pas sélectionnés si le module est affiché dans Netscape. Les algorithmes suivants sont pris en charge par le module PKCS n° 11 de la puce de sécurité intégrée IBM, mais ne sont pas identifiés comme tels lorsqu'ils sont affichés dans Netscape :

- SHA-1
- MD5

Certificat de la puce de sécurité intégrée IBM et algorithmes de chiffrement

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

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

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

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

Utilisation de la protection UVM pour un ID utilisateur Lotus Notes

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

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

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

Limites de l'utilitaire de configuration utilisateur

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

Windows XP Professionnel

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

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

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

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

Ces limites sont annulées lorsqu'un administrateur démarre l'utilitaire d'administration et en sort.

Windows XP Edition familiale

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

- Le logiciel Client Security est installé sur une partition au format NTFS.

- Le dossier Windows se trouve sur une partition au format NTFS.
- Le dossier d'archive se trouve sur une partition au format NTFS.

Messages d'erreur

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

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

Tableaux d'identification des incidents

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

Identification des incidents liés à l'installation

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

Incident	Solution possible
Un message d'erreur s'affiche lors de l'installation du logiciel	**Action**
Un message vous demandant si vous souhaitez retirer l'application sélectionnée et tous ses composants s'affiche lors de l'installation du logiciel.	Cliquez sur **OK** pour sortir de la fenêtre. Relancez le processus d'installation pour installer la nouvelle version du logiciel Client Security.
Un message signalant qu'une version précédente du logiciel Client Security est déjà installée s'affiche lors de l'installation.	Cliquez sur **OK** pour sortir de la fenêtre. Exécutez les opérations suivantes : 1. Désinstallez le logiciel. 2. Réinstallez le logiciel. **Remarque :** Si vous prévoyez d'utiliser le même mot de passe matériel pour sécuriser la puce de sécurité intégrée IBM, vous n'avez pas besoin de vider la puce et de redéfinir le mot de passe.
L'accès à l'installation est refusé, car le mot de passe matériel est inconnu	**Action**
Lorsque vous installez le logiciel sur un client IBM sur lequel une puce de sécurité intégrée IBM est activée, le mot de passe matériel pour la puce de sécurité intégrée IBM est inconnu.	Videz la puce pour continuer l'installation.

Incident	Solution possible
Le fichier setup.exe ne répond pas correctement (CSS version 4.0x)	**Action**
Si vous extrayez tous les fichiers de csec4_0.exe dans un répertoire commun, le fichier setup.exe ne fonctionnera pas correctement.	Exécutez le fichier smbus.exe pour installer le pilote de périphérique SMBus, puis le fichier csec4_0.exe pour installer le code du logiciel Client Security.

Identification des incidents liés à l'utilitaire d'administration

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

Incident	Solution possible
Stratégie de mot de passe composé UVM non imposée	**Action**
La case à cocher **ne doit pas contenir plus de 2 caractères identiques** ne fonctionne pas dans le logiciel IBM Client Security version 5.0	Il s'agit d'une limite connue pour le logiciel IBM Client Security version 5.0.
Le bouton Suivant n'est pas disponible une fois que vous avez entré et confirmé votre mot de passe composé UVM dans l'utilitaire d'administration	**Action**
Lorsque vous ajoutez des utilisateurs à UVM, le bouton **Suivant** risque de ne pas être disponible, une fois que vous avez entré et confirmé votre mot de passe composé UVM dans l'utilitaire d'administration.	Cliquez sur l'option **Information** dans la Barre des tâches Windows et continuez la procédure.
Un message d'erreur s'affiche lorsque vous tentez d'éditer la stratégie UVM locale	**Action**
Lorsque vous éditez la stratégie UVM locale, un message d'erreur peut s'afficher si aucun utilisateur n'est enregistré dans UVM.	Ajoutez un utilisateur à UVM avant de tenter d'éditer le fichier de stratégie.
Un message d'erreur s'affiche lorsque vous modifiez la clé publique d'administrateur	**Action**
Lorsque vous videz la puce de sécurité intégrée et que vous restaurez ensuite l'archive de clés, un message d'erreur peut s'afficher si vous modifiez la clé publique d'administrateur.	Ajoutez les utilisateurs à UVM et demandez de nouveaux certificats, le cas échéant.

Incident	Solution possible
Un message d'erreur s'affiche lorsque vous tentez de récupérer un mot de passe composé UVM	**Action**
Lorsque vous modifiez la clé publique d'administrateur et que vous tentez ensuite de récupérer un mot de passe composé UVM pour un utilisateur, un message d'erreur peut s'afficher.	Exécutez l'une des opérations suivantes : • Si le mot de passe composé UVM pour l'utilisateur n'est pas nécessaire, aucune action n'est requise. • Si le mot de passe composé UVM pour l'utilisateur est requis, vous devez ajouter l'utilisateur à UVM et demander de nouveaux certificats, le cas échéant.
Un message d'erreur s'affiche lorsque vous tentez de sauvegarder le fichier de stratégie UVM	**Action**
Lorsque vous tentez de sauvegarder un fichier de stratégie UVM (globalpolicy.gvm) en cliquant sur **Validation** ou **Sauvegarde**, un message d'erreur s'affiche.	Sortez du message d'erreur, éditez à nouveau le fichier de stratégie UVM pour apporter les modifications souhaitées, puis sauvegardez le fichier.
Un message d'erreur s'affiche lorsque vous tentez d'ouvrir l'éditeur de stratégie UVM	**Action**
Lorsque l'utilisateur en cours (connecté au système d'exploitation) n'a pas été ajouté à UVM, l'éditeur de stratégie UVM ne s'ouvre pas.	Ajoutez l'utilisateur à UVM et ouvrez l'éditeur de stratégie UVM.
Un message d'erreur s'affiche lorsque vous utilisez l'utilitaire d'administration	**Action**
Lorsque vous utilisez l'utilitaire d'administration, le message d'erreur suivant peut s'afficher : Une erreur d'E-S en mémoire tampon s'est produite lors de la tentative d'accès à la puce de sécurité Client Security. Cet incident peut être résolu par un réamorçage.	Sortez du message d'erreur et redémarrez l'ordinateur.
Un message de désactivation de la puce s'affiche lors de la modification du mot de passe de la puce de sécurité	**Action**
Lorsque vous tentez de modifier le mot de passe de la puce de sécurité et que vous appuyez sur Entrée ou Tab > Entrée après avoir tapé le mot de passe de confirmation, le bouton Désactivation de la puce est activé et un message confirmant la désactivation de la puce s'affiche.	Exécutez les opérations suivantes : 1. Sortez de la fenêtre de confirmation de la désactivation de la puce. 2. Pour modifier le mot de passe de la puce de sécurité, tapez le nouveau mot de passe, tapez le mot de passe de confirmation, puis cliquez sur **Modification**. N'appuyez ni sur Entrée, ni sur la touche de tabulation > Entrée après avoir tapé les informations dans la fenêtre de confirmation.

Identification des incidents relatifs à l'utilitaire de configuration utilisateur

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

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

Identification des incidents liés aux ThinkPad

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

Incident	**Solution possible**
Un message d'erreur s'affiche lorsque vous tentez d'exécuter une fonction d'administration Client Security	**Action**
Le message d'erreur suivant s'affiche après que vous avez tenté d'exécuter une fonction d'administration Client Security : ERROR 0197: Invalid Remote change requested. Press <F1> to Setup	Le mot de passe superviseur ThinkPad doit être désactivé pour exécuter certaines fonctions d'administration Client Security. Pour désactiver le mot de passe superviseur, procédez comme suit : 1. Appuyez sur F1 pour accéder à l'utilitaire de configuration du BIOS IBM. 2. Entrez le mot de passe superviseur en cours. 3. Entrez un nouveau mot de passe superviseur vierge, puis confirmez un mot de passe vierge. 4. Appuyez sur Entrée. 5. Appuyez sur F10 pour sauvegarder et sortir.
Un autre détecteur d'empreinte digitale compatible UVM ne fonctionne pas correctement	**Action**
L'ordinateur ThinkPad IBM ne prend pas en charge l'interchangeabilité de plusieurs détecteurs d'empreinte digitale compatibles UVM.	Ne changez pas de modèle de détecteur d'empreinte digitale. Utilisez le même modèle pour un travail à distance et un travail à partir d'une station d'accueil.

Identification des incidents liés aux applications Microsoft

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

Incident	Solution possible
L'écran de veille ne s'affiche que sur l'écran local	**Action**
Lors de l'utilisation de la fonction Bureau étendu de Windows, l'écran de veille du logiciel Client Security s'affiche uniquement sur l'écran local, même si l'accès à votre système et à son clavier est protégé.	Si des informations sensibles sont affichées, réduisez les fenêtres de votre Bureau étendu avant d'appeler l'écran de veille Client Security.
Les fichiers du lecteur Windows Media sont chiffrés plutôt que lus sous Windows XP	**Action**
Sous Windows XP, lorsque vous ouvrez un dossier et que vous cliquez sur **Lire tout**, le contenu du fichier est chiffré plutôt que lu par le lecteur Windows Media.	Pour permettre au lecteur Windows Media de lire les fichiers, exécutez la procédure suivante : 1. Démarrez le lecteur Windows Media. 2. Sélectionnez tous les fichiers dans le dossier approprié. 3. Faites glisser les fichiers sur la zone de sélection du lecteur Windows Media.
Client Security ne fonctionne pas correctement pour un utilisateur enregistré dans UVM	**Action**
L'utilisateur client enregistré a peut-être changé son nom d'utilisateur Windows. Dans ce cas, toutes les fonctions Client Security sont perdues.	Ré-enregistrez le nouveau nom d'utilisateur dans UVM et demandez de nouvelles autorisations d'accès.
Remarque : Sous Windows XP, les utilisateurs enregistrés dans UVM qui avaient modifié précédemment leur nom d'utilisateur Windows ne seront pas reconnus par UVM. Cette limite est valable même si le nom d'utilisateur Windows a été modifié avant l'installation du logiciel Client Security.	
Incidents lors de la lecture du courrier électronique chiffré à l'aide d'Outlook Express	**Action**
Le courrier électronique chiffré ne peut pas être déchiffré en raison des différences de chiffrement renforcé existant entre les navigateurs Web utilisés par l'expéditeur et le destinataire. **Remarque :** Pour utiliser des navigateurs Web 128 bits avec le logiciel Client Security, la puce de sécurité intégrée IBM doit prendre en charge le chiffrement 256 bits. Si la puce de sécurité intégrée IBM prend en charge le chiffrement 56 bits, vous devez utiliser un navigateur Web 40 bits. Le chiffrement renforcé fourni par le logiciel Client Security se trouve dans l'utilitaire d'administration.	Vérifiez les points suivants : 1. Le chiffrement renforcé pour le navigateur Web utilisé par l'expéditeur est compatible avec celui utilisé par le destinataire. 2. Le chiffrement renforcé pour le navigateur Web est compatible avec celui fourni par le microcode du logiciel Client Security.

Incident	Solution possible
Incidents lors de l'utilisation d'un certificat à partir d'une adresse à laquelle sont associés plusieurs certificats	**Action**
Outlook Express peut répertorier plusieurs certificats associés à une seule adresse électronique et certains de ces certificats peuvent ne plus être valables. Un certificat n'est plus valable si la clé privée qui lui est associée n'existe plus sur la puce de sécurité intégrée IBM de l'ordinateur de l'expéditeur sur lequel le certificat a été généré.	Demandez au destinataire de renvoyer son certificat numérique, puis sélectionnez ce certificat dans le carnet d'adresses d'Outlook Express.
Message d'échec lors de la tentative de signature numérique d'un message électronique	**Action**
Si l'auteur d'un message électronique tente de le signer numériquement alors qu'aucun certificat n'est encore associé à son compte de messagerie électronique, un message d'erreur s'affiche.	Utilisez les paramètres de sécurité d'Outlook Express pour indiquer un certificat à associer au compte de l'utilisateur. Pour plus de détails, consultez la documentation fournie pour Outlook Express.
Outlook Express (128 bits) chiffre uniquement les messages électroniques avec l'algorithme 3DES	**Action**
Lors de l'envoi de courrier électronique chiffré entre des clients utilisant Outlook Express avec la version 128 bits d'Internet Explorer 4.0 ou 5.0, seul l'algorithme 3DES peut être utilisé.	Pour utiliser des navigateurs 128 bits avec le logiciel Client Security, la puce de sécurité intégrée IBM doit prendre en charge le chiffrement 256 bits. Si la puce de sécurité intégrée IBM prend en charge le chiffrement 56 bits, vous devez utiliser un navigateur Web 40 bits. Le chiffrement renforcé fourni par le logiciel Client Security se trouve dans l'utilitaire d'administration. Consultez la documentation Microsoft pour obtenir des informations à jour sur les algorithmes de chiffrement utilisés avec Outlook Express.
Les clients Outlook Express renvoient des messages électroniques avec un algorithme différent	**Action**
Un message électronique chiffré avec l'algorithme RC2(40), RC2(64) ou RC2(128) est envoyé d'un client utilisant Netscape Messenger à un client utilisant Outlook Express (128 bits). Un message électronique renvoyé par le client Outlook Express est chiffré avec l'algorithme RC2(40).	Aucune action n'est requise. Une demande de chiffrement RC2(40), RC2(64) ou RC2(128) d'un client Netscape vers un client Outlook Express (128 bits) est toujours renvoyée au client Netscape avec l'algorithme RC2(40). Consultez la documentation Microsoft pour obtenir des informations à jour sur les algorithmes de chiffrement utilisés avec votre version d'Outlook Express.

Incident	Solution possible
Message d'erreur lors de l'utilisation d'un certificat dans Outlook Express après une défaillance de l'unité de disque dur	**Action**
Les certificats peuvent être restaurés à l'aide de la fonction de restauration des clés de l'utilitaire d'administration. Certains certificats, tels que les certificats gratuits fournis par VeriSign, risquent de ne pas être restaurés après une restauration des clés.	Après la restauration des clés, exécutez l'une des opérations suivantes : • Obtenez de nouveaux certificats. • Enregistrez à nouveau l'autorité de certification dans Outlook Express.
Outlook Express ne met pas à jour le chiffrement renforcé associé à un certificat	**Action**
Lorsqu'un expéditeur sélectionne le chiffrement renforcé dans Netscape et envoie un message électronique signé à un client en utilisant Outlook Express avec Internet Explorer 4.0 (128 bits), le chiffrement renforcé du courrier électronique renvoyé risque de ne pas correspondre.	Supprimez le certificat associé dans le carnet d'adresses d'Outlook Express. Ouvrez à nouveau le courrier électronique signé et ajoutez le certificat au carnet d'adresses d'Outlook Express.
Un message d'erreur de déchiffrement s'affiche dans Outlook Express	**Action**
Vous pouvez ouvrir un message dans Outlook Express en cliquant deux fois dessus. Dans certains cas, lorsque vous effectuez cette opération trop rapidement, un message d'erreur de déchiffrement s'affiche.	Fermez le message et ouvrez à nouveau le message électronique chiffré.
Un message d'erreur de déchiffrement peut également s'afficher dans le volet de prévisualisation lorsque vous sélectionnez un message chiffré.	Si un message d'erreur s'affiche dans le volet de prévisualisation, aucune action n'est requise.
Un message d'erreur s'affiche lorsque vous cliquez deux fois sur le bouton Envoyer dans des courriers électroniques chiffrés	**Action**
Lorsque vous utilisez Outlook Express, si vous cliquez deux fois sur le bouton d'envoi pour envoyer un message électronique chiffré, un message d'erreur s'affiche pour indiquer que le message n'a pas pu être envoyé.	Fermez le message d'erreur et cliquez sur le bouton **Envoyer**.
Un message d'erreur s'affiche lorsque vous demandez un certificat	**Action**
Lorsque vous utilisez Internet Explorer, vous risquez de recevoir un message d'erreur si vous demandez un certificat qui utilise le fournisseur de service cryptographique de la puce de sécurité intégrée IBM.	Redemandez le certificat numérique.

Identification des incidents relatifs aux applications Netscape

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

Incident	Solution possible
Incidents lors de la lecture du courrier électronique chiffré	**Action**
Le courrier électronique chiffré ne peut pas être déchiffré en raison des différences de chiffrement renforcé existant entre les navigateurs Web utilisés par l'expéditeur et le destinataire. **Remarque :** Pour utiliser des navigateurs 128 bits avec le logiciel Client Security, la puce de sécurité intégrée IBM doit prendre en charge le chiffrement 256 bits. Si la puce de sécurité intégrée IBM prend en charge le chiffrement 256 bits, vous devez utiliser un navigateur Web 40 bits. Le chiffrement renforcé fourni par le logiciel Client Security se trouve dans l'utilitaire d'administration.	Vérifiez les points suivants : 1. Le chiffrement renforcé pour le navigateur Web utilisé par l'expéditeur est compatible avec celui utilisé par le destinataire. 2. Le chiffrement renforcé pour le navigateur Web est compatible avec celui fourni par le microcode du logiciel Client Security.
Message d'échec lors de la tentative de signature numérique d'un message électronique	**Action**
Lorsque le certificat de la puce de sécurité intégrée IBM n'a pas été sélectionné dans Netscape Messenger et que l'auteur d'un message électronique tente de le signer avec le certificat, un message d'erreur s'affiche.	Utilisez les paramètres de sécurité de Netscape Messenger pour sélectionner le certificat. Lorsque Netscape Messenger est ouvert, cliquez sur l'icône de sécurité de la barre d'outils. La fenêtre relative aux informations de sécurité s'ouvre. Cliquez sur **Messenger** dans le panneau de gauche, puis sélectionnez le **certificat de la puce de sécurité intégrée IBM**. Pour plus de détails, consultez la documentation fournie par Netscape.
Un message électronique est renvoyé au client avec un algorithme différent	**Action**
Un message électronique chiffré avec l'algorithme RC2(40), RC2(64) ou RC2(128) est envoyé d'un client utilisant Netscape Messenger à un client utilisant Outlook Express (128 bits). Un message électronique renvoyé par le client Outlook Express est chiffré avec l'algorithme RC2(40).	Aucune action n'est requise. Une demande de chiffrement RC2(40), RC2(64) ou RC2(128) d'un client Netscape vers un client Outlook Express (128 bits) est toujours renvoyée au client Netscape avec l'algorithme RC2(40). Consultez la documentation Microsoft pour obtenir des informations à jour sur les algorithmes de chiffrement utilisés avec votre version d'Outlook Express.

Incident	Solution possible
Impossible d'utiliser un certificat numérique généré par la puce de sécurité intégrée IBM	**Action**
Le certificat numérique généré par la puce de sécurité intégrée IBM n'est pas disponible pour l'utilisation.	Vérifiez que le mot de passe composé UVM a été tapé correctement lors de l'ouverture de Netscape. Si le mot de passe composé UVM est incorrect, un message d'erreur signalant un échec d'authentification s'affiche. Si vous cliquez sur **OK**, Netscape s'ouvre, mais vous ne pouvez pas utiliser le certificat généré par la puce de sécurité intégrée IBM. Vous devez sortir de Netscape, puis l'ouvrir à nouveau et taper le mot de passe composé UVM correct.
De nouveaux certificats numériques provenant du même expéditeur ne sont pas remplacés dans Netscape	**Action**
Lorsqu'un courrier électronique signé numériquement est reçu plusieurs fois par le même expéditeur, le premier certificat numérique associé au courrier électronique n'est pas remplacé.	Si vous recevez plusieurs certificats de courrier électronique, un seul fait office de certificat par défaut. Utilisez les fonctions de sécurité de Netscape pour supprimer le premier certificat, puis ouvrez à nouveau le deuxième certificat ou demandez à l'expéditeur d'envoyer un autre courrier électronique signé.
Impossible d'exporter le certificat de la puce de sécurité intégrée IBM	**Action**
Le certificat de la puce de sécurité intégrée IBM ne peut pas être exporté dans Netscape. La fonction d'exportation de Netscape peut être utilisée pour effectuer des copies de sauvegarde des certificats.	Accédez à l'utilitaire d'administration ou à l'utilitaire de configuration utilisateur pour mettre à jour l'archive de clés. Lorsque vous mettez à jour l'archive de clés, des copies de tous les certificats associés à la puce de sécurité intégrée IBM sont créées.
Message d'erreur lors de la tentative d'utilisation d'un certificat restauré après une défaillance de l'unité de disque dur	**Action**
Les certificats peuvent être restaurés à l'aide de la fonction de restauration des clés de l'utilitaire d'administration. Certains certificats, tels que les certificats gratuits fournis par VeriSign, risquent de ne pas être restaurés après une restauration des clés.	Après la restauration des clés, obtenez un nouveau certificat.
L'agent Netscape s'ouvre et provoque l'échec de Netscape	**Action**
L'agent Netscape s'ouvre et provoque la fermeture de Netscape.	Mettez l'agent Netscape hors tension.

Incident	Solution possible
Un délai s'écoule lors de la tentative d'ouverture de Netscape	**Action**
Si vous ajoutez le module PKCS n°11 de la puce de sécurité intégrée IBM, puis que vous ouvrez Netscape, un petit délai s'écoule avant l'ouverture de Netscape.	Aucune action n'est requise. Ces informations sont fournies uniquement à titre d'information.

Identification des incidents relatifs à un certificat numérique

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

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

Identification des incidents relatifs à Tivoli Access Manager

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

Incident	Solution possible
Les paramètres de stratégie locaux ne correspondent pas à ceux du serveur	**Action**
Tivoli Access Manager autorise certaines configurations de bit qui ne sont pas prises en charge par UVM. Les exigences de stratégie locales peuvent donc remplacer les paramètres définis par un administrateur lors de la configuration du serveur Tivoli Access Manager.	Il s'agit d'une limite connue.

Incident	Solution possible
Les paramètres de configuration de Tivoli Access Manager ne sont pas accessibles	**Action**
Les paramètres de configuration de Tivoli Access Manager et de la mémoire cache locale ne sont pas accessibles sur la page Définition de stratégie de l'utilitaire d'administration.	Installez l'environnement d'exécution de Tivoli Access Manager. Si l'environnement d'exécution n'est pas installé sur le client IBM, les paramètres de Tivoli Access Manager sur la page Définition de stratégie ne seront pas disponibles.
Une commande utilisateur est valide à la fois pour l'utilisateur et le groupe	**Action**
Lors de la configuration du serveur Tivoli Access Manager, si vous définissez un utilisateur par rapport à un groupe, la commande utilisateur est valide à la fois pour l'utilisateur et le groupe si l'option **Traverse bit** est activée.	Aucune action n'est requise.

Identification des incidents relatifs à Lotus Notes

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

Incident	Solution possible
Une fois que la fonction de protection UVM pour Lotus Notes a été activée, Notes ne peut pas finir sa configuration	**Action**
Lotus Notes ne peut pas finir sa configuration une fois que la fonction de protection UVM a été activée à l'aide de l'utilitaire d'administration.	Il s'agit d'une limite connue. Lotus Notes doit être configuré et en cours d'exécution avant que le support Lotus Notes ne soit activé dans l'utilitaire d'administration.
Un message d'erreur s'affiche lorsque vous tentez de modifier le mot de passe Notes	**Action**
La modification du mot de passe Notes lors de l'utilisation du logiciel Client Security risque de provoquer l'affichage d'un message d'erreur.	Essayez de modifier à nouveau le mot de passe. Si l'opération n'aboutit pas, redémarrez le client.

Incident	Solution possible
Un message d'erreur s'affiche une fois que vous avez généré un mot de passe de façon aléatoire	**Action**
Un message d'erreur risque de s'afficher lorsque vous exécutez les opérations suivantes : • Utilisation de l'outil de configuration de Lotus Notes pour définir la protection UVM pour un ID Notes • Ouverture de Notes et utilisation de la fonction fournie par Notes pour modifier le mot de passe pour un fichier d'ID Notes • Fermeture immédiate de Notes après la modification du mot de passe	Cliquez sur **OK** pour faire disparaître le message d'erreur. Aucune autre action n'est requise. Contrairement aux indications du message d'erreur, le mot de passe a été modifié. Le nouveau mot de passe est généré de façon aléatoire par le logiciel Client Security. Le fichier d'ID Notes est désormais chiffré à l'aide du mot de passe généré de façon aléatoire et l'utilisateur n'a pas besoin d'un nouveau fichier d'ID utilisateur. Si l'utilisateur final modifie à nouveau le mot de passe, UVM génère un nouveau mot de passe de façon aléatoire pour l'ID Notes.

Identification des incidents relatifs au chiffrement

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

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

Identification des incidents relatifs aux périphériques compatibles UVM

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

Incident	Solution possible
Un périphérique compatible UVM cesse de fonctionner correctement	**Action**
Lorsque vous déconnectez un périphérique compatible UVM d'un port USB, puis que vous le reconnectez au port USB, le périphérique risque de ne pas fonctionner correctement.	Redémarrez l'ordinateur une fois que le périphérique a été reconnecté au port USB.

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

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

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

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

La présente annexe contient des informations relatives aux règles liées à différents mots de passe système.

Règles applicables aux mots de passe matériel

Les règles ci-après s'appliquent aux mots de passe matériel.

Longueur
Le mot de passe doit contenir exactement huit caractères.

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

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

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

Règles relatives aux mots de passe composés UVM

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 IBM Client Security.

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-après entre parenthèses.

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

  Par exemple, si le nombre de caractères alphanumériques autorisé défini est ″6″, le mot de passe `1234567xxx` n'est pas valide.
- Définir ou non un nombre minimal de chiffres autorisé (oui, 1)

  Par exemple, si la valeur définie est ″1″, le mot de passe `cestmonmotdepasse` n'est pas valide.
- Définir ou non le nombre minimal d'espaces autorisé (pas de minimum)

Par exemple, si la valeur définie est ″2″, le mot de passe `je ne suis pas là` n'est pas valide.

- Autoriser ou non plus de deux caractères identiques (non)

  Par exemple, si la valeur par défaut est définie, le mot de passe `aaabcdefghijk` n'est pas valide.
- Autoriser ou non le mot de passe composé à commencer par un chiffre (non)

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

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

  Par exemple, par défaut, le mot de passe `NomUtilisateur` n'est pas valide, `NomUtilisateur` étant 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, le mot de passe `monmotdepasse` n'est pas valide 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, le mot de passe `motdepass` n'est pas valide si votre précédent mot de passe était `passe` ou `motde`.

L'interface de stratégie de mot de passe composé UVM de l'utilitaire d'administration permet également aux administrateurs de sécurité de contrôler l'expiration des mots de passe composés. Cette interface permet à l'administrateur de choisir entre les règles d'expiration des mots de passe composés suivantes :

- Autoriser ou non le mot de passe composé à expirer après un certain nombre de jours (oui, 184)

  Par exemple, par défaut, le mot de passe composé expire au bout de 184 jours. Le nouveau mot de passe composé doit être conforme à la stratégie de mot de passe composé établie.
- Autoriser ou non le mot de passe composé à ne jamais expirer

  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 le mot de passe composé UVM dans une session, l'ordinateur ne se verrouille pas. Le nombre de tentatives infructueuses d'ouverture de session n'est pas limité.

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
La Défense 5
2, avenue Gambetta
92066 - Paris-La Défense Cedex
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.

Référence : 59P7637

(1P) P/N: 59P7637