

Solutions IBM Client Security



Logiciel Client Security version 5.1

Guide d'administration

Solutions IBM Client Security



Logiciel Client Security version 5.1

Guide d'administration

Première édition - avril 2003

Réf. US : 59P7665

LE PRESENT DOCUMENT EST LIVRE "EN L'ETAT". IBM DECLINE TOUTE RESPONSABILITE, EXPRESSE OU IMPLICITE, RELATIVE AUX INFORMATIONS QUI Y SONT CONTENUES, Y COMPRIS EN CE QUI CONCERNE LES GARANTIES DE QUALITE 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.

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

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

Vous pouvez également consulter les serveurs Internet suivants :

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

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

© Copyright IBM France 2003. Tous droits réservés.

© **Copyright International Business Machines Corporation 2003. All rights reserved.**

Table des matières

Avis aux lecteurs canadiens	vii
Avant-propos	ix
A qui s'adresse ce guide	x
Utilisation du guide	x
Références au manuel <i>Logiciel Client Security - Guide d'installation</i>	x
Références au manuel <i>Utilisation du logiciel Client Security avec Tivoli Access Manager</i>	x
Références au manuel <i>Logiciel Client Security - Guide d'utilisation</i>	xi
Informations complémentaires.	xi
Chapitre 1. Introduction au logiciel IBM Client Security	1
Applications et composants du logiciel Client Security	1
Fonctions PKI (Public Key Infrastructure).	2
Chapitre 2. Chiffrement de fichiers et de dossiers	5
Protection de fichiers à l'aide d'un clic droit	5
Protection de dossiers à l'aide d'un clic droit	5
Etat du chiffrement d'un dossier	5
Conseils relatifs à l'utilitaire de chiffrement de fichiers et de dossiers	7
Protection de l'identificateur d'unité	7
Suppression de fichiers et de dossiers protégés	7
Avant une mise à niveau à partir d'une version précédente de l'utilitaire IBM de chiffrement de fichiers et de dossiers	7
Avant la désinstallation de l'utilitaire IBM de chiffrement de fichiers et de dossiers	7
Limites de l'utilitaire IBM de chiffrement de fichiers et de dossiers	8
Limites lors du déplacement de fichiers et dossiers protégés	8
Limites lors de l'exécution d'applications	8
Limites relatives à la longueur du chemin d'accès	8
Incidents lors de la protection d'un dossier	8
Chapitre 3. Utilisation du logiciel Client Security	9
Exemple 1 - Un client Windows 2000 et un client Windows XP utilisant tous deux Outlook Express	9
Exemple 2 - Deux clients IBM Windows 2000 utilisant Lotus Notes et l'économiseur d'écran Client Security	10
Exemple 3 - Plusieurs clients IBM Windows 2000 gérés par Tivoli Access Manager et utilisant Netscape pour le courrier électronique	11
Chapitre 4. Autorisation d'utilisateurs	13
Authentification pour les utilisateurs client	13
Éléments d'authentification	13
Opérations préalables à l'autorisation d'utilisateurs.	14
Autorisation d'utilisateurs	14
Suppression d'utilisateurs	15
Création de nouveaux utilisateurs	16
Chapitre 5. Après l'autorisation d'utilisateurs dans le gestionnaire UVM	17
Protection UVM pour la connexion au système d'exploitation	17
Définition de la protection UVM pour la connexion au système d'exploitation	17
Configuration de la protection UVM pour la connexion au système d'exploitation	18

Enregistrement des empreintes digitales à l'aide du gestionnaire UVM	18
Utilisation de la protection UVM pour Lotus Notes	19
Activation et configuration de la protection UVM pour un ID utilisateur Lotus Notes	19
Utilisation de la protection UVM dans Lotus Notes	20
Désactivation de la protection UVM pour un ID utilisateur Lotus Notes	20
Configuration de la protection UVM pour un autre ID utilisateur Lotus Notes	21
Utilisation du logiciel Client Security avec les applications Netscape	22
Installation du module PKCS n° 11 de la puce de sécurité intégrée IBM pour les applications Netscape	22
Utilisation de la protection à la connexion PKCS n° 11 pour les applications Netscape	22
Sélection de la puce de sécurité intégrée IBM pour la génération d'un certificat numérique pour les applications Netscape	23
Mise à jour de l'archive de clés pour les applications Netscape	23
Utilisation du certificat numérique pour les applications Netscape	23
Chapitre 6. Gestion d'une stratégie UVM	25
Edition d'une stratégie UVM locale	26
Sélection d'objet	26
Éléments d'authentification	27
Utilisation de l'éditeur de stratégie UVM.	28
Edition et utilisation d'une stratégie UVM pour des clients éloignés.	29
Chapitre 7. Autres fonctions de l'utilitaire d'administration	31
Utilisation de la console d'administration	31
Enregistrement d'un client d'un réseau de délocalisation (roaming) d'accréditation	32
Modification de l'emplacement de l'archive de clés.	34
Modification de la paire de clés d'archive	34
Restauration de clés à partir d'une archive.	35
Réinitialisation du compteur d'échecs d'authentification	37
Modification des paramètres de Tivoli Access Manager	37
Accès au fichier de configuration de Tivoli Access Manager	37
Régénération de la mémoire cache locale	37
Récupération d'un mot de passe composé UVM	38
Modification du mot de passe de la puce de sécurité IBM	38
Affichage des informations relatives au logiciel Client Security	39
Désactivation de la puce de sécurité intégrée IBM	39
Activation de la puce de sécurité intégrée IBM et définition d'un mot de passe de puce de sécurité	40
Activation du support Entrust.	40
Chapitre 8. Instructions destinées à l'utilisateur client	43
Utilisation de la protection UVM pour la connexion au système	43
Déverrouillage du client.	43
Economiseur d'écran Client Security	44
Configuration de l'économiseur d'écran Client Security	44
Comportement de l'économiseur d'écran Client Security.	44
Utilitaire de configuration utilisateur	45
Fonctions de l'utilitaire de configuration utilisateur	45
Limites de l'utilitaire de configuration utilisateur sous Windows XP.	46
Utilisation de l'utilitaire de configuration utilisateur	46
Utilisation de messagerie électronique et de navigation Web sécurisées.	47
Utilisation du logiciel Client Security avec des applications Microsoft	47
Obtention d'un certificat numérique pour des applications Microsoft	47

Transfert de certificats à partir du fournisseur de service cryptographique Microsoft	48
Mise à jour de l'archive de clés pour des applications Microsoft	48
Utilisation du certificat numérique pour des applications Microsoft	48
Configuration des préférences audio UVM	49
Chapitre 9. Identification des incidents	51
Fonctions d'administrateur	51
Définition d'un mot de passe administrateur (ThinkCentre)	51
Définition d'un mot de passe superviseur (ThinkPad)	52
Protection du mot de passe matériel	53
Vidage de la puce de sécurité intégrée IBM (ThinkCentre)	53
Vidage de la puce de sécurité intégrée IBM (ThinkPad)	53
Utilitaire d'administration	54
Suppression d'utilisateurs	54
Suppression de l'accès à des objets sélectionnés à l'aide du contrôle Tivoli Access Manager	54
Limites connues	54
Utilisation du logiciel Client Security avec des systèmes d'exploitation Windows	55
Utilisation du logiciel Client Security avec des applications Netscape	55
Certificat de la puce de sécurité intégrée IBM et algorithmes de chiffrement	55
Utilisation de la protection UVM pour un ID utilisateur Lotus Notes	56
Limites de l'utilitaire de configuration utilisateur	56
Messages d'erreur	57
Tableaux d'identification des incidents	57
Identification des incidents liés à l'installation	57
Identification des incidents liés à l'utilitaire d'administration	58
Identification des incidents relatifs à l'utilitaire de configuration utilisateur	60
Identification des incidents liés aux ThinkPad	61
Identification des incidents liés aux applications Microsoft	62
Identification des incidents relatifs aux applications Netscape	65
Identification des incidents relatifs à un certificat numérique	67
Identification des incidents relatifs à Tivoli Access Manager	67
Identification des incidents relatifs à Lotus Notes	68
Identification des incidents relatifs au chiffrement	69
Identification des incidents relatifs aux périphériques compatibles UVM	70
Annexe A. Réglementation américaine relative à l'exportation du logiciel Client Security	71
Annexe B. Règles relatives aux mots de passe et aux mots de passe composés	73
Règles applicables aux mots de passe matériel	73
Règles relatives aux mots de passe composés UVM	73
Annexe C. Règles d'utilisation de la protection UVM à l'ouverture de session sur le système	77
Annexe D. Remarques	79
Remarques	79
Marques	80

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

Le présent guide contient des informations sur la configuration et l'utilisation des dispositifs de sécurité fournis avec le logiciel Client Security.

Ce guide est organisé comme suit :

Le "Chapitre 1, «**Introduction au logiciel IBM Client Security**»,» comporte une présentation des applications et des composants inclus dans le logiciel, ainsi qu'une description des dispositifs PKI.

Le "Chapitre 2, «Chiffrement de fichiers et de dossiers»,» contient des informations concernant l'utilisation du logiciel IBM Client Security pour la protection des fichiers et dossiers confidentiels.

Le "Chapitre 3, «Utilisation du logiciel Client Security»,» contient des exemples relatifs à l'utilisation des composants fournis par le logiciel Client Security pour définir les dispositifs de sécurité nécessaires aux utilisateurs clients IBM.

Le "Chapitre 4, «Autorisation d'utilisateurs»,» contient des informations concernant l'authentification des utilisateurs clients, y compris l'autorisation et la suppression d'utilisateurs dans le gestionnaire UVM.

Le "Chapitre 5, «Après l'autorisation d'utilisateurs dans le gestionnaire UVM»,» contient les instructions relatives à la configuration de la protection UVM pour la connexion au système d'exploitation, l'utilisation de la protection UVM pour Lotus Notes et l'utilisation du logiciel Client Security avec des applications Netscape.

Le "Chapitre 6, «Gestion d'une stratégie UVM»,» contient les instructions relatives à l'édition d'une stratégie UVM locale, l'utilisation d'une stratégie UVM pour un client éloigné et la modification du mot de passe pour un fichier de stratégie UVM.

Le "Chapitre 7, «Autres fonctions de l'utilitaire d'administration»,» contient les instructions relatives à l'utilisation de l'utilitaire d'administration pour modifier l'emplacement des archives de clés, restaurer des clés à partir d'une archive, restaurer un mot de passe composé UVM et activer ou désactiver la puce de sécurité intégrée IBM.

Le "Chapitre 8, «Instructions destinées à l'utilisateur client»,» contient les instructions relatives aux différentes tâches exécutées par l'utilisateur client dans le cadre de l'utilisation du logiciel Client Security. Vous y trouverez également les instructions relatives à l'utilisation de la fonction de protection à la connexion UVM, l'économiseur d'écran Client Security, la fonction de courrier sécurisée et l'utilitaire de configuration.

Le "Chapitre 9, «Identification des incidents»,» comporte des informations utiles concernant les limitations et problèmes connus que vous pourriez rencontrer lors de l'application des instructions de ce guide.

L'"Annexe A, «Réglementation américaine relative à l'exportation du logiciel Client Security»,» contient des informations concernant les lois d'exportation de ce logiciel en vigueur aux Etats-Unis.

L'Annexe B, «Règles relatives aux mots de passe et aux mots de passe composés», contient les critères de mot de passe qui peuvent être appliqués à un mot de passe composé UVM et les règles de mot de passe de la puce de sécurité.

L'Annexe C, «Règles d'utilisation de la protection UVM à l'ouverture de session sur le système», contient des informations concernant l'utilisation de la fonction de protection UVM pour la connexion au système d'exploitation.

L'Annexe D, «Remarques», contient des remarques et des informations concernant les marques.

A qui s'adresse ce guide

Le présent guide est destiné aux administrateurs de la sécurité chargés des opérations suivantes :

- Définition de l'authentification utilisateur pour le client IBM
- Définition et édition de la stratégie de sécurité UVM pour les clients IBM
- Utilisation de l'utilitaire d'administration pour la gestion du sous-système de sécurité (puce de sécurité intégrée IBM) et des paramètres associés pour les clients IBM

Ce guide s'adresse également aux administrateurs de Tivoli Access Manager qui vont utiliser IBM Tivoli Access Manager pour gérer les objets d'authentification fournis dans la stratégie UVM. Ces administrateurs doivent être capables de gérer les éléments et opérations suivantes :

- Espace objet de Tivoli Access Manager
- Processus d'authentification, d'autorisation et d'acquisition d'accréditation
- Environnement DCE IBM
- Protocole LDAP IBM SecureWay Directory

Utilisation du guide

Vous pouvez utiliser le présent guide pour définir l'authentification utilisateur et la stratégie de sécurité UVM pour les clients IBM. Ce guide est un complément aux manuels suivants : *Logiciel Client Security - Guide d'installation, Utilisation du logiciel Client Security avec Tivoli Access Manager* et *Logiciel Client Security - Guide d'utilisation*. Ce guide ainsi que toute la documentation relative à Client Security peuvent être téléchargés sur le site Web IBM à l'adresse : <http://www.pc.ibm.com/ww/security/secdownload.html>.

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

Ce document contient des références au manuel *Logiciel Client Security - Guide d'installation*. Vous devez avoir installé le Logiciel Client Security sur un client IBM pour pouvoir utiliser le présent guide. Les instructions relatives à l'installation du logiciel figurent dans le manuel *Logiciel Client Security - Guide d'installation*.

Références au manuel *Utilisation du logiciel Client Security avec Tivoli Access Manager*

Ce document contient des références au manuel *Utilisation du logiciel Client Security avec Tivoli Access Manager*. Les administrateurs de la sécurité qui envisagent d'utiliser Tivoli Access Manager pour gérer les objets d'authentification pour la stratégie UVM doivent lire le manuel *Utilisation du logiciel Client Security avec Tivoli Access Manager*.

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

Ce document contient des références au manuel *Logiciel Client Security - Guide d'utilisation*. Ce guide peut être utile aux administrateurs pour la définition et la gestion d'une stratégie UVM sur des clients IBM utilisant le logiciel Client Security. Une fois l'authentification utilisateur et la stratégie de sécurité UVM définies par l'administrateur, l'utilisateur client peut se reporter au manuel *Logiciel Client Security - Guide d'utilisation* pour apprendre à utiliser le logiciel Client Security.

Le guide d'utilisation contient des informations concernant l'exécution des tâches du logiciel Client Security, telles que l'utilisation de la fonction de protection UVM, la configuration de l'économiseur d'écran Client Security, la création d'un certificat numérique et l'utilisation de l'utilitaire de configuration utilisateur.

Informations complémentaires

Vous pouvez obtenir des informations complémentaires et des mises à jour du produit de sécurité, lorsqu'elles sont disponibles, 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 scanner 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. Chiffrement de fichiers et de dossiers

L'utilitaire de chiffrement des fichiers et dossiers IBM, qui peut être téléchargé à partir du site Web IBM Client Security, permet aux utilisateurs du logiciel Client Security de protéger les fichiers et les dossiers sensibles en cliquant sur le bouton droit de la souris. La méthode de protection des dossiers et fichiers choisie par l'utilitaire varie en fonction du mode de chiffrement initial des fichiers ou dossiers. Prenez connaissance des informations suivantes pour déterminer la technique de chiffrement à utiliser pour protéger vos données. Le logiciel IBM Client Security doit être installé *avant* l'utilitaire de chiffrement des fichiers et dossiers IBM.

L'utilitaire de vérification du disque peut s'exécuter lors du redémarrage du système d'exploitation après une opération de protection ou de déprotection des dossiers. Attendez la vérification du système avant d'utiliser votre ordinateur.

Protection de fichiers à l'aide d'un clic droit

Les fichiers peuvent être chiffrés et déchiffrés manuellement à l'aide du menu affiché à partir d'un clic droit de la souris. Lorsque des fichiers sont chiffrés à l'aide de cette méthode, l'opération de chiffrement ajoute l'extension `.enc` aux fichiers. Ces fichiers chiffrés peuvent ensuite être stockés en toute sécurité sur des serveurs éloignés. Ils resteront chiffrés et indisponibles pour une utilisation par des applications tant que la fonction de clic droit ne sera pas réutilisée pour les déchiffrer.

Protection de dossiers à l'aide d'un clic droit

Un utilisateur UVM peut sélectionner un dossier à protéger ou déprotéger via l'interface de clic droit. Tous les fichiers contenus dans le dossier ou ses sous-dossiers seront alors chiffrés. Lorsque des fichiers sont protégés de cette façon, aucune extension n'est ajoutée au nom de fichier. Lorsqu'une application tente d'accéder à un fichier situé dans un dossier chiffré, le fichier est déchiffré en mémoire, puis re-chiffré avant d'être sauvegardé sur le disque dur.

Toute opération Windows tentant d'accéder à un fichier situé dans un dossier protégé pourra accéder aux données sous forme déchiffrée. Cette fonction offre une facilité d'utilisation qui permet de ne pas avoir à déchiffrer un fichier avant son utilisation, puis à le re-chiffrer une fois qu'un programme a fini de l'utiliser.

Etat du chiffrement d'un dossier

Le logiciel IBM Client Security permet aux utilisateurs de protéger des fichiers et des dossiers sensibles en cliquant à l'aide du bouton droit de la souris. Le mode de protection d'un fichier et d'un dossier dépend de son chiffrement initial.

Un dossier peut prendre l'un des états suivants, chacun étant traité différemment par l'option de protection de dossier par clic droit :

- **Dossier non protégé**

Ni ce dossier, ni ses sous-dossiers ou ses parents n'ont été signalés comme protégés. L'utilisateur peut choisir de protéger ce dossier.

- **Dossier protégé**

Un dossier protégé peut prendre l'un des trois états suivants :

- **Protégé par l'utilisateur en cours**

L'utilisateur en cours a signalé ce dossier comme protégé. Tous les fichiers sont chiffrés, y compris ceux qui se trouvent dans tous les sous-dossiers. L'utilisateur peut choisir de déprotéger le dossier.

– **Sous-dossier d'un dossier protégé par l'utilisateur en cours**

L'utilisateur en cours a signalé l'un des parents de ce dossier comme protégé. Tous les fichiers sont chiffrés. L'utilisateur en cours ne dispose pas d'options de clic droit.

– **Protégé par un autre utilisateur**

Un autre utilisateur a signalé ce dossier comme protégé. Tous les fichiers sont chiffrés, y compris ceux qui se trouvent dans tous les sous-dossiers, et l'utilisateur en cours ne peut pas y accéder. L'utilisateur en cours ne dispose pas d'options de clic droit.

• **Parent d'un dossier protégé**

Un parent d'un dossier protégé peut prendre l'un des trois états suivants :

– **Il peut contenir un ou plusieurs sous-dossiers protégés par l'utilisateur en cours**

L'utilisateur en cours a signalé un ou plusieurs sous-dossiers comme protégés. Tous les fichiers situés dans les sous-dossiers protégés sont chiffrés. L'utilisateur peut choisir de protéger le dossier parent.

– **Il peut contenir un ou plusieurs sous-dossiers protégés par un ou plusieurs autres utilisateurs**

Un ou plusieurs autres utilisateurs ont signalé un ou plusieurs sous-dossiers comme protégés. Tous les fichiers situés dans les sous-dossiers protégés sont chiffrés et l'utilisateur en cours ne peut pas y accéder. L'utilisateur en cours ne dispose pas d'options de clic droit.

– **Il peut contenir des sous-dossiers protégés par l'utilisateur en cours et un ou plusieurs autres utilisateurs**

L'utilisateur en cours et un ou plusieurs autres utilisateurs ont signalé des sous-dossiers comme protégés. L'utilisateur en cours ne dispose pas d'options de clic droit.

• **Dossier critique**

Un dossier critique est un dossier qui est situé dans un chemin critique et ne peut donc pas être protégé. Il existe deux chemins critiques : le chemin Windows et le chemin Client Security.

Chaque état est traité différemment par l'option de protection de dossier par clic droit.

Conseils relatifs à l'utilitaire de chiffrement de fichiers et de dossiers

Les informations suivantes peuvent s'avérer utiles lors de l'exécution de certaines fonctions de chiffrement de fichiers et de dossiers.

Protection de l'identificateur d'unité

L'utilitaire IBM de chiffrement de fichiers et de dossiers permet de chiffrer des fichiers et des dossiers sur l'unité C uniquement. Il ne prend pas en charge le chiffrement sur une autre partition de disque dur ou unité physique.

Suppression de fichiers et de dossiers protégés

Pour vous assurer que des fichiers ou dossiers sensibles ne restent pas déprotégés dans la corbeille, vous devez utiliser la combinaison de touches Maj+Suppr pour supprimer les dossiers et fichiers protégés. La séquence de touches Maj+Suppr exécute une opération de suppression sans condition et ne tente pas de placer les fichiers supprimés dans la corbeille.

Avant une mise à niveau à partir d'une version précédente de l'utilitaire IBM de chiffrement de fichiers et de dossiers

Si vous prévoyez une mise à niveau à partir d'une version précédente de l'utilitaire IBM de chiffrement de fichiers et de dossiers (version 1.04 ou antérieure) et que vous avez protégé des dossiers sur d'autres unités que l'unité C, déprotégez ces dossiers avant d'installer la version 1.05 de l'utilitaire IBM de chiffrement de fichiers et de dossiers. Si vous devez reprotéger ces dossiers après l'installation de la version 1.05, déplacez ces dossiers sur l'unité C et protégez-les.

Avant la désinstallation de l'utilitaire IBM de chiffrement de fichiers et de dossiers

Avant de désinstaller l'utilitaire IBM de chiffrement de fichiers et de dossiers, servez-vous de cet utilitaire pour déprotéger des fichiers ou dossiers protégés.

Limites de l'utilitaire IBM de chiffrement de fichiers et de dossiers

L'utilitaire IBM de chiffrement de fichiers et de dossiers comporte les limites suivantes :

Limites lors du déplacement de fichiers et dossiers protégés

L'utilitaire IBM de chiffrement de fichiers et de dossiers ne prend pas en charge les opérations suivantes :

- Déplacement de fichiers et de dossiers dans des dossiers protégés
- Déplacement de fichiers ou de dossiers entre des dossiers protégés et non protégés

Si vous tentez d'exécuter l'une des ces opérations de déplacement non prises en charge, un message d'accès refusé sera affiché par le système d'exploitation. Ce message est normal. Il indique simplement que cette opération de déplacement n'est pas prise en charge. Pour éviter une opération de déplacement, vous pouvez :

1. Copier les fichiers ou dossiers protégés dans le nouvel emplacement.
2. Supprimer les fichiers ou dossiers d'origine à l'aide de la combinaison de touches Maj+Suppr.

Limites lors de l'exécution d'applications

L'utilitaire IBM de chiffrement de fichiers et de dossiers ne prend pas en charge l'exécution d'applications à partir d'un dossier protégé. Par exemple, si vous disposez d'un fichier exécutable appelé PROGRAM.EXE, vous ne pouvez pas exécuter cette application à partir d'un dossier protégé.

Limites relatives à la longueur du chemin d'accès

Lorsque vous tentez de protéger un dossier à l'aide de l'utilitaire IBM de chiffrement de fichiers et de dossiers ou que vous essayez de copier ou déplacer un fichier ou un dossier d'un dossier non protégé vers un dossier protégé, vous risquez de recevoir un message indiquant qu'un ou plusieurs chemins d'accès sont trop longs de la part du système d'exploitation. Ce message signifie que le chemin d'accès à un ou plusieurs fichiers ou dossiers dépasse le nombre maximal de caractère autorisé. Pour remédier à cet incident, réorganisez la structure du dossier pour la raccourcir ou réduisez le nombre de caractères de certains noms de fichiers ou de dossiers.

Incidents lors de la protection d'un dossier

Si vous tentez de protéger un dossier et que vous recevez un message indiquant que le dossier ne peut pas être protégé, car un ou plusieurs fichiers sont peut-être en cours d'exécution, vérifiez les points suivants :

- Assurez-vous qu'aucun des fichiers situés dans le dossier n'est en cours d'utilisation.
- Si Windows Explorer affiche un ou plusieurs sous-dossiers d'un dossier que vous tentez de protéger, assurez-vous que le dossier que vous essayez de protéger est mis en évidence et actif, et non l'un de ses sous-dossiers.

Chapitre 3. Utilisation du logiciel Client Security

Les administrateurs peuvent utiliser les multiples composants fournis par le logiciel Client Security pour définir les dispositifs de sécurité nécessaires aux utilisateurs clients IBM. Utilisez les exemples fournis ci-après pour planifier votre stratégie et votre configuration Client Security. En environnement Windows NT, par exemple, les utilisateurs peuvent définir une protection UVM pour la connexion système qui empêche la connexion d'utilisateurs non autorisés sur le client IBM.

Exemple 1 - Un client Windows 2000 et un client Windows XP utilisant tous deux Outlook Express

Dans cet exemple, un client IBM (client 1) dispose de Windows 2000 et d'Outlook Express, l'autre client (client 2) disposant de Windows XP et d'Outlook Express. Trois utilisateurs vont nécessiter une configuration d'authentification sous UVM sur le client 1 ; un utilisateur client va nécessiter une configuration d'authentification sous UVM sur le client 2. Tous les utilisateurs clients vont enregistrer leurs empreintes digitales afin qu'elles puissent servir pour l'authentification. Un détecteur d'empreintes digitales compatible UVM va être installé dans le cadre de cet exemple. Il est également établi que les deux clients nécessiteront une protection UVM pour la connexion Windows. L'administrateur a décidé que la stratégie UVM locale sera éditée et utilisée sur chaque client.

Pour configurer la sécurité client, procédez comme suit :

1. Installez le logiciel sur les clients 1 et 2. Pour plus de détails, consultez le manuel *Logiciel Client Security - Guide d'installation*.
2. Installez les détecteurs d'empreinte digitale compatibles UVM ainsi que les logiciels associés sur chaque client.

Pour plus d'informations sur les produits compatibles UVM, rendez-vous sur le site Web IBM <http://www.pc.ibm.com/ww/security/secdownload.html>.

3. Configurez l'authentification utilisateur dans UVM pour chaque client. Effectuez les opérations suivantes :
 - a. Ajoutez des utilisateurs dans le gestionnaire UVM et affectez-leur un mot de passe composé. Le client 1 disposant de trois utilisateurs, vous devez recommencer cette opération autant de fois que nécessaire.
 - b. Configurez la protection UVM pour la connexion Windows sur chaque client.
 - c. Enregistrez les empreintes digitales des utilisateurs. La stratégie indiquant que trois utilisateurs vont utiliser le client 1, chacun d'eux devra enregistrer ses empreintes digitales.

Remarque : Si vous définissez l'empreinte digitale comme procédure d'authentification requise dans le cadre de la stratégie UVM pour un client, il est nécessaire que chaque utilisateur enregistre son ou ses empreintes digitales.

4. Editez et sauvegardez une stratégie UVM locale sur chaque client nécessitant une authentification pour les opérations suivantes :
 - Connexion au système d'exploitation
 - Acquisition d'un certificat numérique
 - Utilisation d'une signature numérique pour les courriers électroniques
5. Redémarrez chaque client afin d'activer la protection UVM pour la connexion Windows.

6. Transmettez aux utilisateurs les mots de passe composés UVM que vous avez définis pour eux ainsi que les procédures d'authentification requises spécifiées dans la stratégie UVM pour le client IBM.

Les utilisateurs clients peuvent à présent exécuter les tâches suivantes :

- Utilisation de la protection UVM pour verrouiller et déverrouiller le système d'exploitation.
- Application d'un certificat numérique et sélection de la puce de sécurité intégrée comme fournisseur de service cryptographique associé au certificat.
- Utilisation du certificat numérique pour chiffrer les messages de courrier électronique créés dans Outlook Express.

Exemple 2 - Deux clients IBM Windows 2000 utilisant Lotus Notes et l'économiseur d'écran Client Security

Dans cet exemple, les deux clients IBM (client 1 et client 2) disposent de Windows 2000 et de Lotus Notes. Deux utilisateurs vont nécessiter une configuration d'authentification sous UVM sur le client 1 ; un utilisateur va nécessiter une configuration d'authentification sous UVM sur le client 2. Les deux clients vont nécessiter une protection UVM pour la connexion système, et ils vont utiliser l'économiseur d'écran Client Security et la protection UVM pour Lotus Notes. L'administrateur a décidé qu'une stratégie UVM pour les clients éloignés devra être éditée sur le client 1, puis copiée sur le client 2.

Pour configurer la sécurité client, procédez comme suit :

1. Installez le logiciel sur les clients 1 et 2. Etant donné qu'une stratégie UVM pour clients éloignés va être utilisée, vous devez utiliser la même clé publique d'administrateur lors de l'installation du logiciel sur les clients 1 et 2. Pour plus de détails sur cette opération, consultez le manuel *Logiciel Client Security - Guide d'installation*.
2. Configurez l'authentification utilisateur dans UVM pour chaque client. Effectuez ensuite les opérations suivantes :
 - a. Ajoutez des utilisateurs dans le gestionnaire UVM et affectez-leur un mot de passe composé. Le client 1 disposant de deux utilisateurs, vous devez recommencer cette opération autant de fois que nécessaire.
 - b. Définissez la protection UVM pour la connexion Windows sur chaque client.
3. Activez la protection UVM pour Lotus Notes sur les deux clients. Pour plus de détails, reportez-vous à la section «Utilisation de la protection UVM pour Lotus Notes» à la page 19.
4. Editez et sauvegardez une stratégie UVM pour les clients éloignés sur le client 1, puis copiez-la sur le client 2. La stratégie UVM peut nécessiter une authentification utilisateur pour la désactivation de l'économiseur d'écran, la connexion à Lotus Notes et la connexion au système d'exploitation. Pour plus de détails, reportez-vous à la section «Edition et utilisation d'une stratégie UVM pour des clients éloignés» à la page 29.
5. Redémarrez chaque client afin d'activer la protection UVM pour la connexion au système.
6. Fournissez aux utilisateurs clients les mots de passe composés UVM ainsi que la stratégie définie pour chaque client.

Les utilisateurs peuvent alors lire le manuel *Logiciel Client Security - Guide d'utilisation* pour exécuter les tâches suivantes :

- Activation de l'économiseur d'écran Client Security
- Utilisation de la protection UVM pour Windows 2000

Exemple 3 - Plusieurs clients IBM Windows 2000 gérés par Tivoli Access Manager et utilisant Netscape pour le courrier électronique

Le public concerné ici est un administrateur d'entreprise qui envisage d'utiliser Tivoli Access Manager pour gérer les objets d'authentification définis par une stratégie UVM. Dans cet exemple, plusieurs clients IBM disposent à la fois de Windows 2000 et Netscape. Le client NetSEAT, composant de Tivoli Access Manager, est installé sur tous les clients. Tous les clients utilisant un serveur LDAP disposent également d'un client LDAP. La stratégie UVM pour clients éloignés va être installée sur tous les clients. Elle permettra à Tivoli Access Manager de contrôler les objets d'authentification sélectionnés pour les clients.

Dans cet exemple, un utilisateur va nécessiter une configuration d'authentification sous UVM sur chaque client. Tous les utilisateurs vont enregistrer leurs empreintes digitales afin qu'elles puissent servir pour l'authentification. Un détecteur d'empreintes digitales compatibles UVM va être installé dans le cadre de cet exemple et tous les clients vont nécessiter une protection UVM pour la connexion Windows.

Pour configurer la sécurité client, procédez comme suit :

1. Installez le composant Client Security sur le serveur Tivoli Access Manager. Pour plus de détails, consultez le manuel *Utilisation du logiciel Client Security avec Tivoli Access Manager*.
2. Installez le logiciel Client Security sur tous les clients. Etant donné qu'une stratégie UVM pour clients éloignés va être utilisée, vous devez utiliser la même clé publique d'administrateur lors de l'installation du logiciel sur tous les clients. Pour plus de détails sur l'installation du logiciel, consultez le manuel *Logiciel Client Security - Guide d'installation*.
3. Installez les détecteurs d'empreinte digitale compatibles UVM ainsi que les logiciels associés sur chaque client. Pour plus d'informations sur les produits compatibles UVM disponibles, rendez-vous sur le site Web IBM <http://www.pc.ibm.com/ww/security/secdownload.html>.
4. Configurez l'authentification utilisateur dans UVM sur chaque client. Reportez-vous à la section «Suppression d'utilisateurs» à la page 15 pour plus de détails. Effectuez ensuite les opérations suivantes :
 - a. Ajoutez des utilisateurs dans le gestionnaire UVM et affectez-leur un mot de passe composé.
 - b. Configurez la protection UVM pour la connexion Windows sur chaque client.
 - c. Enregistrez les empreintes digitales pour chaque utilisateur client. Si une authentification par empreinte digitale est requise sur chaque client IBM, tous les utilisateurs de ce client doivent enregistrer leurs empreintes digitales.
5. Définissez les informations de configuration Tivoli Access Manager sur chaque client. Pour plus de détails, consultez le manuel *Utilisation du logiciel Client Security avec Tivoli Access Manager*.

6. Editez et sauvegardez une stratégie UVM pour clients éloignés sur l'un des clients, puis copiez-la sur les autres clients. La stratégie UVM doit être configurée de sorte que Tivoli Access Manager contrôle les objets d'authentification suivants :
 - Connexion au système d'exploitation
 - Acquisition d'un certificat numérique
 - Utilisation d'une signature numérique pour les courriers électroniques

Pour plus de détails, reportez-vous à la section «Edition et utilisation d'une stratégie UVM pour des clients éloignés» à la page 29.
7. Redémarrez chaque client afin d'activer la protection UVM pour la connexion Windows.
8. Installez le module PKCS n° 11 de la puce de sécurité intégrée IBM sur chaque client. Ce module offre un support de chiffrement sur les clients qui utilisent Netscape pour l'envoi et la réception de courriers électroniques, et la puce de sécurité intégrée IBM pour l'acquisition de certificats numériques. Pour plus d'informations, consultez le manuel *Logiciel Client Security - Guide d'installation*.
9. Utilisez Tivoli Access Manager pour contrôler les objets des solutions IBM Client Security qui figurent sur la console de gestion de Tivoli Access Manager.
10. Indiquez aux utilisateurs clients les mots de passe composés UVM ainsi que la stratégie qui ont été définis pour chaque client.
11. Conseillez aux utilisateurs de lire le manuel *Logiciel Client Security - Guide d'utilisation* pour exécuter les tâches suivantes :
 - Utilisation de la protection UVM pour verrouiller et déverrouiller le système d'exploitation
 - Utilisation de l'utilitaire de configuration utilisateur
 - Application d'un certificat numérique utilisant la puce de sécurité intégrée comme fournisseur de service cryptographique associé au certificat
 - Utilisation du certificat numérique pour chiffrer les messages de courrier électronique créés dans Netscape

Chapitre 4. Autorisation d'utilisateurs

Les informations qui suivent vous seront utiles pour autoriser des utilisateurs Windows à utiliser le gestionnaire de vérification d'utilisateur (UVM).

Authentification pour les utilisateurs client

L'authentification des utilisateurs finals au niveau du client constitue l'un des aspects importants de la sécurité informatique. Le logiciel Client Security fournit l'interface nécessaire à la gestion de la stratégie de sécurité d'un client IBM. Cette interface fait partie du logiciel d'authentification, UVM (gestionnaire de vérification d'utilisateur), qui constitue le composant principal du logiciel Client Security.

Il existe deux façons de gérer la stratégie de sécurité UVM pour un client IBM :

- Au niveau local, à l'aide d'un éditeur de stratégie résidant sur le client IBM
- Au sein d'une entreprise, à l'aide de Tivoli Access Manager

Des clés de chiffrement sont générées dès l'ajout du premier utilisateur.

Éléments d'authentification

Des éléments d'authentification (tels que les mots de passe composés UVM ou les empreintes digitales des utilisateurs) permettent d'autoriser des utilisateurs au niveau du client IBM. Lorsque vous autorisez un utilisateur Windows à utiliser le gestionnaire UVM, vous affectez un mot de passe composé pour l'utilisateur client. Le mot de passe composé UVM, qui peut comporter jusqu'à 256 caractères, représente l'élément d'authentification principal pour le gestionnaire UVM. Lorsque vous affectez un mot de passe composé UVM, des clés de chiffrement sont créées pour l'utilisateur client et stockées dans un seul fichier géré par la puce de sécurité intégrée IBM. Si le client IBM utilise une unité compatible UVM pour l'authentification, l'élément d'authentification (par exemple, les empreintes digitales de l'utilisateur) doit aussi être préalablement enregistré dans le gestionnaire UVM.

Lors de la configuration de l'authentification utilisateur, vous pouvez sélectionner les dispositifs de sécurité suivants qui sont fournis par le logiciel Client Security :

- **Protection UVM pour la connexion au système d'exploitation.** La protection UVM garantit que seuls les utilisateurs reconnus par le gestionnaire UVM peuvent accéder à l'ordinateur. Avant d'activer la protection UVM pour la connexion au système, reportez-vous à la section Configuration de la protection UVM pour la connexion au système d'exploitation pour connaître les informations importantes.
- **Economiseur d'écran Client Security.** Une fois ajouté, l'utilisateur client peut configurer l'économiseur d'écran Client Security. Pour cela, il doit utiliser l'option Affichage du système d'exploitation.

Opérations préalables à l'autorisation d'utilisateurs

Important : N'autorisez que des comptes utilisateur qui pourront être utilisés pour la connexion au système d'exploitation. Si vous autorisez un compte utilisateur qui *ne peut pas* être utilisé pour la connexion au système d'exploitation, **tous** les utilisateurs seront verrouillés sur le système lors de l'activation de la protection UVM.

Lors de l'autorisation d'un utilisateur client, l'utilitaire d'administration vous propose d'effectuer votre choix dans une liste de noms d'utilisateur. Ces noms correspondent à des comptes utilisateur ajoutés dans le cadre de l'utilisation du système d'exploitation. Avant d'ajouter des utilisateurs clients dans UVM, utilisez les applications du système d'exploitation pour créer des comptes utilisateur et des profils pour ces utilisateurs. Le logiciel Client Security est compatible avec les dispositifs de sécurité fournis par le système d'exploitation.

Windows XP et Windows 2000.

Utilisez l'application Utilisateurs et Mots de passe pour créer de nouveaux comptes utilisateur et gérer des comptes ou des groupes existants. Pour plus d'informations, reportez-vous à la documentation du système d'exploitation.

Sous Windows XP, la zone Sélection des utilisateurs Windows à autoriser n'est pas actualisée lorsque vous cliquez sur le bouton **Création d'un nouvel utilisateur Windows**. Vous devez quitter et relancer l'utilitaire d'administration afin de régénérer les informations de cette zone.

Remarques :

1. Lorsque vous créez de nouveaux utilisateurs à l'aide d'applications du système d'exploitation, le mot de passe du domaine doit être identique pour chaque nouvel utilisateur.
2. N'autorisez pas un utilisateur dont l'un des noms utilisateur Windows a été modifié. En effet, UVM pointera sur l'ancien nom utilisateur alors que Windows reconnaîtra le nouveau.
3. Lorsqu'un compte utilisateur autorisé est supprimé de Windows, l'interface de protection à la connexion UVM continue à afficher le compte comme un compte pouvant être utilisé pour la connexion à Windows, alors que cela est incorrect. Ce compte *ne peut pas* être utilisé pour la connexion à Windows.
4. Une fois un utilisateur autorisé, ne modifiez pas son nom utilisateur Windows. Sinon, vous devrez re-autoriser un nouveau nom d'utilisateur dans UVM et demander de nouvelles accréditations.

Autorisation d'utilisateurs

Les utilisateurs doivent se connecter avec des droits d'administrateur pour pouvoir se servir de l'utilitaire d'administration.

Pour autoriser des utilisateurs dans le gestionnaire UVM, procédez comme suit :

1. A partir du bureau Windows du client IBM, cliquez sur **Démarrer > Paramètres > Panneau de configuration > Sous-système de sécurité client IBM**.
Le message Saisie du mot de passe administrateur s'affiche.
2. Entrez le mot de passe administrateur et cliquez sur **OK**.
La fenêtre principale Sous-système de sécurité IBM - Utilitaire d'administration s'affiche.

3. Dans la zone Sélection des utilisateurs Windows à autoriser, sélectionnez un nom d'utilisateur.

Remarque : Les noms d'utilisateur de la liste sont définis par les comptes utilisateur créés sur le système d'exploitation ou sur le réseau.

4. Cliquez sur **Autorisation**.

L'écran Configuration de l'authentification utilisateur s'affiche.

5. Entrez et confirmez un mot de passe composé UVM initial pour le nouvel utilisateur autorisé et cliquez sur **Suivant**.

Si le mot de passe composé ne respecte pas les conditions requises définies dans la stratégie de sécurité, un écran s'affiche afin de vous indiquer que le mot de passe composé entré est incorrect. Dans ce cas, cliquez sur **OK** puis sur **Affichage des conditions requises pour le mot de passe composé** afin d'afficher les paramètres requis pour un mot de passe composé admis.

Lorsque le mot de passe composé est accepté, un message s'affiche afin d'indiquer que l'opération a abouti.

6. Cliquez sur **OK** pour continuer.

L'écran Mot de passe de connexion Windows s'affiche. Si la fonction de connexion UVM sécurisée est activée, le mot de passe Windows en cours de l'utilisateur doit être enregistré afin que l'utilisateur puisse se connecter au système. Cet écran permet à l'administrateur d'effectuer l'une des opérations suivantes :

- **Enregistrement immédiat du mot de passe Windows en cours.** Pour enregistrer immédiatement le mot de passe Windows en cours de l'utilisateur, entrez et confirmez le mot de passe dans les zones prévues à cet effet et cliquez sur **Suivant**.

Remarque : Le mot de passe entré doit correspondre au mot de passe Windows en cours de l'utilisateur. Ce paramètre n'a aucun effet sur le mot de passe enregistré sur le système d'exploitation.

- **Le mot de passe Windows de l'utilisateur sera enregistré ultérieurement à l'aide de l'utilitaire de configuration utilisateur.** Pour que l'utilisateur puisse enregistrer son mot de passe Windows ultérieurement à l'aide de l'utilitaire de configuration utilisateur, sélectionnez le bouton d'option approprié et cliquez sur **Suivant**.

Un message s'affiche afin d'indiquer que l'opération est terminée.

7. Cliquez sur **Terminer**.

Suppression d'utilisateurs

Les utilisateurs doivent se connecter avec des droits d'administrateur pour pouvoir se servir de l'utilitaire d'administration.

Pour annuler l'autorisation d'utilisateurs dans le gestionnaire UVM, procédez comme suit :

1. A partir du bureau Windows du client IBM, cliquez sur **Démarrer > Paramètres > Panneau de configuration > Sous-système de sécurité client IBM**.

Le message Saisie du mot de passe administrateur s'affiche.

2. Entrez le mot de passe administrateur et cliquez sur **OK**.

La fenêtre principale Sous-système de sécurité IBM - Utilitaire d'administration s'affiche.

3. Dans la zone Utilisateurs Windows autorisés à utiliser UVM, sélectionnez un nom d'utilisateur.
4. Cliquez sur **Suppression utilisateur**.
Un message s'affiche afin de vous prévenir que les informations de sécurité de l'utilisateur sélectionné, y compris l'ensemble des clés, certificats, empreintes digitales et mots de passe enregistrés pour cet utilisateur, vont être perdus.
5. Cliquez sur **Oui** pour continuer.
Un message vous invite à indiquer si vous voulez supprimer les informations archivées de l'utilisateur. Si vous supprimez ces informations, l'utilisateur ne pourra plus restaurer aucun des paramètres préalablement sauvegardés sur un système.
6. Cliquez sur **Oui** pour exécuter l'opération.

Création de nouveaux utilisateurs

Les utilisateurs doivent se connecter avec des droits d'administrateur pour pouvoir se servir de l'utilitaire d'administration.

Pour créer de nouveaux utilisateurs, procédez comme suit :

1. A partir du bureau Windows du client IBM, cliquez sur **Démarrer > Paramètres > Panneau de configuration > Sous-système de sécurité client IBM**.
Le message Saisie du mot de passe administrateur s'affiche.
2. Entrez le mot de passe administrateur et cliquez sur **OK**.
La fenêtre principale Sous-système de sécurité IBM - Utilitaire d'administration s'affiche.
3. Dans la zone Sélection des utilisateurs Windows à autoriser, cliquez sur **Création d'un nouvel utilisateur Windows**.
L'écran Nouveau compte utilisateur s'affiche.
4. Cliquez sur **Création d'un nouveau compte**.
5. Entrez un nom pour le nouveau compte utilisateur dans la zone prévue à cet effet ; cliquez ensuite sur **Suivant**.
6. Sélectionnez un type de compte en cliquant sur le bouton d'option approprié.
7. Cliquez sur **Créer un compte**.
8. Retournez dans l'utilitaire d'administration du Sous-système de sécurité client IBM.
Le nouveau compte utilisateur est affiché dans la zone Sélection des utilisateurs Windows à autoriser.

Chapitre 5. Après l'autorisation d'utilisateurs dans le gestionnaire UVM

Une fois que des utilisateurs ont été autorisés dans UVM, des fonctions supplémentaires de Client Security peuvent être utilisées, parmi lesquelles :

- **Configuration de la protection UVM pour la connexion au système d'exploitation.** Reportez-vous à la section «Définition de la protection UVM pour la connexion au système d'exploitation» pour plus de détails.
- **Archivage des clés de chiffrement utilisateur.** Reportez-vous à la section «Modification de l'emplacement de l'archive de clés» à la page 34 pour plus de détails.
- **Configuration de l'économiseur d'écran Client Security.** Reportez-vous au Chapitre 8, «Instructions destinées à l'utilisateur client», à la page 43 pour plus de détails.
- **Enregistrement des empreintes digitales à l'aide du gestionnaire UVM.** Reportez-vous à la section «Enregistrement des empreintes digitales à l'aide du gestionnaire UVM» à la page 18 pour plus de détails.

Si un détecteur d'empreintes digitales compatible UVM est installé avant l'ajout d'utilisateurs dans UVM, il est possible de procéder à ce stade à l'enregistrement des empreintes digitales.

Protection UVM pour la connexion au système d'exploitation

La fonction de protection UVM vient renforcer le dispositif de sécurité par mot de passe fourni avec votre système d'exploitation. L'interface d'ouverture de session UVM remplace l'ouverture de session du système d'exploitation de sorte que la fenêtre d'ouverture de session UVM s'ouvre à chaque essai d'ouverture de session de l'utilisateur sur le système.

Définition de la protection UVM pour la connexion au système d'exploitation

Lisez les informations qui suivent avant de définir et d'utiliser la protection UVM pour la connexion au système :

- Si la stratégie UVM indique qu'une authentification par empreinte digitale est requise pour la connexion système et qu'aucune empreinte digitale n'est enregistrée pour l'utilisateur, il est nécessaire que ce dernier enregistre ses empreintes pour pouvoir se connecter.

Par ailleurs, si le mot de passe Windows de l'utilisateur n'est pas enregistré (ou est enregistré de façon incorrecte) dans UVM, il doit être indiqué correctement par l'utilisateur pour que la connexion soit possible.

- N'effacez pas la puce de sécurité intégrée IBM tant que la protection UVM est activée. Ce faisant, vous verrouillerez complètement le système. Pour plus de détails, consultez les «Conseils pour l'administrateur» au Chapitre 9, «Identification des incidents», à la page 51.
- Si vous désélectionnez la case **Remplacement de la fenêtre de connexion standard de Windows par la fenêtre de connexion sécurisée UVM** dans l'utilitaire d'administration, le système restaure le processus de connexion Windows sans recours à la protection de connexion UVM.
- Si vous remplacez la fenêtre de connexion Windows standard par la fenêtre de connexion sécurisée du gestionnaire UVM et activez la fonction Cisco LEAP, vous devez réinstaller Cisco Aironet Client Utility (ACU).

Configuration de la protection UVM pour la connexion au système d'exploitation

Pour configurer la protection UVM de connexion à votre système d'exploitation, procédez comme suit :

1. A partir du bureau Windows du client IBM, cliquez sur **Démarrer > Paramètres > Panneau de configuration > Sous-système de sécurité client IBM**.
La fenêtre principale de l'utilitaire d'administration s'affiche.
2. Cliquez sur **Configuration du support d'application et des stratégies**.
L'écran Configuration des applications UVM et des stratégies s'affiche.
3. Sélectionnez l'option **Remplacement de la fenêtre de connexion standard de Windows par la fenêtre de connexion sécurisée UVM**.
4. Cliquez sur **OK**.
5. Redémarrez l'ordinateur.

Lors du redémarrage, vous êtes invité à vous connecter. Pour plus d'informations sur la protection UVM, reportez-vous à la section «Protection UVM pour la connexion au système d'exploitation» à la page 17.

Enregistrement des empreintes digitales à l'aide du gestionnaire UVM

Lorsqu'une stratégie UVM indique qu'une authentification par empreinte digitale est requise, il est nécessaire que chaque utilisateur enregistre ses empreintes dans le gestionnaire UVM.

Remarque : Windows XP ne prend pas en charge les détecteurs d'empreinte digitale de type Digital Persona U.are.U Pro.

Pour enregistrer les empreintes digitales d'un utilisateur dans UVM, procédez comme suit dans l'utilitaire d'administration :

1. Dans la zone Utilisateurs Windows autorisés à utiliser UVM, sélectionnez un nom d'utilisateur.
2. Cliquez sur **Edition utilisateur**.
La fenêtre Modification de la configuration de clé de Client Security - Edition des attributs utilisateur UVM s'affiche.
3. Sélectionnez l'option **Enregistrement avec une unité compatible UVM** et cliquez sur **Suivant**.
La fenêtre Modification de la configuration de clé de Client Security - Unités UVM activées s'affiche.
4. Cliquez sur **Enregistrement des empreintes digitales de l'utilisateur**.
5. Dans la zone Sélection d'une main, cliquez sur **Gauche** ou **Droite**.
6. Dans la zone Sélection d'un doigt, sélectionnez le doigt dont vous allez scanner l'empreinte, puis cliquez sur **Début de l'enregistrement**.
7. Placez votre doigt sur le détecteur d'empreinte digitale compatible UVM et suivez les instructions affichées à l'écran.
Suivant votre modèle de scanner, vous devrez peut-être scanner chaque empreinte quatre fois. Cliquez sur **Annulation doigt** pour annuler le scannage d'un doigt.
8. Sélectionnez un autre doigt à enregistrer ou cliquez sur **Sortie**.

Utilisation de la protection UVM pour Lotus Notes

UVM permet d'améliorer la protection des utilisateurs de Lotus Notes.

Activation et configuration de la protection UVM pour un ID utilisateur Lotus Notes

Avant de pouvoir activer la protection UVM pour Lotus Notes, ce dernier doit être installé sur le client IBM, un ID utilisateur et un mot de passe Lotus Notes doivent être définis pour l'utilisateur et celui-ci doit disposer de droits suffisants pour utiliser le gestionnaire UVM.

Pour configurer la protection UVM de connexion à Lotus Notes, procédez comme suit :

1. A partir du bureau Windows du client IBM, cliquez sur **Démarrer > Paramètres > Panneau de configuration > Sous-système de sécurité client IBM**.
La fenêtre principale de l'utilitaire d'administration s'affiche.
2. Cliquez sur **Configuration du support d'application et des stratégies**.
L'écran Configuration des applications UVM et des stratégies s'affiche.
3. Sélectionnez l'option **Activation du support Lotus Notes**.
La protection UVM pour l'ID utilisateur Lotus Notes est à présent activée. Si nécessaire, suivez les étapes facultatives ci-après pour configurer la stratégie de connexion Lotus Notes.
4. Cliquez sur **Stratégie d'application**.
L'écran Modification de la configuration de stratégie de Client Security s'affiche.
5. Cliquez sur **Edition de la stratégie**.
6. Entrez le mot de passe administrateur et cliquez sur **OK**. L'écran Stratégie UVM IBM : Connexion Lotus Notes s'affiche.
7. Cliquez sur l'onglet Sélection d'objet, puis sélectionnez Connexion Lotus Notes dans le menu déroulant Action.
8. Cliquez sur l'onglet Eléments d'authentification, puis sélectionnez les éléments d'authentification requis pour la connexion Lotus Notes.
9. Cliquez sur **Validation** pour sauvegarder vos choix.
L'écran Clé privée d'administrateur obligatoire s'affiche.
10. Indiquez l'emplacement de la clé privée. Pour cela, entrez directement le chemin d'accès dans la zone prévue à cet effet ou cliquez sur **Parcourir** et sélectionnez le dossier approprié.
11. Cliquez sur **OK**.
L'écran Gestionnaire de vérification d'utilisateur IBM : Récapitulatif de stratégie affiche un récapitulatif des objets contrôlés par la stratégie client locale.
12. Lancez Lotus Notes.
L'enregistrement du mot de passe UVM est terminé une fois Lotus Notes démarré.

Utilisation de la protection UVM dans Lotus Notes

Avant de commencer à utiliser la protection UVM pour Lotus Notes, vous devez suivre la procédure décrite à la section «Configuration de la protection UVM dans Lotus Notes».

Configuration de la protection UVM dans Lotus Notes

Pour configurer la protection UVM dans Lotus Notes, procédez comme suit :

1. Connectez-vous à Lotus Notes.
La fenêtre Gestionnaire de vérification d'utilisateur IBM s'affiche.
2. Entrez et vérifiez votre mot de passe Lotus Notes dans les zones prévues à cet effet.
Votre mot de passe Lotus Notes est à présent enregistré dans UVM.

Re-définition de votre mot de passe Lotus Notes

Pour redéfinir votre mot de passe Lotus Notes, procédez comme suit :

1. Connectez-vous à Lotus Notes.
2. A partir de la barre de menus de Lotus Notes, cliquez sur **Fichier > Outils > ID utilisateur**.
La fenêtre Gestionnaire de vérification d'utilisateur IBM s'affiche.
3. Entrez votre mot de passe composé UVM et cliquez sur **OK**.
La fenêtre ID utilisateur s'affiche.
4. Cliquez sur **Définition de mot de passe**.
La fenêtre Gestionnaire de vérification d'utilisateur IBM s'affiche.
5. Sélectionnez le bouton **Création de votre propre mot de passe**.
6. Entrez et vérifiez votre mot de passe Lotus Notes dans les zones prévues à cet effet, puis cliquez sur **OK**.

Remarque : Si vous essayez de changer votre mot de passe par une valeur déjà utilisée auparavant, Lotus Notes rejette la modification mais il n'en informe pas le logiciel Client Security. Par conséquent, le nouveau mot de passe rejeté est stocké dans UVM.

Si vous recevez un message indiquant que le mot de passe a déjà été utilisé par le passé, vous devez quitter Lotus Notes, lancer l'utilitaire de configuration utilisateur, puis restaurer la valeur initiale du mot de passe Lotus Notes.

Si cette erreur se produit alors que votre mot de passe Lotus Notes a été généré de façon aléatoire, vous n'avez aucun moyen de savoir quel était ce mot de passe et vous ne pouvez donc pas le restaurer manuellement. Vous devez demander un nouveau fichier d'ID à votre administrateur ou restaurer une version préalablement sauvegardée de ce fichier.

Désactivation de la protection UVM pour un ID utilisateur Lotus Notes

Si vous souhaitez désactiver la protection UVM pour un ID utilisateur Lotus Notes, procédez comme suit :

1. A partir du bureau Windows du client IBM, cliquez sur **Démarrer > Paramètres > Panneau de configuration > Sous-système de sécurité client IBM**. Une fois le mot de passe saisi, la fenêtre principale de l'utilitaire d'administration s'affiche.

2. Cliquez sur **Configuration du support d'application et des stratégies**.
L'écran Configuration des applications UVM et des stratégies s'affiche.
3. Désélectionnez l'option **Activation du support Lotus Notes**.
4. Cliquez sur **OK**.
L'écran Actions du support d'application affiche un message indiquant que le support Lotus Notes est désactivé.

Configuration de la protection UVM pour un autre ID utilisateur Lotus Notes

Pour passer d'un ID utilisateur dont la protection UVM est activée à un autre ID utilisateur, procédez comme suit :

1. Quittez Lotus Notes.
2. Désactivez la protection UVM pour l'ID utilisateur en cours. Reportez-vous à la section «Désactivation de la protection UVM pour un ID utilisateur Lotus Notes» à la page 20 pour plus de détails.
3. Lancez Lotus Notes et changez d'ID utilisateur. Pour plus de détails sur cette opération, consultez votre documentation Lotus Notes.
4. Pour configurer la protection UVM de cet ID utilisateur, lancez l'outil de configuration de Lotus Notes (fourni par le logiciel Client Security), et définissez la protection UVM. Reportez-vous à la section «Utilisation de la protection UVM dans Lotus Notes» à la page 20.

Utilisation du logiciel Client Security avec les applications Netscape

Les instructions de la présente section sont spécifiques à l'utilisation du logiciel Client Security pour ce qui concerne l'obtention et l'utilisation de certificats numériques avec des applications prenant en charge la norme PKCS n° 11, en particulier les applications Netscape.

Pour plus de détails concernant l'utilisation de paramètres de sécurité pour les applications Netscape, consultez la documentation fournie avec ce dernier. Seul Netscape version 4.7x est pris en charge par le logiciel IBM Client Security.

Remarque : L'utilisation de navigateurs 128 bits avec le logiciel Client Security n'est possible que si la puce de sécurité intégrée IBM prend en charge le chiffrement 256 bits. La puissance de chiffrement fournie par le logiciel Client Security est indiquée dans l'utilitaire d'administration (bouton **Paramètres de puce**).

Installation du module PKCS n° 11 de la puce de sécurité intégrée IBM pour les applications Netscape

Avant d'utiliser un certificat numérique, vous devez installer le module PKCS n° 11 de la puce de sécurité intégrée IBM sur l'ordinateur. Cette installation nécessitant un mot de passe composé UVM, vous devez ajouter au moins un utilisateur dans la stratégie de sécurité pour l'ordinateur.

Pour installer la norme PKCS n° 11 de la puce de sécurité intégrée IBM, procédez comme suit :

1. Lancez Netscape et cliquez **File > Open page**.
2. Recherchez le fichier d'installation IBMPKCSINSTALL.HTML.
(Si vous avez accepté le répertoire par défaut lors de l'installation du logiciel, ce fichier se trouve dans C:\Program Files\IBM\Security.)
3. Ouvrez le fichier IBMPKCSINSTALL.HTML dans Netscape.
Dès l'ouverture du fichier dans Netscape, la séquence d'installation démarre et la fenêtre du mot de passe composé UVM s'affiche.
4. Entrez le mot de passe composé UVM et cliquez sur **OK**.
Un message vous invite à confirmer l'installation de ce module de sécurité.
5. Cliquez sur **OK**.
Un message s'affiche pour indiquer que le module est installé.
6. Cliquez sur **OK**.

Utilisation de la protection à la connexion PKCS n° 11 pour les applications Netscape

Une fois la protection à la connexion PKCS n° 11 configurée pour l'ordinateur, vous devez suivre la procédure d'authentification requise à chaque connexion sous Netscape. Vous devrez peut-être entrer votre mot de passe composé UVM et/ou scanner vos empreintes digitales. Les besoins d'authentification sont définis dans la stratégie de sécurité UVM pour l'ordinateur.

Sélection de la puce de sécurité intégrée IBM pour la génération d'un certificat numérique pour les applications Netscape

Pendant la création du certificat numérique, lorsque vous serez invité à sélectionner la carte ou la base de données dans laquelle générer la clé, sélectionnez **Sous-système de sécurité intégré IBM**.

Pour plus d'informations sur la génération d'un certificat numérique et son utilisation dans Netscape, consultez la documentation fournie avec ce dernier.

Mise à jour de l'archive de clés pour les applications Netscape

Après avoir créé un certificat numérique, sauvegardez-le lors de la mise à jour de l'archive de clés. Vous pouvez effectuer cette mise à jour à l'aide de l'utilitaire de configuration.

Utilisation du certificat numérique pour les applications Netscape

Utilisez les paramètres de sécurité de vos applications Netscape pour afficher, sélectionner et utiliser les certificats numériques. Par exemple, dans les paramètres de sécurité de Netscape Messenger, vous devez d'abord sélectionner le certificat pour pouvoir créer des signatures numériques ou chiffrer vos messages électroniques. Pour plus d'informations, consultez la documentation fournie par Netscape.

Après avoir installé le module PKCS n° 11 de la puce de sécurité intégrée IBM, UVM vous invitera à appliquer des procédures d'authentification à chaque utilisation du certificat numérique. Vous devrez peut-être entrer votre mot de passe composé UVM et/ou scanner vos empreintes digitales. Les besoins d'authentification sont définis dans la stratégie de sécurité UVM pour l'ordinateur.

Si vous ne parvenez pas à vous authentifier suivant la procédure définie dans la stratégie UVM, un message d'erreur s'affiche. Lorsque vous cliquez sur **OK** en réponse au message, Netscape est lancé, mais vous ne pouvez pas utiliser le certificat numérique généré par la puce de sécurité intégrée IBM tant que Netscape n'a pas été redémarré et que vous n'avez pas indiqué le mot de passe composé et/ou les empreintes digitales qui conviennent.

Chapitre 6. Gestion d'une stratégie UVM

Avant d'essayer d'éditer la stratégie UVM du client local, assurez-vous qu'un utilisateur au moins est autorisé à utiliser le gestionnaire UVM. Sinon, un message d'erreur va s'afficher à chaque tentative d'ouverture d'un fichier de stratégie local à l'aide de l'éditeur.

Après l'autorisation d'utilisateurs dans le gestionnaire UVM, vous devez éditer et sauvegarder une stratégie de sécurité pour chaque client IBM. La stratégie de sécurité fournie par le logiciel Client Security est appelée stratégie UVM ; elle intègre les paramètres que vous avez indiqués à la section "Autorisation d'utilisateurs", ainsi que les procédures d'authentification au niveau du client. La stratégie UVM permet de contrôler la stratégie de sécurité d'un client local, ou peut être copiée sur des clients éloignés au sein d'un réseau.

L'utilitaire d'administration intègre un éditeur de stratégie UVM grâce auquel vous pouvez éditer et sauvegarder une stratégie UVM pour un client local. Les tâches exécutées au niveau du client IBM, telles que la connexion au système d'exploitation ou le déverrouillage de l'économiseur d'écran, sont appelées des objets d'authentification, auxquels sont associées des procédures d'authentification dans le cadre de la stratégie UVM. Vous pouvez, par exemple, définir les procédures d'authentification suivantes dans une stratégie UVM :

- Chaque utilisateur doit entrer un mot de passe composé UVM et effectuer une authentification par badge de proximité pour se connecter au système d'exploitation.
- Chaque utilisateur doit entrer un mot de passe composé UVM lors de chaque acquisition d'un certificat numérique.

Vous pouvez contrôler des objets d'authentification spécifiques qui sont définis dans la stratégie UVM à l'aide de Tivoli Access Manager.

Les objets d'authentification définis dans la stratégie UVM concernent le client IBM et non l'utilisateur individuel. Par conséquent, si vous définissez dans une stratégie UVM un objet impliquant une authentification par empreinte digitale (pour la connexion au système d'exploitation, par exemple), chacun des utilisateurs ajoutés dans UVM doit enregistrer son empreinte digitale pour pouvoir utiliser cet objet. Pour plus de détails sur l'autorisation d'un utilisateur, reportez-vous à la section «Suppression d'utilisateurs» à la page 15.

La stratégie UVM est sauvegardée dans un fichier appelé `globalpolicy.gvm`. Pour pouvoir utiliser le gestionnaire UVM sur des clients éloignés, il est nécessaire de sauvegarder la stratégie UVM sur un client IBM puis de la copier sur les clients éloignés. La copie du fichier de stratégie UVM sur des clients éloignés peut vous permettre de gagner du temps lors de la configuration.

Edition d'une stratégie UVM locale

Une stratégie UVM locale ne peut être éditée et utilisée que sur le client pour lequel elle a été éditée. Si vous avez installé le logiciel Client Security à l'emplacement par défaut, la stratégie UVM est stockée dans le répertoire \Program Files\IBM\Security\UVM_Policy\globalpolicy.gvm. Pour éditer et sauvegarder une stratégie UVM locale, utilisez l'éditeur de stratégie UVM. Seul un utilisateur inscrit dans le gestionnaire UVM peut utiliser l'éditeur de stratégie UVM. L'interface de cet éditeur est fournie dans l'utilitaire d'administration.

Lors de la sauvegarde de la stratégie UVM, un message vous invite à entrer la clé privée d'administrateur. Après avoir entré cette clé, cliquez sur **OK** afin de sauvegarder vos modifications. Si la clé indiquée est incorrecte, vos modifications ne seront pas sauvegardées.

L'authentification effectuée dépend de ce que vous sélectionnez dans l'éditeur de stratégie. Par exemple, si vous sélectionnez "Aucun mot de passe composé obligatoire après ce type de première utilisation" pour la connexion Lotus Notes, vous serez invité à suivre cette procédure d'authentification UVM lors de la première connexion à Lotus Notes. Ensuite, tant que vous n'avez pas effectué de réamorçage ni de déconnexion, vous n'avez pas à ressaisir ce mot de passe composé chaque fois que vous accédez à Lotus Notes.

Lorsque vous définissez dans une stratégie UVM un objet d'authentification impliquant la détection d'empreinte digitale (pour la connexion au système d'exploitation, par exemple), chacun des utilisateurs ajoutés dans UVM doit enregistrer ses empreintes digitales pour pouvoir utiliser cet objet.

Lorsque vous éditez une stratégie UVM, vous pouvez en afficher les informations récapitulatives en cliquant sur Récapitulatif de la stratégie. Vous pouvez également cliquer sur **Validation** afin de sauvegarder vos modifications. Dans ce cas, un message vous invite à entrer la clé privée d'administrateur. Après avoir entré cette clé, cliquez sur **OK** afin de sauvegarder vos modifications. Si la clé indiquée est incorrecte, vos modifications ne seront pas sauvegardées.

Sélection d'objet

Les objets de stratégie UVM permettent d'établir différentes stratégies de sécurité pour les différentes actions de l'utilisateur. Les objets UVM admis sont indiqués dans la page **Sélection d'objet** de l'écran Stratégie UVM IBM dans l'utilitaire d'administration.

Les objets de stratégie UVM admis sont les suivants :

Connexion système

Cet objet contrôle les procédures d'authentification nécessaires à la connexion au système.

Déverrouillage système

Cet objet contrôle les procédures d'authentification nécessaires au déverrouillage de l'économiseur d'écran du logiciel Client Security.

Lotus Notes - Connexion

Cet objet contrôle les procédures d'authentification nécessaires à la connexion à Lotus Notes.

Lotus Notes - Modification de mot de passe

Cet objet contrôle les procédures d'authentification nécessaires à la génération d'un mot de passe Lotus Notes à l'aide du gestionnaire UVM.

Signature numérique (courrier électronique)

Cet objet contrôle les procédures d'authentification nécessaires lors de la connexion sous Microsoft Outlook ou Outlook Express.

Déchiffrement (courrier électronique)

Cet objet contrôle les procédures d'authentification nécessaires lors d'une opération de déchiffrement dans Microsoft Outlook ou Outlook Express.

Protection des fichiers et des dossiers

Cet objet contrôle les procédures d'authentification nécessaires lors d'opérations de chiffrement et de déchiffrement opérées à l'aide du bouton droit de la souris.

Gestionnaire de mots de passe

Cet objet contrôle les procédures d'authentification nécessaires lorsque vous utilisez le gestionnaire de mots de passe IBM, lequel est disponible à partir du site Web d'IBM. Lorsqu'il est activé, il est préférable, pour la plupart des utilisateurs, de conserver le paramètre "Aucun mot de passe composé obligatoire après ce type de première utilisation".

Netscape - Module de connexion PKCS n° 11

Cet objet contrôle la procédure d'authentification nécessaire lorsqu'un appel PKCS n° 11 C_OpenSession est reçu par le module PKCS n° 11. Pour la plupart des utilisateurs, il est préférable de conserver le paramètre "Aucun mot de passe composé obligatoire après ce type de première utilisation."

Connexion Entrust

Cet objet contrôle les procédures d'authentification nécessaires lorsque Entrust émet un appel PKCS n° 11 C_OpenSession destiné au module PKCS n° 11. Pour la plupart des utilisateurs, il est préférable de conserver le paramètre "Aucun mot de passe composé obligatoire après ce type de première utilisation."

Entrust - Modification du mot de passe de connexion

Cet objet contrôle les procédures d'authentification nécessaires à la modification du mot de passe de connexion Entrust. Pour ce faire, Entrust émet un appel PKCS#11 C_OpenSession destiné au module PKCS n° 11. Pour la plupart des utilisateurs, il est préférable de conserver le paramètre "Aucun mot de passe composé obligatoire après ce type de première utilisation."

Éléments d'authentification

La stratégie UVM définit les éléments d'authentification disponibles qui sont requis pour chacun des objets que vous activez. Cela vous permet d'établir différentes stratégies de sécurité pour les différentes actions de l'utilisateur.

Les éléments d'authentification qui peuvent être sélectionnés à partir de la page **Éléments d'authentification** de l'écran Stratégie UVM IBM dans l'utilitaire d'administration sont les suivants :

Choix de mot de passe composé

Ce choix permet à l'administrateur d'établir le mot de passe composé UVM à utiliser pour authentifier un utilisateur de l'une des trois manières suivantes :

- Nouveau mot de passe composé obligatoire à chaque fois.

- Aucun mot de passe composé obligatoire après ce type de première utilisation.
- Mot de passe composé non obligatoire si indiqué à l'ouverture de session sur le système.

Sélection d'empreintes digitales

Ce choix permet à l'administrateur d'établir que la détection d'une empreinte digitale peu être utilisée pour authentifier un utilisateur de l'une des trois manières suivantes :

- Nouvelle empreinte digitale obligatoire à chaque fois.
- Aucune empreinte digitale obligatoire après ce type de première utilisation.
- Aucune empreinte digitale obligatoire si donnée à l'ouverture de session sur le système.

Paramètres globaux d'empreintes digitales

Ce choix permet à l'administrateur d'établir un nombre maximal de tentatives d'authentification avant le verrouillage du système pour un utilisateur. Cette zone permet également à l'administrateur d'autoriser le remplacement de la protection par authentification d'empreinte digitale par un mot de passe composé.

Sélection de carte à puce

Cette sélection permet à un administrateur d'exiger qu'une carte à puce soit fournie comme dispositif d'authentification supplémentaire.

Paramètres globaux de carte à puce

Cette sélection permet à un administrateur de définir la stratégie permettant la substitution lorsque le mot de passe composé UVM est fourni.

Utilisation de l'éditeur de stratégie UVM

Pour utiliser l'éditeur de stratégie UVM, procédez comme suit dans l'utilitaire d'administration :

1. Cliquez sur le bouton **Configuration du support d'application et des stratégies**.
L'écran Configuration des applications UVM et des stratégies s'affiche.
2. Cliquez sur le bouton **Stratégie d'application**.
L'écran Modification de la configuration de stratégie de Client Security s'affiche.
3. Cliquez sur le bouton **Edition de la stratégie**.
L'écran Saisie du mot de passe administrateur s'affiche.
4. Entrez votre mot de passe administrateur et cliquez sur **OK**.
L'écran Stratégie UVM IBM s'affiche.
5. Cliquez sur l'onglet Sélection d'objet, puis sur **Action** ou **Type d'objet** et sélectionnez l'objet auquel vous souhaitez associer des procédures d'authentification.
Les actions proposées sont les suivantes : Connexion système, Déverrouillage système et Déchiffrement de courrier électronique. Exemple de type d'objet : Acquisition de certificat numérique.
6. Pour chaque objet sélectionné, effectuez les opérations suivantes :
 - Cliquez sur l'onglet **Éléments d'authentification** et éditez les paramètres des éléments d'authentification disponibles que vous souhaitez affecter à l'objet.

- Sélectionnez **Access Manager contrôle l'objet sélectionné** afin de permettre à Tivoli Access Manager de contrôler l'objet que vous avez choisi. Ne sélectionnez cette option que si vous voulez que Tivoli Access Manager contrôle les éléments d'authentification pour le client IBM. Pour plus de détails, consultez le manuel *Utilisation du logiciel Client Security avec Tivoli Access Manager*.
- Important** : Si vous activez le contrôle de Tivoli Access Manager sur l'objet, vous lui accordez également le contrôle sur l'espace objet. Dans ce cas, vous devez réinstaller le logiciel Client Security pour établir à nouveau un contrôle local sur cet objet.
- Sélectionnez **Refuser tout accès à l'objet sélectionné** afin qu'aucun accès ne soit possible à l'objet que vous avez choisi.
7. Cliquez sur **OK** afin de sauvegarder vos modifications et sortir.

Edition et utilisation d'une stratégie UVM pour des clients éloignés

Pour pouvoir appliquer une stratégie UVM à plusieurs clients IBM, vous devez l'éditer et la sauvegarder pour un client éloigné, puis copier le fichier correspondant sur d'autres clients IBM. Si vous installez le logiciel Client Security à l'emplacement par défaut, le fichier de stratégie UVM se trouve dans le répertoire \Program Files\IBM\Security\UVM_Policy\remote\globalpolicy.gvm.

Copiez les fichiers suivants sur les autres clients IBM éloignés qui vont utiliser cette stratégie UVM :

- \IBM\Security\UVM_Policy\remote\globalpolicy.gvm
- \IBM\Security\UVM_Policy\remote\globalpolicy.gvm.sig

Si vous avez installé le logiciel Client Security à l'emplacement par défaut, le répertoire principal des chemins précédents est \Program Files. Copiez les deux fichiers dans le répertoire \IBM\Security\UVM_Policy\ sur les clients éloignés.

Chapitre 7. Autres fonctions de l'utilitaire d'administration

Lors de la configuration du logiciel Client Security sur les clients IBM, vous utilisez l'utilitaire d'administration pour activer la puce de sécurité intégrée IBM, définir un mot de passe pour la puce de sécurité, générer des clés matérielles ou encore configurer la stratégie de sécurité. La présente section contient les instructions relatives à l'utilisation des autres fonctions de l'utilitaire d'administration.

Pour lancer l'utilitaire d'administration, procédez comme suit :

1. A partir du bureau Windows du client IBM, cliquez sur **Démarrer > Paramètres > Panneau de configuration > Sous-système de sécurité client IBM.**

L'accès à l'utilitaire d'administration étant protégé par le mot de passe de la puce de sécurité, un message vous invite à entrer ce mot de passe.

2. Entrez le mot de passe de la puce de sécurité et cliquez sur **OK.**

Utilisation de la console d'administration

La console d'administration du logiciel Client Security permet à un administrateur de la sécurité d'exécuter des tâches spécifiques à sa fonction à distance à partir de son système.

L'application de la console d'administration (console.exe) doit être installée et lancée à partir du répertoire `\program files\ibm\security`.

La console d'administration permet à un administrateur de la sécurité d'exécuter les fonctions suivantes :

- **Contournement ou substitution des éléments d'authentification.** Fonctions de contournement ou de substitution que l'administrateur peut appliquer :
 - **Contournement des mots de passe composés UVM.** Cette fonction permet à l'administrateur de contourner les mots de passe composés UVM. Lorsqu'elle est utilisée, un mot de passe composé aléatoire est créé de façon temporaire, ainsi qu'un fichier des mots de passe. L'administrateur envoie le fichier des mots de passe à l'utilisateur et communique le mot de passe par d'autres moyens. Ce système garantit la sécurité du nouveau mot de passe composé.
 - **Affichage/modification du mot de passe d'effacement d'empreinte digitale/de carte à puce.** Cette fonction permet à l'administrateur de remplacer la stratégie de sécurité même si elle a été définie pour NE PAS permettre la substitution de mot de passe composé pour l'empreinte digitale ou la carte à puce. Cela peut s'avérer nécessaire si le lecteur d'empreinte digitale d'un utilisateur est hors service ou si sa carte à puce est indisponible. L'administrateur peut ainsi communiquer oralement ou par courrier électronique le mot de passe de substitution à l'utilisateur.
- **Accès aux informations de clés d'archive.** L'administrateur peut accéder aux informations suivantes :
 - **Répertoire d'archivage.** Cette zone permet à l'administrateur de localiser les informations de clé d'archive à partir d'un emplacement éloigné.
 - **Emplacement de clé privée admin.** Cette zone permet à l'administrateur de localiser la clé privée de l'administrateur.

- **Autres fonctions d'administration à distance.** La console d'administration permet à un administrateur de sécurité d'exécuter à distance les fonctions suivantes :
 - **Création d'un fichier de config admin.** Cette fonction permet à l'administrateur de générer le fichier de configuration administrateur, lequel est requis lorsqu'un utilisateur souhaite s'inscrire ou réinitialiser son profil à l'aide de l'utilitaire client. L'administrateur envoie généralement ce fichier à l'utilisateur par courrier électronique.
 - **Fichier de configuration chiffrement/déchiffrement.** Cette fonction permet de chiffrer le fichier de configuration pour une sécurité supplémentaire. Elle permet également de déchiffrer le fichier pour pouvoir le modifier.
 - **Configuration de la délocalisation (roaming) d'accréditation.** Cette fonction enregistre le système en tant que serveur CSS Roaming Serveur. Une fois enregistré, tout utilisateur autorisé UVM du réseau pourra accéder à ses données personnelles (mots de passe composés, certificat, etc.) sur le système.

Enregistrement d'un client d'un réseau de délocalisation (roaming) d'accréditation

Pour enregistrer un client d'un réseau de délocalisation (roaming) d'accréditation, procédez comme suit :

1. A l'aide de l'utilitaire de la console, déchiffrez un fichier CSEC.INI précédemment généré. Ce fichier contient déjà le mot de passe matériel et les utilisateurs à enregistrer.
2. Dans la section csssetup du fichier, ajoutez "enable roaming=1". Vous indiquez ainsi que le système doit être enregistré comme client itinérant.
3. Dans la même section, ajoutez l'entrée "username=OPTION". Trois options sont possibles pour cette valeur :
 - a. **La chaîne "[promptcurrent]" - crochets inclus.** Cette désignation doit être utilisée si un fichier .dat pour le client actuellement connecté a été généré sur le serveur de délocalisation (roaming) et si l'utilisateur actuel connaît le mot de passe d'enregistrement du système. Cette option entraîne l'affichage d'une zone invitant l'utilisateur à saisir sysregpwd. Naturellement, s'il s'agit d'une installation en mode silencieux, l'administrateur souhaitera éviter ce paramètre puisqu'il nécessite l'intervention d'un utilisateur sur le clavier.
 - b. **La chaîne "[current]" - crochets inclus.** Cette désignation doit être utilisée si un fichier .dat pour le client actuellement connecté a été généré sur le serveur. Le sysregpwd sera géré comme décrit au point suivant.
 - c. **Un nom d'utilisateur réel tel que "joseph".** Si un nom d'utilisateur désigné de ce type est utilisé, le fichier "joseph.dat" doit avoir été préalablement généré par le serveur de délocalisation. Le sysregpwd pour ce cas sera également généré comme décrit au point suivant.
4. Enfin, si les options deux ou trois ci-dessus sont utilisées, une autre entrée "sysregpwd=SYSREGPW" doit être fournie. Il s'agit d'un mot de passe à huit chiffres, associé à l'utilisateur actuel (si l'option deux est mise en oeuvre) ou à l'utilisateur désigné (si l'option trois est mise en oeuvre).
5. Pour terminer l'enregistrement du client, connectez le système à la configuration de l'emplacement d'archive via le serveur de délocalisation. Cet emplacement d'archive sera indiqué dans le fichier CSEC.INI.

Exemples de fichier CSEC.INI

Les exemples ci-dessous montrent un échantillon de fichier CSEC.INI, et illustrent la façon dont ce fichier change en fonction de l'option de délocalisation (roaming) d'accréditation sélectionnée. Ces options sont les suivantes :

- **Aucune valeur de délocalisation.** Ce fichier de base n'est pas activé pour la délocalisation (roaming) d'accréditation.
- **Délocalisation option 1.** Ce fichier est activé pour la délocalisation à l'aide de l'option 1 pour l'enregistrement client. L'utilisateur actuel doit indiquer le mot de passe d'enregistrement système.
- **Délocalisation option 2.** Ce fichier est activé pour la délocalisation à l'aide de l'option 2 pour l'enregistrement client. L'utilisateur actuel doit indiquer son ID utilisateur, ainsi que le mot de passe d'enregistrement système.
- **Délocalisation option 3.** Ce fichier est activé pour la délocalisation à l'aide de l'option 3 pour l'enregistrement client. L'utilisateur est désigné. L'utilisateur désigné doit indiquer le mot de passe d'enregistrement système.

Exemples de quatre fichiers CSEC.INI distincts :

[CSSSetup] suppw=bootup hwpw=11111111 newkp=1 keysplit=1 kpl=c:\jgk kal=c:\jgk\archive clean=0	[CSSSetup] suppw=bootup hwpw=11111111 newkp=1 keysplit=1 kpl=c:\jgk kal=c:\jgk\archive enableroaming=1 username=[promptcurrent] clean=0	[CSSSetup] suppw=bootup hwpw=11111111 newkp=1 keysplit=1 kpl=c:\jgk kal=c:\jgk\archive enableroaming=1 username=[current] sysregpwd=12345678 clean=0	[CSSSetup] suppw=bootup hwpw=11111111 newkp=1 keysplit=1 kpl=c:\jgk kal=c:\jgk\archive enableroaming=1 username=joseph sysregpwd=12345678 clean=0
[UVMEnrollment] enrollall=0 user1=joseph user1uvmpw=q1234r user1winpw= user1domain=0 user1ppchange=0 user1ppexppolicy=0 user1ppexpdays=184 enrollusers=1	[UVMEnrollment] enrollall=0 user1=joseph user1uvmpw=q1234r user1winpw= user1domain=0 user1ppchange=0 user1ppexppolicy=0 user1ppexpdays=184 enrollusers=1	[UVMEnrollment] enrollall=0 user1=joseph user1uvmpw=q1234r user1winpw= user1domain=0 user1ppchange=0 user1ppexppolicy=0 user1ppexpdays=184 enrollusers=1	[UVMEnrollment] enrollall=0 user1=joseph user1uvmpw=q1234r user1winpw= user1domain=0 user1ppchange=0 user1ppexppolicy=0 user1ppexpdays=184 enrollusers=1
[UVMAppConfig] uvmlogon=0 entrust=0 notes=0 netscape=0 passman=0 folderprotect=0 autoprotect=0	[UVMAppConfig] uvmlogon=0 entrust=0 notes=0 netscape=0 passman=0 folderprotect=0 autoprotect=0	[UVMAppConfig] uvmlogon=0 entrust=0 notes=0 netscape=0 passman=0 folderprotect=0 autoprotect=0	[UVMAppConfig] uvmlogon=0 entrust=0 notes=0 netscape=0 passman=0 folderprotect=0 autoprotect=0

Modification de l'emplacement de l'archive de clés

Lors de la première création d'archive de clés, des copies de toutes les clés de chiffrement sont créées et sauvegardées à un emplacement spécifié au moment de l'installation.

Remarque : L'emplacement de l'archive de clés peut également être modifié par l'utilisateur client à l'aide de l'utilitaire de configuration client. Pour plus de détails, reportez-vous au Chapitre 8, «Instructions destinées à l'utilisateur client», à la page 43.

Pour modifier l'emplacement de l'archive de clés, procédez comme suit dans l'utilitaire d'administration :

1. Cliquez sur le bouton **Configuration de clé**.
L'écran Modification de la configuration de clé de Client Security - Configuration de clés s'affiche.
2. Cliquez sur le bouton d'option **Modification de l'emplacement d'une archive**, puis sur le bouton **Suivant**.
L'écran Modification de la configuration de clé de Client Security - Nouvel emplacement de l'archive de clés s'affiche.
3. Entrez le nouveau chemin, ou cliquez sur **Parcourir** pour le sélectionner.
4. Cliquez sur **OK**.
Un message s'affiche afin d'indiquer que l'opération a abouti.
5. Cliquez sur **Terminer**.

Modification de la paire de clés d'archive

Lors de la première création de la paire de clés d'archive, cette dernière est généralement stockée sur une disquette ou dans un répertoire réseau. Si la paire de clés d'archive est endommagée, vous pouvez en changer.

Remarque : Avant de modifier la paire de clés d'archive, vérifiez que l'archive est à jour.

Pour modifier la paire de clés d'archive, procédez comme suit dans l'utilitaire d'administration :

1. Cliquez sur le bouton **Configuration de clé**.
L'écran Modification de la configuration de clé de Client Security - Configuration de clés s'affiche.
2. Cliquez sur le bouton d'option **Modification de la paire de clés d'archive du Sous-système de sécurité IBM**, puis sur **Suivant**.
L'écran Modification de la configuration de clé de Client Security - Nouveau fichier de clé publique d'administrateur UVM s'affiche.
3. Dans la zone Nouvelle clé d'archive CSS, entrez le nom de fichier de la nouvelle clé publique d'archive en regard de l'invite Fichier de clés publiques. Vous pouvez également cliquer sur **Parcourir** afin de rechercher le nouveau fichier, ou sur **Création** pour générer une nouvelle clé publique d'archive.

Remarque : Veillez à créer la nouvelle clé publique dans un emplacement différent de celui contenant les anciens fichiers de clés d'archive.

4. Dans la zone Nouvelle clé d'archive CSS, entrez le nom de fichier de la nouvelle clé privée d'archive en regard de l'invite Fichier de clés privées. Vous

pouvez également cliquer sur **Parcourir** afin de rechercher le nouveau fichier, ou sur **Création** pour générer une nouvelle paire de clés d'archive.

Remarque : Veillez à créer la nouvelle paire de clés dans un emplacement différent de celui contenant les anciens fichiers de clés d'archive.

5. Dans la zone Ancienne clé d'archive CSS, entrez le nom de fichier de l'ancienne clé publique d'archive en regard de l'invite Fichier de clés publiques, ou cliquez sur **Parcourir** afin de rechercher le fichier.
6. Dans la zone Ancienne clé d'archive CSS, entrez le nom de fichier de l'ancienne clé privée d'archive en regard de l'invite Fichier de clés privées, ou cliquez sur **Parcourir** afin de rechercher le fichier.
7. Dans la zone Emplacement de l'archive, entrez le chemin d'accès au fichier dans lequel est stockée l'archive de clés, ou cliquez sur **Parcourir** afin de sélectionner le chemin.
8. Cliquez sur **Suivant**.

Remarque : Si la paire de clés d'archive a été scindée en plusieurs fichiers, un message vous invite à entrer le chemin et le nom de chaque fichier. Cliquez sur **Lecture fichier suivant** après avoir entré chaque nom de fichier dans la zone Fichier de clés.

Un message s'affiche afin d'indiquer que l'opération est terminée.

9. Cliquez sur **OK**.

Un message s'affiche afin d'indiquer que l'opération a abouti.

10. Cliquez sur **Terminer**.

Restauration de clés à partir d'une archive

Vous devrez peut-être restaurer des clés en cas de remplacement d'une carte principale ou d'une unité de disque dur défaillante. Lors de la restauration des clés, vous copiez les fichiers de clés utilisateur les plus récents de l'archive de clés et les stockez dans la puce de sécurité intégrée IBM. Ces fichiers figurent dans le même répertoire que celui où il figuraient auparavant sur l'ordinateur.

Si une défaillance d'unité de disque dur compromet l'intégrité des clés utilisateur, vous pouvez restaurer ces dernières à partir d'une archive de clés. Les clés restaurées remplacent les clés préalablement stockées.

Si vous remplacez la carte principale de votre ordinateur par une carte principale contenant la puce de sécurité intégrée IBM, et que les clés de chiffrement sont toujours valables sur votre unité de disque dur, vous pouvez restaurer les clés qui étaient auparavant associées à l'ordinateur en les "re-chiffrant" sur la puce de sécurité intégrée IBM de la nouvelle carte principale.

Vous ne pouvez restaurer des clés qu'après avoir activé la nouvelle puce et défini un mot de passe de puce de sécurité. Pour plus de détails, reportez-vous à la section «Activation de la puce de sécurité intégrée IBM et définition d'un mot de passe de puce de sécurité» à la page 40.

Remarque : La fonction de connexion UVM est activée automatiquement après une restauration de clés. En conséquence, vous DEVEZ, si une procédure d'authentification par empreinte digitale était requise pour la

connexion UVM, installer le logiciel de détection d'empreinte digitale avant le réamorçage après restauration afin d'éviter un verrouillage du système.

Dans les instructions ci-après, l'on suppose que l'utilitaire d'administration n'est pas endommagé par une défaillance de l'unité de disque dur. En cas d'endommagement des fichiers de sécurité client, vous devrez peut-être réinstaller le logiciel Client Security.

Pour restaurer des clés de chiffrement à partir d'une archive de clés, procédez comme suit dans l'utilitaire d'administration :

Remarque : Si vous modifiez la paire de clés d'administrateur après la restauration de l'archive, un message d'erreur s'affiche. Dans ce cas, vous devez ajouter des utilisateurs dans UVM, puis demander de nouveaux certificats.

1. Cliquez sur le bouton **Configuration de clé**.
L'écran Modification de la configuration de clé de Client Security - Configuration de clés s'affiche.
2. Cliquez sur le bouton d'option **Restauration des clés du Sous-système de sécurité IBM à partir d'une archive**, puis sur **Suivant**.
L'écran Modification de la configuration de clé de Client Security - Restauration de toutes les clés du Sous-système de sécurité IBM s'affiche.
3. Dans la zone Répertoire de l'archive (chemin), entrez le chemin d'accès au répertoire d'archivage, ou cliquez sur **Parcourir** afin de rechercher le répertoire.
4. Dans la zone Fichier de clés privées d'archive CSS, entrez le chemin et le nom de fichier de la clé publique d'administrateur, ou cliquez sur **Parcourir** afin de rechercher le fichier.
5. Dans la zone Fichier de clés privées d'archive CSS, entrez le chemin et le nom de fichier de la clé privée d'administrateur, ou cliquez sur **Parcourir** afin de rechercher le fichier.
6. Cliquez sur **Suivant**.
Un message s'affiche afin d'indiquer que l'opération est terminée.

Remarque : Si la clé privée d'administrateur a été scindée en plusieurs fichiers, un message vous invite à entrer le chemin et le nom de chaque fichier. Cliquez sur **Lecture fichier suivant** après avoir entré chaque nom de fichier dans la zone Fichier de clés.

7. Cliquez sur **OK**.
8. Cliquez sur **Terminer**.

Réinitialisation du compteur d'échecs d'authentification

Pour réinitialiser le compteur d'échecs d'authentification d'un utilisateur, procédez comme suit dans l'utilitaire d'administration :

1. Dans la zone Utilisateurs Windows autorisés à utiliser UVM, sélectionnez un nom d'utilisateur.
2. Cliquez sur **Réinitialisation du compteur d'échecs**.
L'écran Réinitialisation du nombre d'échecs d'authentification pour un utilisateur s'affiche.
3. Entrez le mot de passe composé UVM pour l'utilisateur sélectionné et cliquez sur **OK**.
Un message s'affiche pour indiquer que l'opération a abouti.
4. Cliquez sur **OK**.

Modification des paramètres de Tivoli Access Manager

Les informations ci-après sont destinées aux administrateurs de la sécurité qui envisagent d'utiliser Tivoli Access Manager pour gérer les objets d'authentification de la stratégie de sécurité UVM. Pour plus de détails, consultez le manuel *Utilisation du logiciel Client Security avec Tivoli Access Manager*.

Accès au fichier de configuration de Tivoli Access Manager

Pour configurer les informations de configuration de Tivoli Access Manager sur le client IBM, le logiciel Client Security utilise un fichier de configuration. Ce fichier permet d'établir un lien entre Tivoli Access Manager et les objets dont la stratégie UVM lui cède le contrôle. Pour accéder à la configuration de Tivoli Access Manager, procédez comme suit dans l'utilitaire d'administration :

1. Cliquez sur le bouton **Configuration du support d'application et des stratégies**.
L'écran Configuration des applications UVM et des stratégies s'affiche.
2. Dans la zone Tivoli Access Manager - Informations de configuration, entrez le chemin et le nom du fichier de configuration, ou cliquez sur **Parcourir** afin de rechercher le fichier.
3. Cliquez sur le bouton **Edition de la stratégie**.
4. Poursuivez la procédure d'édition de stratégie.

Régénération de la mémoire cache locale

Une réplique locale des informations de stratégie de sécurité, gérée par Tivoli Access Manager, figure sur le client IBM. Vous pouvez définir la fréquence de régénération de cette mémoire cache locale par incréments de mois et de jour, ou bien vous pouvez effectuer une mise à jour immédiate de la mémoire cache locale en cliquant sur le bouton approprié.

Pour ce faire, procédez comme suit dans l'utilitaire d'administration :

1. Cliquez sur le bouton **Configuration du support d'application et des stratégies**.
L'écran Configuration des applications UVM et des stratégies s'affiche.
2. Dans la zone Fréquence de régénération de la mémoire cache locale, procédez comme suit :
 - Pour régénérer la mémoire cache locale immédiatement, cliquez sur **Régénération de la mémoire cache locale**.

- Pour définir la fréquence de régénération, entrez le nombre de mois et de jours souhaités dans les zones prévues à cet effet. Les valeurs indiquées représentent l'intervalle entre les régénérations planifiées.

Récupération d'un mot de passe composé UVM

Un mot de passe composé UVM est créé pour chaque utilisateur autorisé dans la stratégie de sécurité du client IBM. L'utilitaire d'administration permet à un administrateur de récupérer un mot de passe composé, qui peut être perdu ou oublié, ou encore modifié par l'utilisateur client.

Pour récupérer un mot de passe composé, procédez comme suit dans l'utilitaire d'administration :

1. Sélectionnez un utilisateur à partir de la zone Utilisateurs Windows autorisés à utiliser UVM.
2. Cliquez sur le bouton **Modification du mot de passe composé**.
L'écran de modification du mot de passe composé s'affiche.
3. Dans la zone Emplacement des archives du Sous-système de sécurité IBM, entrez le chemin et le nom du répertoire de l'archive de clés, ou cliquez sur **Parcourir** afin de localiser le répertoire.
4. Dans la zone Clé d'archive du Sous-système de sécurité IBM, entrez le chemin et le nom de fichier de la clé privée en regard de l'invite Clé privée, ou cliquez sur **Parcourir** afin de localiser le fichier.
5. Dans la zone Clé d'archive du Sous-système de sécurité IBM, entrez le chemin et le nom de fichier de la clé publique d'administrateur en regard de l'invite Clé publique, ou cliquez sur **Parcourir** afin de localiser le fichier.
6. Cliquez sur **OK**.
Un message vous indique le mot de passe composé UVM pour l'utilisateur.
7. Cliquez sur **OK**.
Si la clé privée d'administrateur a été scindée en plusieurs fichiers, un message vous invite à entrer le chemin et le nom de chaque fichier. Cliquez sur **Lecture fichier suivant** après avoir entré chaque nom de fichier dans la zone Fichier de clés privées.
Cette procédure produit un mot de passe temporaire aléatoire et un fichier de mots de passe. Ces deux éléments sont nécessaires pour pouvoir de nouveau accéder au système verrouillé.
8. Envoyez ce fichier à l'utilisateur et communiquez le mot de passe correspondant par d'autres moyens.

Modification du mot de passe de la puce de sécurité IBM

Vous devez définir 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. Pour une sécurité accrue, vous devez modifier régulièrement le mot de passe de la puce de sécurité. Un mot de passe qui demeure inchangé pendant longtemps devient plus vulnérable pour l'extérieur. Protégez le mot de passe de la puce de sécurité pour empêcher les utilisateurs non autorisés de modifier des paramètres de l'utilitaire d'administration. Pour plus d'informations sur les règles de mot de passe de la puce de sécurité, reportez-vous à l'Annexe B, «Règles relatives aux mots de passe et aux mots de passe composés», à la page 73.

Pour modifier le mot de passe de la puce de sécurité, procédez comme suit dans l'utilitaire d'administration :

1. Cliquez sur le bouton **Paramètres de puce**.
L'écran Modification des paramètres de la puce de sécurité IBM s'affiche.
2. Cliquez sur **Modification du mot de passe**.
L'écran Modification du mot de passe de la puce de sécurité IBM s'affiche.
3. Dans la zone Nouveau mot de passe, entrez un nouveau mot de passe.
4. Dans la zone Confirmation, entrez de nouveau le mot de passe.
5. Cliquez sur **OK**.

Un message s'affiche pour indiquer que l'opération a abouti.

Attention : N'appuyez pas sur les touches Entrée ou Tab > Entrée pour sauvegarder les modifications. Ce faisant, l'écran Désactivation de la puce s'afficherait. Si c'est le cas, ne désactivez pas la puce mais quittez l'écran.

6. Cliquez sur **OK**.

Affichage des informations relatives au logiciel Client Security

Les informations suivantes concernant la puce de sécurité intégrée IBM et le logiciel Client Security sont accessibles en cliquant sur le bouton **Paramètres de puce** de l'utilitaire d'administration :

- Numéro de version du microcode utilisé avec le logiciel Client Security
- Etat de chiffrement de la puce de sécurité intégrée
- Validité des clés de chiffrement matérielles
- Etat de la puce de sécurité intégrée IBM

Désactivation de la puce de sécurité intégrée IBM

L'utilitaire d'administration permet de désactiver la puce de sécurité intégrée IBM. Le mot de passe de la puce de sécurité étant requis pour lancer l'utilitaire d'administration et désactiver la puce, vous devez le protéger afin d'empêcher des utilisateurs non autorisés de désactiver la puce.

Important : N'effectuez pas un vidage de la puce de sécurité intégrée IBM pendant que la protection UVM est activée. Ce faisant, vous verrouillerez complètement le système. Pour annuler la protection UVM, ouvrez l'utilitaire d'administration et désélectionnez la case à cocher **Remplacement de la fenêtre de connexion standard de Windows par la fenêtre de connexion sécurisée UVM**. Vous devez ensuite redémarrer l'ordinateur pour que la protection UVM de connexion système soit désactivée.

Pour désactiver la puce de sécurité intégrée, procédez comme suit dans l'utilitaire d'administration :

1. Cliquez sur le bouton **Paramètres de puce**.
2. Cliquez sur le bouton **Désactivation de la puce** et suivez les instructions affichées à l'écran.
3. Si la sécurité avancée a été activée sur votre ordinateur, vous devrez peut-être saisir le mot de passe administrateur qui a été défini dans l'utilitaire de configuration pour pouvoir désactiver la puce.

Après désactivation de la puce, il n'est pas possible de réutiliser la puce de sécurité intégrée IBM et les clés de chiffrement. Une réactivation de la puce est nécessaire pour cela.

Activation de la puce de sécurité intégrée IBM et définition d'un mot de passe de puce de sécurité

Si vous devez activer la puce de sécurité intégrée IBM alors que le logiciel est déjà installé, vous pouvez, grâce à l'utilitaire d'administration, redéfinir le mot de passe de la puce de sécurité et configurer de nouvelles clés de chiffrement.

Vous pouvez également être amené à activer la puce de sécurité intégrée IBM pour restaurer l'archive de clés après le remplacement d'une carte principale ou la désactivation de la puce.

Pour activer la puce et définir un mot de passe de sécurité, procédez comme suit :

1. A partir du bureau Windows du client IBM, cliquez sur **Démarrer > Paramètres > Panneau de configuration > Sous-système de sécurité client IBM.**

Un message s'affiche afin de vous demander si vous souhaitez activer la puce de sécurité intégrée IBM pour le client IBM.

2. Cliquez sur **Oui.**

Un message s'affiche afin de vous inviter à redémarrer l'ordinateur. Vous devez redémarrer l'ordinateur afin que la puce de sécurité intégrée IBM puisse être activée. Si la sécurité avancée a été activée sur votre ordinateur, vous devrez peut-être saisir le mot de passe administrateur qui a été défini dans l'utilitaire de configuration pour pouvoir activer la puce.

3. Cliquez sur **OK** pour redémarrer l'ordinateur.

4. A partir du bureau Windows, cliquez sur **Démarrer > Paramètres > Panneau de configuration > Sous-système de sécurité client IBM.**

L'accès à l'utilitaire d'administration étant protégé par le mot de passe de la puce de sécurité, un message vous invite à entrer ce mot de passe.

5. Entrez un nouveau mot de passe pour la puce de sécurité dans la zone Nouveau mot de passe, puis entrez de nouveau ce mot de passe dans la zone Confirmation.

6. Cliquez sur **OK.**

Activation du support Entrust

La puce de sécurité intégrée IBM associée au logiciel Client Security permet d'améliorer les dispositifs de sécurité Entrust. L'activation du support Entrust sur un ordinateur doté du logiciel Client Security a pour effet de transférer les fonctions de sécurité du logiciel Entrust sur la puce de sécurité IBM.

Le logiciel Client Security localise automatiquement le fichier entrust.ini afin d'activer le support Entrust ; néanmoins, si le fichier entrust.ini ne se trouve pas dans son emplacement habituel, une boîte de dialogue s'affiche dans laquelle l'utilisateur peut rechercher entrust.ini. Une fois le fichier localisé et sélectionné par l'utilisateur, le support Entrust peut être activé par Client Security. Après sélection de l'option **Activation du support Entrust**, un réamorçage est nécessaire pour que le logiciel Entrust puisse utiliser la puce de sécurité intégrée IBM.

Pour activer le support Entrust, procédez comme suit :

1. A partir du bureau Windows du client IBM, cliquez sur **Démarrer > Paramètres > Panneau de configuration > Sous-système de sécurité client IBM.**

La fenêtre principale de l'utilitaire d'administration s'affiche.

2. Cliquez sur **Configuration du support d'application et des stratégies.**

L'écran Configuration des applications UVM et des stratégies s'affiche.

3. Sélectionnez l'option **Activation du support Entrust**.
4. Cliquez sur **Validation**.

L'écran IBM Client Security - Prise en charge d'Entrust affiche un message indiquant que le support Entrust est activé.

Remarque : Vous devez redémarrer l'ordinateur afin que les modifications soient prises en compte.

Chapitre 8. Instructions destinées à l'utilisateur client

La présente section fournit des informations pour aider un utilisateur client à exécuter les opérations suivantes :

- Utilisation de la protection UVM pour la connexion au système
- Configuration de l'économiseur d'écran Client Security
- Utilisation de l'utilitaire de configuration utilisateur
- Utilisation de messagerie électronique et de navigation Web sécurisées
- Configuration des préférences audio UVM

Utilisation de la protection UVM pour la connexion au système

La présente section contient des informations relatives à l'utilisation de la protection UVM pour la connexion au système. La protection UVM doit être activée pour l'ordinateur pour que vous puissiez l'utiliser.

La protection UVM permet de contrôler l'accès au système d'exploitation via une interface de connexion. Elle remplace l'application de connexion Windows, si bien que lorsqu'un utilisateur déverrouille l'ordinateur, la fenêtre de connexion UVM s'affiche à la place de la fenêtre de connexion Windows. Une fois que la protection UVM est activée pour l'ordinateur, l'interface de connexion UVM s'affiche au démarrage de l'ordinateur.

Lorsque l'ordinateur fonctionne, vous pouvez accéder à l'interface de connexion UVM en appuyant sur les touches **Ctrl + Alt + Suppr** pour arrêter ou verrouiller l'ordinateur ou pour ouvrir le Gestionnaire des tâches ou déconnecter l'utilisateur actuel.

Déverrouillage du client

Pour déverrouiller un client Windows utilisant la protection UVM, exécutez la procédure suivante :

1. Appuyez sur les touches **Ctrl + Alt + Suppr** pour accéder à l'interface de connexion UVM.
2. Tapez votre ID utilisateur et le domaine auquel vous êtes connecté, puis cliquez sur **Déverrouillage système**.

La fenêtre de mot de passe composé UVM s'affiche.

Remarque : Bien qu'UVM reconnaisse plusieurs domaines, votre mot de passe utilisateur doit être identique pour tous les domaines.

3. Tapez votre mot de passe composé UVM, puis cliquez sur **OK** pour accéder au système d'exploitation.

Remarques :

1. Si le mot de passe composé UVM ne correspond pas à l'ID utilisateur et au domaine entrés, la fenêtre de connexion UVM s'affiche à nouveau.
2. En fonction des conditions d'authentification UVM requises pour le client, d'autres processus d'authentification peuvent également être nécessaires.

Economiseur d'écran Client Security

L'économiseur d'écran Client Security est composé d'une série d'images en mouvement qui s'affichent lorsque l'ordinateur est en veille pendant une période donnée. La configuration de l'économiseur d'écran Client Security permet de contrôler l'accès à l'ordinateur via une application d'écran de veille. Une fois que l'économiseur d'écran Client Security s'affiche sur le bureau, vous devez taper votre mot de passe composé UVM pour accéder au bureau système.

Configuration de l'économiseur d'écran Client Security

La présente section contient des informations sur la configuration de l'économiseur d'écran Client Security. Un utilisateur au minimum doit être enregistré dans la stratégie de sécurité de l'ordinateur pour que vous puissiez utiliser l'économiseur d'écran Client Security.

Pour configurer l'économiseur d'écran Client Security, exécutez la procédure suivante :

1. Cliquez sur **Démarrer > Paramètres > Panneau de configuration**.
2. Cliquez deux fois sur l'icône **Affichage**.
3. Cliquez sur l'onglet **Ecran de veille**.
4. Dans le menu déroulant Ecran de veille, sélectionnez **Client Security**. Pour modifier la vitesse de l'économiseur d'écran, cliquez sur **Paramètres** et sélectionnez la vitesse souhaitée.
5. Cliquez sur **OK**.

Comportement de l'économiseur d'écran Client Security

Le comportement de l'économiseur d'écran Client Security varie en fonction des paramètres de l'utilitaire d'administration UVM et de l'écran de veille Windows. Le système vérifie d'abord les paramètres Windows, puis ceux de l'utilitaire d'administration UVM. Par conséquent, l'économiseur d'écran se verrouille uniquement si la case **Protégé par mot de passe** a été cochée dans l'onglet des paramètres de l'écran de veille Windows.

Si cette case a été cochée, le système requiert le mot de passe Windows ou le mot de passe composé UVM, suivant si la case **Remplacement de la fenêtre de connexion standard de Windows par la fenêtre de connexion sécurisée UVM** a été cochée dans l'utilitaire d'administration. Si tel est le cas, le système requiert le mot de passe composé UVM. Sinon, il demande le mot de passe Windows.

D'autres conditions d'authentification peuvent également être définies dans la stratégie de sécurité de l'ordinateur ; par conséquent, une authentification supplémentaire peut être requise. Par exemple, vous pouvez avoir besoin de scanner vos empreintes digitales pour déverrouiller l'ordinateur.

Remarque : Si vous désactivez la puce de sécurité intégrée IBM ou que vous supprimez tous les utilisateurs de la stratégie de sécurité, l'économiseur d'écran Client Security n'est plus disponible.

Utilitaire de configuration utilisateur

L'utilitaire de configuration utilisateur permet à l'utilisateur client d'exécuter diverses tâches de maintenance de la sécurité qui ne requièrent pas d'accès administrateur.

Fonctions de l'utilitaire de configuration utilisateur

L'utilitaire de configuration utilisateur permet à l'utilisateur client d'exécuter les opérations suivantes :

- **Mise à jour des mots de passe et des archives.** Cet onglet vous permet d'exécuter les fonctions suivantes :
 - **Modifier le mot de passe composé UVM.** Pour améliorer la sécurité, vous pouvez changer périodiquement le mot de passe composé UVM.
 - **Mettre à jour le mot de passe Windows.** Lorsque vous modifiez le mot de passe Windows pour un utilisateur client autorisé UVM à l'aide du Gestionnaire des utilisateurs Windows, vous devez également modifier le mot de passe à l'aide de l'utilitaire de configuration utilisateur du logiciel IBM Client Security. Si un administrateur utilise l'utilitaire d'administration pour modifier le mot de passe de connexion Windows pour un utilisateur, toutes les clés de chiffrement utilisateur créées précédemment pour cet utilisateur seront supprimées et les certificats numériques associés ne seront plus valides.
 - **Redéfinir le mot de passe Lotus Notes.** Pour améliorer la sécurité, les utilisateurs Lotus Notes peuvent modifier leur mot de passe Lotus Notes.
 - **Mettre à jour l'archive de clés.** Si vous créez des certificats numériques et que vous souhaitez effectuer des copies de la clé privée stockée sur la puce de sécurité intégrée IBM ou si vous souhaitez déplacer l'archive de clés, mettez à jour l'archive de clés.
- **Configurer les préférences audio UVM.** L'utilitaire de configuration utilisateur vous permet de sélectionner un fichier audio qui sera lu lors de l'aboutissement ou non de l'authentification.
- **Configuration utilisateur.** Cet onglet vous permet d'exécuter les fonctions suivantes :
 -
 - **Réinitialisation utilisateur.** Cette fonction vous permet de redéfinir votre configuration de sécurité. Lorsque vous effectuez cette opération, toutes les clés, empreintes digitales et tous les certificats précédents sont effacés.
 - **Restaurer la configuration de sécurité utilisateur à partir d'une archive.** Cette fonction vous permet de restaurer des paramètres à partir de l'archive. Cela s'avère utile si vos fichiers ont été endommagés ou que vous souhaitez revenir à une configuration précédente.
 - **Enregistrement auprès d'un serveur itinérant CSS.** Cette fonction vous permet d'enregistrer ce système auprès d'un serveur itinérant CSS. Une fois le système enregistré, vous pourrez y importer votre configuration en cours.

Limites de l'utilitaire de configuration utilisateur sous Windows XP

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.

Utilisation de l'utilitaire de configuration utilisateur

Pour utiliser l'utilitaire de configuration utilisateur, exécutez la procédure suivante :

1. Cliquez sur **Démarrer > Programmes > Access IBM > Logiciel IBM Client Security > Modification de vos paramètres de sécurité.**

L'écran principal de l'utilitaire de configuration utilisateur du logiciel IBM Client Security s'affiche.

2. Tapez le mot de passe composé UVM pour l'utilisateur client qui requiert une modification du mot de passe composé UVM ou du mot de passe Windows et cliquez sur **OK**.
3. Sélectionnez l'un des onglets suivants :
 - **Mise à jour des mots de passe et des archives.** Cet onglet vous permet de modifier votre mot de passe composé UVM, de mettre à jour votre mot de passe Windows dans UVM, de redéfinir votre mot de passe Lotus Notes dans UVM et de mettre à jour votre archive de chiffrement.
 - **Configuration des sons UVM.** Cet onglet vous permet de sélectionner un fichier audio qui sera lu lors de l'aboutissement ou non de l'authentification.

- **Configuration utilisateur.** Cet onglet permet à un utilisateur de restaurer sa configuration à partir d'une archive ou de redéfinir sa configuration de sécurité.
4. Cliquez sur **OK** pour sortir.

Utilisation de messagerie électronique et de navigation Web sécurisées

Si vous envoyez des transactions non sécurisées sur Internet, elles risquent d'être interceptées et lues. Vous pouvez empêcher l'accès non autorisé à vos transactions Internet en vous procurant un certificat numérique et en l'utilisant pour signer et chiffrer de façon numérique vos messages électroniques ou pour sécuriser votre navigateur Web.

Un certificat numérique (également appelé ID numérique ou certificat de sécurité) est une autorisation d'accès électronique émise et signée de façon numérique par une autorité de certification. Lorsqu'un certificat numérique est émis pour vous, l'autorité de certification valide votre identité en tant que propriétaire du certificat. Une autorité de certification est un fournisseur de certificats numériques digne de confiance, qui peut être un émetteur tiers comme VeriSign, ou être configuré en tant que serveur au sein de votre société. Le certificat numérique contient votre identité, comme votre nom et votre adresse électronique, les dates d'expiration du certificat, une copie de votre clé publique et l'identité de l'autorité de certification ainsi que sa signature numérique.

Utilisation du logiciel Client Security avec des applications Microsoft

Les instructions fournies dans cette section sont propres à l'utilisation du logiciel Client Security, car elles expliquent comment obtenir et utiliser des certificats numériques avec des applications prenant en charge l'API de chiffrement Microsoft CryptoAPI, comme Outlook Express.

Pour plus de détails sur la création de paramètres de sécurité et l'utilisation d'applications de messagerie électronique telles qu'Outlook Express et Outlook, consultez la documentation fournie avec ces applications.

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. Le chiffrement renforcé fourni par le logiciel Client Security se trouve dans l'utilitaire d'administration.

Obtention d'un certificat numérique pour des applications Microsoft

Lorsque vous utilisez une autorité de certification pour créer un certificat numérique à utiliser avec des applications Microsoft, vous êtes invité à choisir un fournisseur de service cryptographique pour le certificat.

Pour utiliser les fonctions cryptographiques de la puce de sécurité intégrée IBM pour vos applications Microsoft, assurez-vous que vous sélectionnez **le fournisseur de service cryptographique du sous-système de sécurité intégré IBM** lors de l'obtention de votre certificat numérique. Cela garantit ainsi le stockage de la clé privée du certificat numérique sur la puce de sécurité IBM.

De même, sélectionnez un chiffrement renforcé pour une sécurité optimale, si cette option est disponible. La puce de sécurité intégrée IBM permettant un chiffrement 1024 bits au maximum pour la clé privée du certificat numérique, sélectionnez cette

option si elle est disponible dans l'interface de l'autorité de certification ; le chiffrement 1024 bits est également appelé chiffrement renforcé.

Une fois que vous avez sélectionné **le fournisseur de service cryptographique du sous-système de sécurité intégré IBM**, vous pouvez être amené à taper votre mot de passe composé UVM et/ou à scanner vos empreintes digitales pour répondre aux besoins d'authentification afin d'obtenir un certificat numérique. Les besoins d'authentification sont définis dans la stratégie UVM pour l'ordinateur.

Transfert de certificats à partir du fournisseur de service cryptographique Microsoft

L'outil de transfert de certificats IBM Client Security permet de déplacer des certificats qui ont été créés avec le fournisseur de service cryptographique Microsoft par défaut vers le fournisseur de service cryptographique du système de sécurité intégré IBM. La protection offerte aux clés privées associées aux certificats s'en trouve alors fortement accrue, car les clés sont désormais stockées en toute sécurité sur la puce de sécurité intégrée IBM et non plus sur un logiciel vulnérable.

Pour lancer l'outil de transfert de certificats, exécutez la procédure suivante :

1. Exécutez le programme `xfercert.exe` à partir du répertoire principal du logiciel de sécurité (en général, `C:\Program Files\IBM\Security`). La boîte de dialogue principale affiche les certificats associés au fournisseur de service cryptographique Microsoft par défaut.

Remarque : Seuls les certificats dont les clés privées ont été signalées comme *exportables* lors de leur création s'affichent dans cette liste.

2. Sélectionnez les certificats à transférer vers le fournisseur de service cryptographique du système de sécurité intégré IBM.
3. Cliquez sur le bouton **Transfert de certificats**.

Les certificats sont désormais associés au fournisseur de service cryptographique du système de sécurité intégré IBM et les clés privées sont protégées par la puce de sécurité intégrée IBM. Toutes les opérations qui utilisent ces clés privées, telles que la création de signatures numériques ou le déchiffrement du courrier électronique, sont effectuées dans l'environnement protégé de la puce.

Mise à jour de l'archive de clés pour des applications Microsoft

Une fois que vous avez créé un certificat numérique, effectuez une copie de sauvegarde du certificat en mettant à jour l'archive de clés. Vous pouvez mettre à jour l'archive de clés à l'aide de l'utilitaire d'administration.

Utilisation du certificat numérique pour des applications Microsoft

Utilisez les paramètres de sécurité de vos applications Microsoft pour visualiser et utiliser des certificats numériques. Pour plus de détails, consultez la documentation fournie par Microsoft.

Une fois que vous avez créé le certificat numérique et que vous l'avez utilisé pour signer un message électronique, UVM vous invite à vous authentifier la première fois que vous signez numériquement un message électronique. Vous pouvez être amené à taper votre mot de passe composé UVM et/ou à scanner vos empreintes digitales pour répondre aux besoins d'authentification afin d'utiliser le certificat numérique. Les besoins d'authentification sont définis dans la stratégie UVM pour l'ordinateur.

Configuration des préférences audio UVM

L'utilitaire de configuration utilisateur vous permet de configurer les préférences audio à l'aide de l'interface fournie. Pour modifier les préférences audio par défaut, exécutez la procédure suivante :

1. Cliquez sur **Démarrer > Programmes > Access IBM > Logiciel IBM Client Security > Modification de vos paramètres de sécurité.**
L'écran de l'utilitaire de configuration utilisateur du logiciel IBM Client Security s'affiche.
2. Sélectionnez l'onglet **Configuration des sons UVM.**
3. Dans la zone Sons d'authentification UVM, tapez le chemin d'accès au fichier audio à associer à une authentification réussie dans la zone Aboutissement de l'authentification, ou cliquez sur **Parcourir** pour sélectionner le fichier.
4. Dans la zone Sons d'authentification UVM, tapez le chemin d'accès au fichier audio à associer à une authentification qui n'a pas abouti dans la zone Echec de l'authentification, ou cliquez sur **Parcourir** pour sélectionner le fichier.
5. Cliquez sur **OK** pour terminer la procédure.

Chapitre 9. 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 : <ol style="list-style-type: none"> 1. Désinstallez le logiciel. 2. Réinstallez le logiciel. <p>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.</p>
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 smbush.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
<p>Un message d'erreur s'affiche lorsque vous tentez de récupérer un mot de passe composé UVM</p>	<p>Action</p>
<p>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.</p>	<p>Exécutez l'une des opérations suivantes :</p> <ul style="list-style-type: none"> • 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.
<p>Un message d'erreur s'affiche lorsque vous tentez de sauvegarder le fichier de stratégie UVM</p>	<p>Action</p>
<p>Lorsque vous tentez de sauvegarder un fichier de stratégie UVM (globalpolicy.gvm) en cliquant sur Validation ou Sauvegarde, un message d'erreur s'affiche.</p>	<p>Sortez du message d'erreur, éditez à nouveau le fichier de stratégie UVM pour apporter les modifications souhaitées, puis sauvegardez le fichier.</p>
<p>Un message d'erreur s'affiche lorsque vous tentez d'ouvrir l'éditeur de stratégie UVM</p>	<p>Action</p>
<p>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.</p>	<p>Ajoutez l'utilisateur à UVM et ouvrez l'éditeur de stratégie UVM.</p>
<p>Un message d'erreur s'affiche lorsque vous utilisez l'utilitaire d'administration</p>	<p>Action</p>
<p>Lorsque vous utilisez l'utilitaire d'administration, le message d'erreur suivant peut s'afficher :</p> <p>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.</p>	<p>Sortez du message d'erreur et redémarrez l'ordinateur.</p>
<p>Un message de désactivation de la puce s'affiche lors de la modification du mot de passe de la puce de sécurité</p>	<p>Action</p>
<p>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.</p>	<p>Exécutez les opérations suivantes :</p> <ol style="list-style-type: none"> 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 : <ul style="list-style-type: none">• 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 : <ul style="list-style-type: none">• 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 : <ol style="list-style-type: none">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 : <ol style="list-style-type: none"> 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.	Vérifiez les points suivants : <ol style="list-style-type: none"> 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.
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.	

Incident	Solution possible
<p>Incidents lors de l'utilisation d'un certificat à partir d'une adresse à laquelle sont associés plusieurs certificats</p>	<p>Action</p>
<p>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.</p>	<p>Demandez au destinataire de renvoyer son certificat numérique, puis sélectionnez ce certificat dans le carnet d'adresses d'Outlook Express.</p>
<p>Message d'échec lors de la tentative de signature numérique d'un message électronique</p>	<p>Action</p>
<p>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.</p>	<p>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.</p>
<p>Outlook Express (128 bits) chiffre uniquement les messages électroniques avec l'algorithme 3DES</p>	<p>Action</p>
<p>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.</p>	<p>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.</p> <p>Consultez la documentation Microsoft pour obtenir des informations à jour sur les algorithmes de chiffrement utilisés avec Outlook Express.</p>
<p>Les clients Outlook Express renvoient des messages électroniques avec un algorithme différent</p>	<p>Action</p>
<p>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).</p>	<p>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.</p>

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 : <ul style="list-style-type: none"> • 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
<p>Incidents lors de la lecture du courrier électronique chiffré</p> <p>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.</p> <p>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.</p>	<p>Action</p> <p>Vérifiez les points suivants :</p> <ol style="list-style-type: none"> 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.
<p>Message d'échec lors de la tentative de signature numérique d'un message électronique</p> <p>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.</p>	<p>Action</p> <p>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.</p>
<p>Un message électronique est renvoyé au client avec un algorithme différent</p> <p>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).</p>	<p>Action</p> <p>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.</p>

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
<p>Un message d'erreur risque de s'afficher lorsque vous exécutez les opérations suivantes :</p> <ul style="list-style-type: none"> • 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 	<p>Cliquez sur OK pour faire disparaître le message d'erreur. Aucune autre action n'est requise.</p> <p>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.</p>

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
<p>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.</p>	<p>Il s'agit d'une limite connue.</p> <p>Vous devez déchiffrer tous les fichiers qui ont été chiffrés à l'aide de versions précédentes du logiciel Client Security <i>avant</i> 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.</p>

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. Règles d'utilisation de la protection UVM à l'ouverture de session sur le système

La protection UVM garantit que seuls les utilisateurs qui ont été ajoutés à UVM pour un client IBM spécifique peuvent accéder au système d'exploitation. Les systèmes d'exploitation Windows comportent des applications qui assurent la protection à l'ouverture de session. Bien que la protection UVM soit conçue pour fonctionner en parallèle de ces applications d'ouverture de session Windows, elle diffère d'un système d'exploitation à un autre.

L'interface d'ouverture de session UVM remplace l'ouverture de session du système d'exploitation, de sorte que la fenêtre d'ouverture de session UVM s'ouvre à chaque essai d'ouverture de session de l'utilisateur sur le système.

Avant de configurer et d'utiliser la protection UVM pour l'ouverture de session sur le système, prenez connaissance des conseils suivants :

- Ne videz pas la puce de sécurité intégrée IBM tant que la protection UVM est activée. Le contenu du disque dur deviendrait inutilisable et il vous faudrait reformater ce dernier et réinstaller tous les logiciels.
- Si vous désélectionnez la case **Remplacement de la fenêtre de connexion standard de Windows par la fenêtre de connexion sécurisée UVM** dans l'utilitaire d'administration, le système restaure le processus de connexion Windows sans recours à la protection de connexion UVM.
- Vous avez la possibilité d'indiquer le nombre maximal de tentatives autorisées pour la saisie du mot de passe de l'application de connexion Windows. Cette option ne s'applique *pas* à la protection de la connexion UVM. Vous ne pouvez pas indiquer de valeur maximale comme nombre maximal de tentatives d'entrée du mot de passe composé UVM.

Annexe D. 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 : 59P7636

(1P) P/N: 59P7636

