

Solutions IBM Client Security



# Logiciel Client Security version 5.4

## Guide d'administration et d'utilisation



Solutions IBM Client Security



# Logiciel Client Security version 5.4

## Guide d'administration et d'utilisation

**Important**

Avant d'utiliser le présent document et le produit associé, prenez connaissance des informations générales figurant à l'Annexe D, «Réglementation américaine relative à l'exportation du logiciel Client Security», à la page 101 et à l'Annexe E, «Remarques», à la page 103.

**Première édition - octobre 2004**

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 2004. Tous droits réservés.

© Copyright International Business Machines Corporation 2004. All rights reserved.

---

# Table des matières

<b>Avis aux lecteurs canadiens . . . . .</b>	<b>vii</b>
--	------------

---

## Partie 1. Introduction au logiciel

<b>Client Security . . . . .</b>	<b>1</b>
----------------------------------	----------

### Chapitre 1. Introduction . . . . . 3

Le sous-système de sécurité intégré IBM . . . . .	3
La puce de sécurité intégrée IBM . . . . .	3
Logiciel IBM Client Security . . . . .	4
Les relations entre les mots de passe et les clés . . . . .	4
Le mot de passe administrateur . . . . .	5
Les clés publique et privée matérielles . . . . .	5
Les clés publique et privée administrateur . . . . .	6
Archive ESS . . . . .	6
Clés publique et privée utilisateur . . . . .	6
Hiérarchie de substitution de clés IBM. . . . .	6
Fonctions PKI (Public Key Infrastructure) CSS . . . . .	8

---

## Partie 2. Informations utilisateur . . . 11

### Chapitre 2. Instructions destinées à l'utilisateur client . . . . . 13

Utilisation de la protection UVM pour la connexion au système . . . . .	13
Déverrouillage du client . . . . .	13
Utilitaire de configuration utilisateur . . . . .	13
Fonctions de l'utilitaire de configuration utilisateur . . . . .	14
Limites de l'utilitaire de configuration utilisateur sous Windows XP . . . . .	14
Utilisation de l'utilitaire de configuration utilisateur . . . . .	15
Utilisation de messagerie électronique et de navigation Web sécurisées . . . . .	15
Utilisation du logiciel Client Security avec des applications Microsoft . . . . .	16
Obtention d'un certificat numérique pour des applications Microsoft . . . . .	16
Transfert de certificats à partir du fournisseur de service cryptographique Microsoft. . . . .	16
Mise à jour de l'archive de clés pour des applications Microsoft . . . . .	17
Utilisation du certificat numérique pour des applications Microsoft . . . . .	18
Configuration des préférences audio UVM . . . . .	18

### Chapitre 3. IBM Password Manager . . . 19

Introduction à IBM Password Manager . . . . .	19
Procédures IBM Password Manager . . . . .	20
Création de nouvelles entrées . . . . .	20
Extraction d'entrées . . . . .	21
Gestion des entrées. . . . .	21
Exportation des informations de connexion. . . . .	23

### Chapitre 4. Itinérance des accréditations CSS . . . . . 25

Itinérance des accréditations CSS - Configuration requise . . . . .	25
Configuration d'un serveur itinérant . . . . .	25
Configuration d'un serveur itinérant . . . . .	26
Enregistrement de clients sur le serveur itinérant . . . . .	26
Fin du processus d'enregistrement de client itinérant . . . . .	27
Enregistrement d'un client itinérant via l'utilitaire d'administration. . . . .	27
Enregistrement d'un client itinérant via l'utilitaire de configuration utilisateur . . . . .	27
Enregistrement d'un client itinérant par déploiement global (mode automatique). . . . .	27
Gestion d'un réseau itinérant . . . . .	29
Autorisation d'utilisateurs . . . . .	29
Synchronisation des données utilisateur . . . . .	30
Récupération d'un mot de passe composé perdu dans un environnement itinérant . . . . .	30
Importation d'un profil utilisateur. . . . .	30
Retrait et réintégration d'utilisateurs dans un réseau itinérant . . . . .	32
Suppression et réintégration de clients enregistrés dans un réseau itinérant . . . . .	32
Restriction de l'accès aux clients enregistrés dans un réseau itinérant . . . . .	33
Restauration d'un réseau itinérant. . . . .	34
Modification de la paire de clés administrateur . . . . .	34
Modification du dossier d'archive . . . . .	34
Utilitaire de chiffrement de fichiers et de dossiers (FFE) . . . . .	35
IBM Password Manager . . . . .	35
Termes et définitions relatifs à l'itinérance . . . . .	35

---

## Partie 3. Informations administrateur. . . . . 37

### Chapitre 5. Utilisation du logiciel Client Security . . . . . 39

Exemple 1 - Un client Windows 2000 et un client Windows XP utilisant tous deux Outlook Express . . . . .	39
Exemple 2 - Deux clients CSS Windows 2000 utilisant Lotus Notes . . . . .	40
Exemple 3 - Plusieurs clients CSS Windows 2000 gérés par Tivoli Access Manager et utilisant Netscape pour le courrier électronique . . . . .	41

### Chapitre 6. Autorisation d'utilisateurs 43

Authentification pour les utilisateurs client . . . . .	43
Éléments d'authentification . . . . .	43
Opérations préalables à l'autorisation d'utilisateurs . . . . .	44
Autorisation d'utilisateurs . . . . .	44
Suppression d'utilisateurs . . . . .	45
Création de nouveaux utilisateurs . . . . .	46

## Chapitre 7. Fonctions UVM supplémentaires . . . . . 47

Authentification Windows améliorée . . . . .	47
Planification de la la protection de connexion UVM . . . . .	47
Configuration de la protection de connexion UVM . . . . .	47
Récupération d'un mot de passe composé UVM	48
Protection de l'authentification améliorée pour les utilisateurs Lotus Notes . . . . .	49
Activation et configuration de la protection de connexion UVM pour un ID utilisateur Lotus Notes . . . . .	49
Utilisation de la protection de connexion UVM dans Lotus Notes . . . . .	50
Désactivation de la protection de connexion UVM pour un ID utilisateur Lotus Notes . . . . .	50
Configuration de la protection de connexion UVM pour un autre ID utilisateur Lotus Notes . . . . .	51
Activation des applications conformes au module PKCS 11 . . . . .	51
Installation du module PKCS 11 de la puce de sécurité intégrée IBM . . . . .	51
Sélection du sous-système de sécurité intégré IBM pour générer un certificat numérique . . . . .	52
Mise à jour de l'archive de clés . . . . .	52
Utilisation du certificat numérique du module PKCS 11 . . . . .	52
Réinitialisation d'un mot de passe composé . . . . .	52
Réinitialisation à distance d'un mot de passe composé . . . . .	53
Réinitialisation manuelle d'un mot de passe composé . . . . .	53
Enregistrement des empreintes digitales de l'utilisateur . . . . .	53

## Chapitre 8. Gestion d'une stratégie UVM . . . . . 55

Edition d'une stratégie UVM . . . . .	55
Sélection d'objet . . . . .	56
Éléments d'authentification . . . . .	57
Utilisation de l'éditeur de stratégie UVM . . . . .	58
Edition et utilisation d'une stratégie UVM . . . . .	59

## Chapitre 9. Autres fonctions de l'utilitaire d'administration . . . . . 61

Utilisation de la console d'administration . . . . .	61
Modification de l'emplacement de l'archive de clés	62
Modification de la paire de clés d'archive . . . . .	62
Restauration de clés à partir d'une archive . . . . .	63
Conditions requises pour la restauration de clé	64
Scénarios de restauration . . . . .	64
Réinitialisation du compteur d'échecs d'authentification . . . . .	66
Modification des paramètres de Tivoli Access Manager . . . . .	66
Configuration des paramètres de Tivoli Access Manager sur un client . . . . .	66
Régénération de la mémoire cache locale . . . . .	67
Modification du mot de passe administrateur . . . . .	67

Affichage des informations relatives au logiciel Client Security . . . . .	68
Désactivation du sous-système de sécurité intégré IBM . . . . .	68
Activation du sous-système de sécurité intégré IBM et définition d'un mot de passe administrateur . . . . .	69
Activation du support Entrust . . . . .	69

## Partie 4. Annexes . . . . . 71

### Annexe A. Identification des incidents 73

Fonctions d'administrateur . . . . .	73
Autorisation d'utilisateurs . . . . .	73
Suppression d'utilisateurs . . . . .	73
Définition d'un mot de passe administrateur BIOS (ThinkCentre). . . . .	73
Définition d'un mot de passe superviseur (ThinkPad) . . . . .	74
Protection du mot de passe administrateur . . . . .	75
Vidage du sous-système de sécurité intégré IBM (ThinkCentre). . . . .	75
Vidage du sous-système de sécurité intégré IBM (ThinkPad) . . . . .	76
Incidents ou limitations connus concernant CSS version 5.4. . . . .	76
Limitations relatives à l'itinérance . . . . .	76
Restauration de clés . . . . .	77
Noms d'utilisateurs de domaine et locaux . . . . .	78
Réinstallation du logiciel d'empreinte digitale Targus . . . . .	78
Mot de passe composé superviseur BIOS . . . . .	78
Utilisation de Netscape 7.x . . . . .	78
Utilisation d'une disquette pour l'archivage	78
Limitations relatives aux cartes à puce . . . . .	79
Affichage du caractère + devant les dossiers après le chiffrement . . . . .	79
Limites relatives aux utilisateurs limités de Windows XP . . . . .	79
Autres limites . . . . .	79
Utilisation du logiciel Client Security avec des systèmes d'exploitation Windows . . . . .	79
Utilisation du logiciel Client Security avec des applications Netscape . . . . .	79
Certificat du sous-système de sécurité intégré IBM et algorithmes de chiffrement. . . . .	80
Utilisation de la protection UVM pour un ID utilisateur Lotus Notes . . . . .	80
Limites de l'utilitaire de configuration utilisateur	81
Limites relatives à Tivoli Access Manager . . . . .	81
Messages d'erreur . . . . .	81
Tableaux d'identification des incidents . . . . .	82
Identification des incidents liés à l'installation . . . . .	82
Identification des incidents liés à l'utilitaire d'administration. . . . .	83
Identification des incidents relatifs à l'utilitaire de configuration utilisateur . . . . .	84
Identification des incidents liés aux ThinkPad . . . . .	85
Identification des incidents liés aux applications Microsoft . . . . .	85

Identification des incidents relatifs aux applications Netscape . . . . .	88	Nombre d'échecs sur les systèmes utilisant le TPM Atmel . . . . .	96
Identification des incidents relatifs à un certificat numérique. . . . .	90	Réinitialisation d'un mot de passe composé . . . . .	96
Identification des incidents relatifs à Tivoli Access Manager . . . . .	90	Réinitialisation à distance d'un mot de passe composé . . . . .	97
Identification des incidents relatifs à Lotus Notes	91	Réinitialisation manuelle d'un mot de passe composé . . . . .	97
Identification des incidents relatifs au chiffrement	92		
Identification des incidents relatifs aux périphériques compatibles UVM . . . . .	92	<b>Annexe C. Règles d'utilisation de la protection UVM à l'ouverture de session sur le système. . . . .</b>	<b>99</b>
<b>Annexe B. Informations relatives aux mots de passe et mots de passe composés . . . . .</b>	<b>93</b>	<b>Annexe D. Réglementation américaine relative à l'exportation du logiciel Client Security . . . . .</b>	<b>101</b>
Règles relatives aux mots de passe et aux mots de passe composés . . . . .	93	<b>Annexe E. Remarques . . . . .</b>	<b>103</b>
Règles applicables au mot de passe administrateur . . . . .	93	Remarques . . . . .	103
Règles relatives aux mots de passe composés UVM . . . . .	94	Marques . . . . .	104
Nombre d'échecs sur les systèmes utilisant le TPM national . . . . .	95		





---

## 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.

<b>France</b>	<b>Canada</b>	<b>Etats-Unis</b>
 (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.

---

## Partie 1. Introduction au logiciel Client Security

<b>Chapitre 1. Introduction</b>	<b>3</b>
Le sous-système de sécurité intégré IBM	3
La puce de sécurité intégrée IBM	3
Logiciel IBM Client Security	4
Les relations entre les mots de passe et les clés	4
Le mot de passe administrateur	5
Les clés publique et privée matérielles	5
Les clés publique et privée administrateur	6
Archive ESS	6
Clés publique et privée utilisateur	6
Hiérarchie de substitution de clés IBM	6
Fonctions PKI (Public Key Infrastructure) CSS	8



---

## Chapitre 1. Introduction

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

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

---

### Le sous-système de sécurité intégré IBM

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

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

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

### La puce de sécurité intégrée IBM

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

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

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

- Toutes les fonctions TCG (Trusted Computing Group) définies dans TCG Main Specification version 1.1
- Communication avec le processeur principal via le bus LPC (Low Pin Count)

## Logiciel IBM Client Security

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

- **Utilitaire d'administration** : Cet utilitaire est l'interface que l'administrateur utilise pour activer ou désactiver le sous-système de sécurité intégré et pour créer, archiver et régénérer les clés de chiffrement et les mots de passe composés. En outre, l'administrateur peut ajouter des utilisateurs dans la stratégie de sécurité fournie par le logiciel Client Security.
- **Console d'administration** : La console d'administration du logiciel Client Security permet à l'administrateur de configurer un réseau itinérant d'accréditation, de créer et de configurer des fichiers qui activent le déploiement, de créer une configuration non administrateur et de récupérer des profils.
- **Utilitaire de configuration utilisateur** : Cet utilitaire permet à l'utilisateur client de modifier le mot de passe composé UVM, d'autoriser la reconnaissance des mots de passe de connexion Windows par UVM, de mettre à jour les archives de clés et d'enregistrer des empreintes digitales. L'utilisateur peut également créer des certificats numériques générés à l'aide du sous-système de sécurité intégré IBM.
- **Gestionnaire de vérification d'utilisateur (UVM)** : Le logiciel Client Security utilise le gestionnaire UVM pour gérer les mots de passe composés et d'autres éléments d'authentification des utilisateurs du système. Par exemple, un lecteur d'empreintes digitales peut être utilisé par le gestionnaire UVM pour l'authentification à l'ouverture de session. Le logiciel Client Security offre les fonctions suivantes :
  - **Protection de stratégie client UVM** : Le logiciel Client Security permet à l'administrateur de la sécurité de définir la stratégie de sécurité client, qui régit le mode d'identification de l'utilisateur client sur le système.  
Si la stratégie indique que l'empreinte digitale est requise pour la connexion et que les empreintes digitales de l'utilisateur ne sont pas enregistrées, ce dernier peut choisir de les enregistrer lors de la connexion. Enfin, si le mot de passe Windows n'est pas enregistré ou est enregistré de façon incorrecte dans UVM, l'utilisateur a la possibilité de fournir le mot de passe Windows correct lors de la connexion.
  - **Protection de la connexion au système par UVM** : Le logiciel Client Security permet à l'administrateur de la sécurité de contrôler l'accès à l'ordinateur via une interface d'ouverture de session. La protection UVM garantit que seuls les utilisateurs reconnus par la stratégie de sécurité peuvent accéder au système d'exploitation.

---

## Les relations entre les mots de passe et les clés

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

## Le mot de passe administrateur

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

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

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

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

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

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

## Les clés publique et privée matérielles

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

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

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

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

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

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

## Les clés publique et privée administrateur

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

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

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

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

---

## Archive ESS

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

## Clés publique et privée utilisateur

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

## Hierarchie de substitution de clés IBM

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

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

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



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

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

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

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

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

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

---

## Fonctions PKI (Public Key Infrastructure) CSS

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

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

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

- **Archive de clés et solutions de reprise.** L'une des fonctions importantes de l'architecture PKI est de permettre la création d'une archive de clés, à partir de laquelle des clés peuvent être restaurées en cas de perte des clés d'origine ou si celles-ci sont endommagées. Le logiciel Client Security IBM offre une interface

permettant de générer une archive pour les clés et les certificats numériques créés à l'aide du sous-système de sécurité intégré IBM et de les restaurer si nécessaire.

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



---

## Partie 2. Informations utilisateur

### Chapitre 2. Instructions destinées à l'utilisateur client

Utilisation de la protection UVM pour la connexion au système	13
Déverrouillage du client	13
Utilitaire de configuration utilisateur	13
Fonctions de l'utilitaire de configuration utilisateur	14
Limites de l'utilitaire de configuration utilisateur sous Windows XP	14
Utilisation de l'utilitaire de configuration utilisateur	15
Utilisation de messagerie électronique et de navigation Web sécurisées	15
Utilisation du logiciel Client Security avec des applications Microsoft	16
Obtention d'un certificat numérique pour des applications Microsoft	16
Transfert de certificats à partir du fournisseur de service cryptographique Microsoft	16
Mise à jour de l'archive de clés pour des applications Microsoft	17
Utilisation du certificat numérique pour des applications Microsoft	18
Configuration des préférences audio UVM	18

### Chapitre 3. IBM Password Manager

Introduction à IBM Password Manager	19
Procédures IBM Password Manager	20
Création de nouvelles entrées	20
Extraction d'entrées	21
Gestion des entrées	21
Exportation des informations de connexion	23

### Chapitre 4. Itinérance des accréditations CSS

Itinérance des accréditations CSS - Configuration requise	25
Configuration d'un serveur itinérant	25
Configuration d'un serveur itinérant	26
Enregistrement de clients sur le serveur itinérant	26
Fin du processus d'enregistrement de client itinérant	27
Enregistrement d'un client itinérant via l'utilitaire d'administration	27
Enregistrement d'un client itinérant via l'utilitaire de configuration utilisateur	27
Enregistrement d'un client itinérant par déploiement global (mode automatique)	27
Exemples de fichier csec.ini	28
Gestion d'un réseau itinérant	29
Autorisation d'utilisateurs	29
Synchronisation des données utilisateur	30
Récupération d'un mot de passe composé perdu dans un environnement itinérant	30
Importation d'un profil utilisateur	30
Importation d'un profil utilisateur via l'utilitaire de configuration utilisateur	31

Importation d'un profil utilisateur via l'utilitaire d'administration	31
Importation d'un profil utilisateur via l'interface de connexion UVM	31
Retrait et réintégration d'utilisateurs dans un réseau itinérant	32
Suppression et réintégration de clients enregistrés dans un réseau itinérant	32
Restriction de l'accès aux clients enregistrés dans un réseau itinérant	33
Restauration d'un réseau itinérant	34
Modification de la paire de clés administrateur	34
Modification du dossier d'archive	34
Utilitaire de chiffrement de fichiers et de dossiers (FFE)	35
IBM Password Manager	35
Termes et définitions relatifs à l'itinérance	35



---

## Chapitre 2. 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
- 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 de connexion UVM doit être activée pour l'ordinateur pour que vous puissiez l'utiliser.

La protection de connexion 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-logon 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 de connexion UVM, exécutez la procédure suivante :

1. Tapez votre nom d'utilisateur et votre mot de passe composé UVM.
2. Sélectionnez le domaine auquel vous êtes connecté.
3. Cliquez sur **OK**.

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

**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.

---

### 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 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.** 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 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. 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, de redéfinir sa configuration de sécurité ou de s'enregistrer sur un serveur itinérant (si l'ordinateur peut être utilisé en tant que client itinérant).

3. Cliquez sur **OK** pour sortir.

Une aide spécifique pour chaque procédure est disponible dans l'aide du logiciel Client Security.

---

## **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.

### 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 de chiffrement 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 CSS vous 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. Ces déplacements vous permettent d'accroître la protection offerte aux clés privées associées aux certificats, car les clés sont désormais stockées en toute sécurité via le sous-système de sécurité intégré IBM et non plus via un logiciel vulnérable.

Les deux types de certificat de sécurité pouvant être déplacés sont les suivants :

- **Certificat utilisateur** : Utilisé afin d'autoriser un utilisateur spécifique. Il est courant de se procurer un certificat utilisateur auprès d'une autorité de certification telle que cssdesk. Une autorité de certification est une entité sécurisée qui contient, émet et publie des certificats. Vous pouvez avoir recours à un certificat utilisateur pour signer et chiffrer vos messages électroniques, ou pour vous connecter à un serveur spécifique.
- **Certificat machine** : Utilisé afin de créer un identificateur unique pour une machine spécifique. Avec ce type de certificat, l'authentification s'effectue sur la base de l'ordinateur utilisé et non pas en fonction de la personne qui l'utilise.

L'outil de transfert de certificats IBM CSS ne permet de déplacer que des certificats Microsoft qui sont marqués comme étant exportables et dont la taille des clés n'excède pas 1024 bits.

Si un utilisateur a besoin de déplacer un certificat machine et qu'il ne détient aucun droit administrateur sur le système, un administrateur peut envoyer un fichier de configuration administrateur qui permettra à l'utilisateur de transférer un certificat sans avoir à spécifier de mot de passe administrateur. La console d'administration, située dans le dossier c:\program files\ibm\security, vous permet de créer un fichier de configuration administrateur.

Pour utiliser l'assistant de transfert de certificats CSS, exécutez la procédure suivante :

1. Cliquez sur **Démarrer > Programmes > Access IBM > Logiciel IBM Client Security > Assistant de transfert de certificats CSS**.

L'écran de bienvenue de l'assistant de transfert de certificats IBM CSS s'affiche.

2. Cliquez sur **Suivant**.
3. Sélectionnez les types de certificats que vous souhaitez transférer, puis cliquez sur **Suivant**. Seuls les certificats marqués comme étant exportables peuvent être transférés dans un espace de stockage de certificats Microsoft.
4. Sélectionnez le certificat à transférer en cliquant sur son nom dans la zone Emis vers de l'interface, puis cliquez sur **Suivant**. Un message s'affiche afin de vous indiquer que le transfert est terminé.

**Remarque** : Le mot de passe administrateur ou un fichier de configuration utilisateur est nécessaire pour le transfert d'un certificat machine.

5. Cliquez sur **OK** pour revenir dans l'assistant de transfert de certificats CSS.

Une fois transférés, les certificats sont associés au fournisseur de service cryptographique du sous-système de sécurité intégré IBM et les clés privées sont protégées par ce sous-système. Toutes les opérations qui utilisent ces clés privées, telles que la création de signatures numériques ou le déchiffrement du courrier électronique, sont effectuées à partir de l'environnement protégé du sous-système de sécurité intégré IBM.

## 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 mettez à jour cette archive 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 3. IBM Password Manager

La présente section fournit une introduction à IBM Password Manager, ainsi que des procédures pas à pas qui expliquent comment exécuter les fonctions courantes d'IBM Password Manager.

---

### Introduction à IBM Password Manager

IBM Password Manager permet de gérer vos informations de connexion sensibles et difficilement mémorisables, telles que les ID utilisateur, les mots de passe et d'autres informations personnelles, grâce à IBM Client Security. IBM Password Manager du logiciel Client Security stocke toutes les informations via le sous-système de sécurité intégré IBM, de sorte que votre stratégie d'authentification utilisateur UVM contrôle l'accès à vos applications sécurisés et sites Web.

Ainsi, plutôt que d'avoir à mémoriser et fournir une foule de mots de passe individuels-- tous soumis à des règles et des dates d'expiration différentes-- il vous suffira de vous rappeler un mot de passe composé unique, de fournir votre empreinte digitale, votre badge de proximité ou n'importe quelle combinaison d'éléments d'identification.

IBM Client Security Password Manager vous permet d'exécuter les fonctions suivantes :

- **Chiffrement de toutes les informations stockées via le sous-système de sécurité intégré IBM**

IBM Password Manager chiffre automatiquement toutes les informations via le sous-système de sécurité intégré IBM. Ainsi, toutes vos informations de mot de passe sensibles sont sécurisées par les clés de chiffrement IBM Client Security.

- **Transfert rapide et facile d'ID utilisateur et de mots de passe à l'aide d'une interface de saisie-et-transfert simple**

Utilisez l'interface de saisie-et-transfert d'IBM Password Manager pour placer des informations directement dans la boîte de dialogue de connexion de votre navigateur Web ou de votre application. Le risque d'erreurs de saisie s'en trouve ainsi réduit et vous pouvez sauvegarder toutes vos informations en toute sécurité via le sous-système de sécurité intégré IBM.

- **Saisie automatique des ID utilisateur et des mots de passe**

IBM Password Manager automatise le processus d'ouverture de session en saisissant automatiquement les informations d'ouverture de session lorsque vous accédez aux sites Web pris en compte dans IBM Password Manager.

- **Exportation des informations de connexion sensibles sur un navigateur sécurisé**

IBM Password Manager vous permet d'exporter vos informations de connexion sensibles de sorte que vous puissiez les porter d'un ordinateur à un autre en toute sécurité. Lorsque vous exportez vos informations de connexion à partir d'IBM Password Manager, un fichier d'exportation protégé par mot de passe est créé et peut être stocké sur un support amovible. Vous pouvez utiliser ce fichier pour accéder à vos informations et mots de passe utilisateur.

- **Génération de mots de passe aléatoires**  
IBM Password Manager permet de générer des mots de passe aléatoires pour chaque site Web ou application. Vous pouvez ainsi accroître la sécurité des données car chaque application disposera d'une protection par mot de passe plus rigoureuse. Les mots de passe aléatoires sont beaucoup plus sûrs que les mots de passe définis par les utilisateurs car l'expérience prouve que la plupart des utilisateurs utilisent des informations personnelles faciles à mémoriser qui sont souvent relativement faciles à deviner.
- **Edition des entrées à l'aide de l'interface Password Manager**  
IBM Password Manager permet d'éditer toutes les entrées de compte et de définir toutes les fonctions de mot de passe facultatives à l'aide d'une interface d'utilisation facile. La gestion des mots de passe et des informations personnelles est ainsi facilitée.
- **Accès à Password Manager à partir de la barre d'icônes du bureau Windows ou à l'aide d'un simple raccourci clavier**  
L'icône IBM Password Manager vous permet d'accéder instantanément à Password Manager, chaque fois que vous souhaitez lui ajouter une autre application, en particulier à partir du Web. Vous pouvez également accéder à chaque fonction Password Manager à l'aide d'un raccourci clavier.
- **Archivage des informations d'ouverture de session**  
Grâce à la fonction d'archivage de Client Security, IBM Password Manager vous permet de restaurer les informations d'ouverture de session à partir d'une archive Client Security afin de les protéger contre une éventuelle défaillance du disque dur ou du système. Pour plus d'informations sur l'archivage des informations, reportez-vous au manuel *Logiciel Client Security - Guide d'utilisation*.

---

## Procédures IBM Password Manager

IBM Client Security Password Manager permet de saisir des informations dans des sites Web et des applications à l'aide de l'interface Password Manager. IBM Password Manager chiffre et sauvegarde les informations saisies dans les zones appropriées à l'aide du sous-système de sécurité intégré IBM. Une fois que les informations sont enregistrées dans Password Manager, ces zones sont automatiquement complétées avec les informations de sécurité chaque fois qu'un accès au site Web ou à l'application est accordé conformément à la stratégie d'authentification utilisateur UVM.

### Création de nouvelles entrées

Pour saisir les informations relatives au mot de passe dans IBM Client Security Password Manager, procédez comme suit :

1. Affichez l'écran d'ouverture de session du site Web ou de l'application.
2. Cliquez à l'aide du bouton droit de la souris sur l'icône **Password Manager** dans la barre des icônes Windows et sélectionnez **Créer**.

**Remarque :** Vous pouvez également accéder à la fonction Créer de Password Manager à l'aide du raccourci clavier **Ctrl+Maj+H**.

3. Tapez les informations destinées à une zone dans la fenêtre Password Manager - Création d'une nouvelle entrée.

**Remarque :** Les informations de cette zone doivent comporter moins de 260 caractères.

4. Si vous ne souhaitez pas que le texte saisi soit affiché, cochez la case **Masquer le texte saisi**.

**Remarque :** Cette case à cocher permet uniquement de contrôler l'affichage du texte dans Password Manager. Une fois le texte intégré au site Web ou à l'application, c'est l'application concernée qui contrôlera les propriétés du texte.

5. Utilisez l'icône "cible" Sélection d'une zone pour transférer le texte de Password Manager dans la zone appropriée du site Web ou de l'application.

**Remarque :** Cette icône permet de copier le texte sans utiliser le presse-papiers de l'ordinateur ou d'autres outils non sécurisés.

6. Répétez les étapes 3 à 5 pour chaque zone, le cas échéant.
7. Cliquez sur l'option de **sauvegarde de nouvelle entrée**.
8. Entrez un nom explicite pour la nouvelle entrée.
9. Cochez la case **Ajouter "Entrée" pour transmission automatique** si vous souhaitez que Password Manager transmette les informations d'ouverture de session après leur extraction.

**Remarque :** Certains sites Web n'utilisent pas la touche Entrée pour transmettre les informations d'ouverture de session. En cas d'échec de l'ouverture de session, désactivez cette fonction.

10. Cliquez sur **Enregistrer...** pour terminer l'opération.

## Extraction d'entrées

L'extraction des mots de passe est très simple avec IBM Client Security Password Manager.

Pour extraire les informations stockées dans IBM Client Security Password Manager, procédez comme suit :

1. Affichez l'écran d'ouverture de session du site Web ou de l'application pour obtenir les informations à extraire.
2. Cliquez deux fois sur l'icône **Password Manager** dans la barre d'icônes Windows. Password Manager remplit alors les zones de l'écran d'ouverture de session avec les informations stockées.

**Remarque :** Vous pouvez également accéder à la fonction Extraire de Password Manager à l'aide du raccourci clavier **Ctrl+Maj+G**.

3. Tapez votre mot de passe composé UVM ou exécutez les opérations d'accès requises par la stratégie d'authentification utilisateur UVM.
4. Si la case **Ajouter "Entrée" pour transmission automatique** n'est pas cochée, cliquez sur le bouton de transmission de l'application ou du site Web.

Si aucune entrée n'est trouvée, une invite vous demande si vous souhaitez créer une nouvelle entrée. Cliquez sur **Oui** pour ouvrir la fenêtre Password Manager - Création d'une nouvelle entrée.

## Gestion des entrées

IBM Client Security Password Manager permet de gérer les informations stockées dans Password Manager. La fenêtre de gestion des entrées de Password Manager permet à l'utilisateur de modifier son ID utilisateur, son mot de passe et les autres informations saisies dans Password Manager qui renseignent les zones d'un site Web ou d'une application.

Pour modifier les informations stockées dans IBM Client Security Password Manager, procédez comme suit :

1. Cliquez à l'aide du bouton droit de la souris sur l'icône **Password Manager** dans la barre des icônes Windows et cliquez sur **Gérer**.

**Remarque :** Vous pouvez également accéder à la fonction Gérer de Password Manager à l'aide du raccourci clavier **Ctrl+Maj+B**.

2. Tapez votre mot de passe composé UVM ou exécutez les opérations d'accès requises par la stratégie d'authentification utilisateur UVM.
3. Modifiez les informations. Choisissez l'une des options suivantes :

- Informations d'entrée

Pour modifier les informations d'entrée, procédez comme suit :

- a. Cliquez à l'aide du bouton droit de la souris sur l'entrée à modifier.
- b. Sélectionnez l'une des actions suivantes :

- Ajouter "Entrée"

Sélectionnez Ajouter "Entrée" pour que vos informations d'entrée soient automatiquement saisies dans le site Web ou l'application. Une icône de contrôle s'affiche en regard de l'option Ajouter "Entrée" lorsque cette fonction est activée.

- Supprimer

Sélectionnez Supprimer pour supprimer totalement une entrée.

- c. Cliquez sur **Enregistrer les modifications**.

- Informations de la zone de saisie

Pour modifier les informations de la zone de saisie, procédez comme suit :

- a. Cliquez à l'aide du bouton droit de la souris sur la zone à modifier.
- b. Sélectionnez l'une des actions suivantes :

- Modifier la zone d'entrée

Sélectionnez Modifier la zone d'entrée pour pouvoir modifier les informations stockées dans cette zone. Pour modifier une zone d'entrée, vous avez le choix entre plusieurs possibilités :

- Création d'une entrée aléatoire

Pour créer une entrée aléatoire, sélectionnez Générer une entrée aléatoire. Password Manager crée des entrées aléatoires comportant 7, 14 ou 127 caractères.

- Modification manuelle d'une zone d'entrée

Pour modifier manuellement une zone d'entrée, sélectionnez Editer et apportez les modifications voulues à la zone.

- Supprimer

Sélectionnez Supprimer pour supprimer totalement une zone d'entrée.

**Remarque :** La modification d'une zone de Password Manager met les informations d'ouverture de session à jour uniquement dans Password Manager. Si vous voulez améliorer la sécurité de vos mots de passe à l'aide de la fonction de génération d'entrée aléatoire de Password Manager, vous devez synchroniser l'application ou le site Web avec le nouveau mot de passe aléatoire généré par cette fonction. Utilisez l'outil de transfert de zones de Password Manager pour transférer le nouveau mot de passe aléatoire dans le formulaire de changement de mot de passe de l'application ou du site Web. Vérifiez que le nouveau mot de passe est admis pour l'application ou le site Web, puis sélectionnez l'option



Enregistrer les modifications dans la fenêtre de gestion des entrées de Password Manager. Il est inutile de recréer l'entrée avec le nouveau mot de passe étant donné que toutes les informations nécessaires ont été conservées.

- c. Cliquez sur **Enregistrer les modifications**.
4. Cliquez sur **Enregistrer les modifications**.

## Exportation des informations de connexion

IBM Password Manager vous permet d'exporter vos informations de connexion sensibles de sorte que vous puissiez les porter d'un ordinateur à un autre en toute sécurité. Lorsque vous exportez vos informations de connexion à partir d'IBM Password Manager, un fichier d'exportation protégé par mot de passe est créé et peut être stocké sur un support amovible. Vous pouvez utiliser ce fichier pour accéder à vos informations et mots de passe utilisateur.

Pour exporter les informations de connexion stockées dans IBM Client Security Password Manager, procédez comme suit :

1. Cliquez à l'aide du bouton droit de la souris sur l'icône **Password Manager** dans la barre des icônes Windows et cliquez sur **Gérer**.

**Remarque :** Vous pouvez également accéder à la fonction Gérer de Password Manager à l'aide du raccourci clavier **Ctrl+Maj+B**.

2. Tapez votre mot de passe composé UVM ou exécutez les opérations d'accès requises par la stratégie d'authentification utilisateur UVM.
3. Cliquez sur **Exportation**. La fenêtre de sauvegarde en tant que s'affiche. Elle contient le chemin par défaut et le nom de fichier PwMgrExportReader.
4. Sélectionnez l'emplacement de sauvegarde du fichier d'exportation.
5. Cliquez sur **Enregistrer** pour accepter l'emplacement et le nom de fichier spécifiés. Un écran vous invite à définir un mot de passe composé pour votre fichier d'exportation.
6. Définissez un mot de passe composé pour votre fichier d'exportation et cliquez sur **OK**. Ce mot de passe composé sera requis pour accéder aux données exportées. Un message s'affiche pour vous indiquer que l'exportation a abouti.
7. Cliquez sur **OK**.
8. Fermez IBM Password Manager.
9. Récupérez le fichier d'exportation créé à partir de l'emplacement que vous avez spécifié et copiez-le sur un support amovible.

Avant de pouvoir ouvrir ce fichier sur un autre ordinateur, vous serez invité à indiquer le mot de passe composé d'exportation et que vous avez défini au cours de la procédure décrite précédemment. IBM Password Manager affiche vos informations sensibles dans un programme de lecture sécurisé. Ces informations ne peuvent pas être imprimées ni être sauvegardées sur le disque dur de l'ordinateur. Cliquez sur **OK** pour fermer le fichier du programme de lecture d'exportation.



---

## Chapitre 4. Itinérance des accréditations CSS

La fonction d'itinérance des accréditations du logiciel IBM Client Security permet d'utiliser les accréditations d'un utilisateur UVM sur tous les ordinateurs compatibles ESS d'un réseau. Ce réseau, appelé réseau itinérant, améliore la souplesse de travail des utilisateurs et augmente la disponibilité des applications en permettant aux utilisateurs de travailler facilement à partir de n'importe quel ordinateur du réseau.

---

### Itinérance des accréditations CSS - Configuration requise

un réseau itinérant d'accréditation CSS se compose des éléments suivants :

- Serveur itinérant
- Clients itinérants
- Unité réseau mappée partagée destinée au stockage des archives utilisateur UVM

**Remarque :** Le serveur itinérant et les clients itinérants autorisés sont simplement des ordinateurs compatibles ESS, dotés de mots de passe administrateur établis, et sur lesquels est installé le logiciel IBM Client Security 5.1 ou suivant.

---

### Configuration d'un serveur itinérant

Pour configurer un réseau itinérant d'accréditation CSS, vous devez désigner un ordinateur comme le *serveur* itinérant (qui est appelé système A). Une fois enregistrés par le serveur itinérant, les autres ordinateurs deviennent des *clients* autorisés enregistrés dans CSS. (Le premier client enregistré est appelé système B.)

Il n'y a pas d'exigence spéciale concernant l'ordinateur qui est désigné comme serveur itinérant. Vous pouvez utiliser n'importe quel ordinateur qui fera partie du réseau itinérant. Le serveur itinérant est simplement l'ordinateur désigné pour établir quels sont les ordinateurs "sécurisés" vis-à-vis du réseau itinérant. Une fois qu'un ordinateur est enregistré dans le réseau itinérant, il est considéré par tous les autres ordinateurs du réseau comme étant sécurisé.

La configuration d'un réseau itinérant s'effectue en deux étapes :

1. Configuration du serveur itinérant en définissant les clés, les archives et les utilisateurs itinérants.
2. Enregistrement d'un client initial (système B) et de tous les autres ordinateurs en tant que clients itinérants dans le réseau itinérant.

Le serveur itinérant définit le réseau itinérant et lance l'enregistrement des clients itinérants, mais le point central de ce type de réseau est l'unité réseau mappée sur laquelle les archives utilisateur sont stockées. C'est dans cette archive que sont stockées toutes les mises à jour des accréditations des utilisateurs. Cette archive ne doit *en aucun cas* être placée sur le serveur itinérant ou sur l'un des clients itinérants. Après avoir initialisé les clients CSS, le serveur itinérant se comporte comme n'importe quel autre client enregistré dans CSS.

## Configuration d'un serveur itinérant

Pour configurer un serveur itinérant, procédez comme suit :

1. Sur l'ordinateur désigné, démarrez la console d'administration et cliquez sur **Configuration de l'itinérance des accréditations**. Ou, si l'ordinateur est déjà configuré pour l'itinérance, sélectionnez **Reconfigurer ce système en tant que serveur itinérant CSS** et cliquez sur **Suivant**.
2. Créez le dossier c:\roaming sur l'ordinateur désigné comme serveur itinérant.
3. Démarrez la console d'administration et cliquez sur **Configuration de l'itinérance des accréditations**.
4. Sélectionnez **Configurer ce système en tant que serveur itinérant CSS** et cliquez sur **Suivant**.
5. Cliquez sur **Configurer**.
6. Sélectionnez **Créer de nouvelles clés d'archive** et tapez un nom dans la zone Dossier des clés d'archive correspondant au dossier stocké dans c:\roaming .
7. Choisissez d'utiliser une paire de clés existante ou de créer une nouvelle paire de clés, puis cliquez sur **Suivant**.
8. Entrez le nom du dossier d'archive, puis cliquez sur **Suivant**.

**Remarque :** Le dossier d'archive et le dossier des clés doivent être accessibles aux autres ordinateurs enregistrés pour l'itinérance (clients itinérants). Le répertoire c:\roaming doit être une unité réseau mappée.

Si l'archive contient des fichiers, la page suivante de l'assistant vous invite à indiquer la façon dont les fichiers devront être gérés.

9. Cliquez sur **Terminer**.

## Enregistrement de clients sur le serveur itinérant

Pour enregistrer un client itinérant sur le serveur itinérant, procédez comme suit :

1. Une fois la configuration du serveur itinérant terminée, l'écran Configuration du réseau itinérant d'accréditation s'affiche. Sélectionnez **Activer l'enregistrement du client**, puis cliquez sur **Suivant**.
2. Indiquez le nom de l'utilisateur du système B possédant les droits d'administrateur qui effectuera l'enregistrement du client.
3. Tapez le mot de passe qui devra être utilisé par cet utilisateur, puis confirmez-le. (Ne confondez pas cette procédure avec l'accord du droit d'utilisation d'UVM à un utilisateur, procédure qui a lieu ultérieurement).
4. Pour pouvoir enregistrer le client via l'utilitaire de configuration utilisateur, vous devez créer un fichier de configuration administrateur pour cet utilisateur. Cette procédure génère un fichier qui est unique pour cet utilisateur. Stockez-le dans un emplacement accessible à cet utilisateur et au système B.

**Remarque :** Il n'est pas nécessaire de générer ce fichier si vous enregistrez un client via l'utilitaire d'administration.

5. Cliquez sur **Suivant**.
6. Si vous avez créé un fichier de configuration administrateur, enregistrez-le dans un emplacement accessible à l'utilisateur et au système B.

Une fois que vous avez exécuté les procédures indiquées précédemment, votre serveur itinérant est configuré. Avant de pouvoir utiliser le réseau itinérant, vous devez avoir exécuté et terminé l'enregistrement sur chaque client itinérant.

---

## Fin du processus d'enregistrement de client itinérant

Une fois que la liste des systèmes sécurisés a été enregistrée sur le serveur itinérant, vous devez exécuter l'une des procédures ci-après sur les systèmes client. Pour qu'un client itinérant puisse être enregistré, vous devez avoir démarré le serveur itinérant et avoir établi une connexion à l'archive.

### Enregistrement d'un client itinérant via l'utilitaire d'administration

Pour enregistrer un client itinérant via l'utilitaire d'administration, procédez comme suit :

1. Cliquez sur **Configuration de clé**.
2. Cliquez sur **Non** lorsque le système vous demande si vous souhaitez restaurer les clés à partir de l'archive.
3. Sélectionnez Enregistrer ce système auprès d'un serveur itinérant CSS et cliquez sur **Suivant**.
4. Indiquez l'emplacement d'archive créé par le système A, tapez le mot de passe d'enregistrement système défini pour cet utilisateur sur le système A et cliquez sur **Suivant**.

La procédure d'enregistrement dure environ une minute.

### Enregistrement d'un client itinérant via l'utilitaire de configuration utilisateur

Pour enregistrer un client itinérant via l'utilitaire de configuration utilisateur, procédez comme suit :

1. Sous l'onglet Configuration utilisateur, cliquez sur **Enregistrement auprès d'un serveur itinérant CSS**.
2. Sélectionnez le fichier de configuration administrateur généré sur le système A, tapez le mot de passe d'enregistrement système défini pour cet utilisateur sur le système A et cliquez sur **Suivant**.
3. Indiquez l'emplacement d'archive créé par le système A et cliquez sur **Suivant**.

La procédure d'enregistrement dure environ une minute.

### Enregistrement d'un client itinérant par déploiement global (mode automatique)

Pour enregistrer un client itinérant en mode automatique par déploiement global, procédez comme suit :

1. Créez le fichier `csec.ini`. Pour en savoir plus sur la création d'un fichier CSS `.ini`, consultez le manuel *Logiciel Client Security - Guide d'installation*.
2. Ajoutez `"enableroaming=1"` dans la section `csssetup` du fichier. Vous indiquez ainsi que l'ordinateur doit être enregistré comme client itinérant.
3. Dans la même section, ajoutez l'entrée `"username=OPTION"`. Trois options sont possibles pour cette valeur :
  - **Option 1 : La chaîne "[promptcurrent]" - crochets inclus.** Cette désignation doit être utilisée si un fichier `.dat` pour l'utilisateur actuellement connecté a été généré sur le serveur itinérant et si cet utilisateur connaît le mot de passe d'enregistrement système. Cette option provoque l'affichage d'une fenêtre en incrustation qui invite l'utilisateur à taper le mot de passe d'enregistrement système (`sysregpwd`) avant le déploiement.

- **Option 2 : 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. La gestion du paramètre sysregpwd s'effectue comme indiqué dans l'étape suivante.
  - **Option 3 : 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 itinérant. Dans ce cas, la gestion du paramètre sysregpwd sera effectuée comme indiqué dans l'étape suivante.
4. 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 d'enregistrement système associé à l'utilisateur en cours (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 l'ordinateur à l'archive définie par le serveur itinérant. Cette archive est désignée dans le fichier csec.ini . Le dossier de clés qui a été défini sur le serveur itinérant CSS est également mentionné dans le fichier csec.ini.
  6. Chiffrez le fichier csec.ini à l'aide de la console d'administration.

### Exemples de fichier csec.ini

Les exemples ci-après représentent un échantillon de fichier csec.ini, et illustrent la façon dont ce fichier change en fonction de l'option d'itinérance d'accréditation sélectionnée. Ces options sont les suivantes :

- **Aucune valeur d'itinérance.** Ce fichier de base n'est pas activé pour l'itinérance des accréditations.
- **Itinérance option 1.** Ce fichier est activé pour l'itinérance à l'aide de l'option 1 pour l'enregistrement client. L'utilisateur en cours doit taper le mot de passe d'enregistrement système avant le déploiement.
- **Itinérance option 2.** Ce fichier est activé pour l'itinérance à l'aide de l'option 2 pour l'enregistrement client. L'utilisateur en cours doit indiquer l'ID utilisateur et le mot de passe d'enregistrement système spécifiés dans le fichier .ini.
- **Itinérance option 3.** Ce fichier est activé pour l'itinérance à l'aide de l'option 3 pour l'enregistrement client. L'utilisateur est mentionné dans le fichier .ini. Le mot de passe d'enregistrement système pour l'utilisateur désigné doit être indiqué dans le fichier .ini.

Exemples de quatre fichiers CSEC.INI distincts :

[CSSSetup]	Option 1 [CSSSetup]	Option 2 [CSSSetup]	Option 3 [CSSSetup]
suppw=bootup	suppw=bootup	suppw=bootup	suppw=bootup
hwpw=1111111	hwpw=1111111	hwpw=1111111	hwpw=1111111
newkp=1	newkp=1	newkp=1	newkp=1
keysplit=1	keysplit=1	keysplit=1	keysplit=1
kpl=c:\jgk	kpl=c:\\computer name\jgk, où la paire de clés a été placée sur le serveur itinérant par l'ordinateur	kpl=c:\\computer name\jgk, où la paire de clés a été placée sur le serveur itinérant par l'ordinateur	kpl=c:\\computer name\jgk, où la paire de clés a été placée sur le serveur itinérant par l'ordinateur

kal=c:\jgk\archive pub= c:\jk\admin.key pri= c:\jk\private1.key wiz=0	kal=c:\\computer name\archive, où l'archive a été placée sur le serveur itinérant par l'ordinateur pub= c:\jk\admin.key pri= c:\jk\private1.key wiz=0	kal=c:\\computer name\archive, où l'archive a été placée sur le serveur itinérant par l'ordinateur pub= c:\jk\admin.key pri= c:\jk\private1.key wiz=0	kal=c:\\computer name\archive, où l'archive a été placée sur le serveur itinérant par l'ordinateur pub= c:\jk\admin.key pri= c:\jk\private1.key wiz=0
clean=0	<b>enableroaming=1</b> <b>username=[promptcurrent]</b>  clean=0	<b>enableroaming=1</b> <b>username=[current]</b> <b>sysregpwd=12345678</b> clean=0	<b>enableroaming=1</b> <b>username=joseph</b> <b>sysregpwd=12345678</b> clean=0
[UVMEnrollment] enrollall=0 enrollusers=1 user1=joseph user1uvmpw=q1234r user1winpw= user1domain=0 user1ppchange=0 user1ppexppolicy=0 user1ppexppdays=184	[UVMEnrollment] enrollall=0 enrollusers=1 user1=joseph user1uvmpw=q1234r user1winpw= user1domain=0 user1ppchange=0 user1ppexppolicy=0 user1ppexppdays=184	[UVMEnrollment] enrollall=0 enrollusers=1 user1=joseph user1uvmpw=q1234r user1winpw= user1domain=0 user1ppchange=0 user1ppexppolicy=0 user1ppexppdays=184	[UVMEnrollment] enrollall=0 enrollusers=1 user1=joseph user1uvmpw=q1234r user1winpw= user1domain=0 user1ppchange=0 user1ppexppolicy=0 user1ppexppdays=184
[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

---

## Gestion d'un réseau itinérant

L'administrateur réseau d'un réseau itinérant doit autoriser les utilisateurs et gérer les accès client et utilisateur au réseau. Cela peut donner lieu à des opérations d'importation d'un profil utilisateur, de synchronisation de données utilisateur ou d'ajout et de retrait d'utilisateurs facilement et rapidement sur un réseau itinérant CSS. Cela peut également impliquer de restaurer le réseau itinérant, modifier la paire de clés administrateur ou modifier l'emplacement de l'archive.

### Autorisation d'utilisateurs

Une fois les procédures indiquées précédemment terminées, le réseau itinérant d'accréditation CSS est configuré et les clients itinérants sont enregistrés pour l'itinérance. Il est à présent possible d'autoriser les utilisateurs via l'utilitaire d'administration.

## Synchronisation des données utilisateur

Les données de chaque utilisateur sont stockées dans l'emplacement de l'archive. Une copie de ces données est également stockée localement sur chaque ordinateur utilisé par l'utilisateur. En cas de modifications (telles que l'obtention d'un certificat ou la modification d'un mot de passe composé), les données locales sont mises à jour. Si l'ordinateur est connecté à l'archive, les données de l'utilisateur sont également mises à jour. Lorsque l'utilisateur ouvre une session sur un autre ordinateur, les mises à jour sont automatiquement téléchargées vers cet ordinateur, à condition que ce dernier soit connecté à l'archive.

La connexion à l'archive n'est pas toujours garantie. Par conséquent, il arrive que les données utilisateur soient incohérentes entre un ordinateur du réseau et l'archive. Si les données d'un utilisateur sont modifiées sur un ordinateur qui n'est pas connecté à l'archive, ces modifications ne sont pas prises en compte dans l'archive et, par conséquent, ne le sont pas non plus sur les autres ordinateurs. Une fois que l'ordinateur est connecté à l'archive, les modifications sont transmises à l'archive et à tous les autres ordinateurs connectés. Cependant, si des modifications sont effectuées sur un autre ordinateur qui était connecté à l'archive avant que le premier ordinateur contenant les modifications ne le soit lui-même, des incohérences de données non rectifiables interviennent. Les données de l'archive contiennent des modifications qui sont absentes sur le premier ordinateur, alors que ce dernier contient des modifications qui sont elles-mêmes absentes de l'archive. Dans ce cas, l'utilisateur est averti des deux différentes configurations et est invité à choisir la configuration qu'il souhaite conserver (configuration locale ou configuration de l'archive). Les modifications de configuration qui ne sont pas sélectionnées sont perdues. Il est donc important de s'assurer que toutes les modifications apportées à une configuration utilisateur sont retransmises à l'archive avant d'effectuer des modifications sur tout autre ordinateur.

## Récupération d'un mot de passe composé perdu dans un environnement itinérant

Lorsqu'un mot de passe composé est perdu ou oublié, l'administrateur peut réinitialiser le mot de passe composé utilisateur sur le serveur itinérant ou sur n'importe quel client enregistré. Cette modification est mise à jour sur tous les systèmes du réseau, *sauf* sur ceux dotés de la protection de connexion UVM sécurisée et sur lesquels l'utilisateur a procédé à des importations. Dans ces cas-là, la mise à jour du mot de passe composé n'est *pas* prise en compte sur l'ordinateur. Pour accéder à l'ordinateur, l'utilisateur doit alors disposer d'un fichier de remplacement de mot de passe et exécuter la procédure de remplacement de mot de passe.

## Importation d'un profil utilisateur

Vous pouvez importer un profil utilisateur sur un autre ordinateur du réseau itinérant via l'utilitaire d'administration, l'utilitaire de configuration utilisateur ou l'interface de connexion UVM. Si vous souhaitez importer un utilisateur qui ne dispose d'aucun compte utilisateur sur l'autre ordinateur, vous devez créer un compte utilisateur Windows via le panneau de configuration Windows.

**Remarque :** Pour pouvoir importer un utilisateur sur un réseau itinérant, l'utilisateur doit être autorisé sur un autre ordinateur du réseau itinérant.



## Importation d'un profil utilisateur via l'utilitaire de configuration utilisateur

Pour importer un profil utilisateur sur un autre ordinateur du réseau itinérant à l'aide de l'utilitaire de configuration utilisateur, connectez-vous au système à l'aide de l'ID utilisateur que vous souhaitez importer, puis cliquez sur **Démarrer > Programmes > Access IBM > Logiciel IBM Client Security > Modification des paramètres de sécurité**, puis sur **Importation d'une configuration existante à partir d'une archive** sous l'onglet Configuration utilisateur.

## Importation d'un profil utilisateur via l'utilitaire d'administration

Pour importer un profil utilisateur sur un autre ordinateur du réseau itinérant via l'utilitaire d'administration, sélectionnez l'utilisateur et cliquez sur **Autorisation**. Cliquez sur **Oui** lorsque le système vous demande si vous souhaitez importer l'utilisateur à partir de l'archive.

## Importation d'un profil utilisateur via l'interface de connexion UVM

Vous pouvez importer un profil utilisateur sur un autre ordinateur du réseau itinérant via l'interface de connexion UVM. Cette procédure commence à partir de l'écran de connexion UVM. Si un utilisateur n'est pas encore autorisé à utiliser UVM sur un système donné du réseau, une boîte de message s'affiche pour demander à l'utilisateur s'il souhaite être importé à partir de l'archive.

### Remarques :

1. Si vous souhaitez importer un utilisateur qui ne dispose d'aucun compte utilisateur sur l'autre ordinateur, vous devez créer un compte utilisateur Windows via le panneau de configuration Windows avant de pouvoir poursuivre.
2. Le répertoire doit être une unité réseau mappée pour que vous puissiez accéder à l'archive sur le serveur itinérant.

Pour importer un profil utilisateur sur un autre ordinateur du réseau itinérant (doté de Windows 2000) via la GINA UVM, procédez comme suit :

1. Entrez le nom utilisateur et le mot de passe composé UVM de l'utilisateur que vous souhaitez importer. Un message vous invite à indiquer si vous voulez importer le profil utilisateur à partir de l'archive.
2. Répondez **Oui**, puis cliquez sur **OK**.
3. Si l'emplacement de l'archive se trouve sur une unité réseau, répondez **Oui** à l'invite spécifiant qu'un partage réseau doit être spécifié.
4. Entrez votre mot de passe Windows à l'écran de connexion Windows. Le système vous invite à indiquer le chemin de l'archive.
5. Entrez le chemin d'accès à l'archive.
6. Entrez le nom utilisateur et le mot de passe appropriés.
7. Cliquez sur **OK**. Si l'opération aboutit, un message vous indique que le profil a été importé.

Pour importer un profil utilisateur sur un autre ordinateur du réseau itinérant (doté de Windows XP) via la GINA UVM, procédez comme suit :

1. Entrez le nom utilisateur et le mot de passe composé UVM de l'utilisateur que vous souhaitez importer. Un message vous invite à indiquer si vous voulez importer le profil utilisateur à partir de l'archive.
2. Répondez **Oui**, puis cliquez sur **OK**.

3. Si l'emplacement de l'archive se trouve sur une unité réseau, répondez **Oui** à l'invite spécifiant qu'un partage réseau doit être spécifié.
4. A l'invite de mappage d'unité réseau Windows, entrez le chemin d'accès à l'archive.
5. Cliquez sur **Terminer**.
6. Entrez le nom utilisateur et le mot de passe appropriés et cliquez sur **OK**. Si l'opération aboutit, un message vous indique que le profil a été importé.

**Remarque :** Pour pouvoir importer un utilisateur sur un réseau itinérant, l'utilisateur doit être autorisé sur un autre ordinateur du réseau itinérant.

Une fois le profil utilisateur importé, l'authentification auprès d'UVM est basée sur la stratégie de sécurité de l'ordinateur. Les conditions de sécurité requises pour cet ordinateur doivent être remplies pour que cet utilisateur puisse se connecter.

## Retrait et réintégration d'utilisateurs dans un réseau itinérant

Pour retirer un utilisateur d'un serveur itinérant, l'administrateur réseau doit exécuter la procédure suivante à partir de la console d'administration :

1. Démarrer l'utilitaire de console d'administration et entrer le mot de passe administrateur.
2. Cliquer sur **Configuration de l'itinérance des accréditations**.
3. Sélectionner **Supprimer des utilisateurs du gestionnaire UVM et du réseau itinérant d'accréditation**, puis cliquer sur **Suivant**. Répéter cette opération autant de fois que nécessaire.
4. Sélectionner l'utilisateur à retirer et cliquer sur **Supprimer**.

**Remarque :** La suppression d'un utilisateur sur le réseau entraîne la perte irréversible de toutes les accréditations qui lui sont associées.

Les utilisateurs supprimés ne peuvent pas être autorisés à utiliser UVM et le réseau itinérant tant qu'ils ne sont pas réintégré par le réseau administrateur.

Pour réintégrer un utilisateur sur un serveur itinérant, l'administrateur réseau doit exécuter la procédure suivante à partir de la console d'administration :

1. Démarrer l'utilitaire de console et entrer le mot de passe administrateur.
2. Cliquer sur **Configuration de l'itinérance des accréditations**.
3. Sélectionner **Réintégrer des utilisateurs supprimés** et cliquer sur **Suivant**.
4. Sélectionner l'utilisateur à réintégrer et cliquer sur **Réintégrer**. Répéter cette opération autant de fois que nécessaire.

Une fois que l'utilisateur est réintégré, il peut être de nouveau autorisé à utiliser UVM. Le fait de réintégrer un utilisateur n'entraîne pas d'autorisation automatique pour l'utilisation d'UVM.

## Suppression et réintégration de clients enregistrés dans un réseau itinérant

Pour supprimer un client enregistré d'un serveur itinérant, l'administrateur réseau doit exécuter la procédure suivante à partir de la console d'administration :

1. Démarrer l'utilitaire de console et entrer le mot de passe administrateur.
2. Cliquer sur **Configuration de l'itinérance des accréditations**.
3. Sélectionner **Supprimer des clients enregistrés du réseau itinérant d'accréditation**, puis cliquer sur **Suivant**.

4. Sélectionner le système à retirer et cliquer sur **Supprimer**. Répéter cette opération autant de fois que nécessaire.

**Remarque :** La suppression d'un client sur le réseau entraîne la perte irréversible de toutes les accréditations basées machine qui lui sont associées.

Les clients supprimés ne peuvent pas être enregistrés avec le serveur itinérant du réseau tant qu'ils ne sont pas réintégré par l'administrateur réseau.

Pour réintégrer un client enregistré sur un réseau itinérant, l'administrateur réseau doit exécuter la procédure suivante à partir de la console d'administration :

1. Démarrer l'utilitaire de console et entrer le mot de passe administrateur.
2. Cliquer sur **Configuration de l'itinérance des accréditations**.
3. Sélectionner **Réintégrer des clients supprimés** et cliquer sur **Suivant**.
4. Sélectionner le client à réintégrer et cliquer sur **Réintégrer**. Répéter cette opération autant de fois que nécessaire.

Une fois que le client est réintégré, il peut être à nouveau enregistré sur le serveur itinérant. Le fait de réintégrer un client n'entraîne pas son ré-enregistrement automatique.

**Remarque :** Il se peut que les utilisateurs dont les accréditations figuraient sur le système au moment de la suppression du client doivent importer à nouveau leurs accréditations.

## Restriction de l'accès aux clients enregistrés dans un réseau itinérant

Il peut arriver qu'un administrateur réseau souhaite permettre à certains utilisateurs d'accéder à un client enregistré spécifique tout en interdisant cet accès à d'autres utilisateurs.

Pour gérer les droits d'accès des utilisateurs, l'administrateur réseau doit exécuter la procédure suivante à partir de la console d'administration :

1. Démarrer l'utilitaire de console et entrer le mot de passe administrateur.
2. Cliquer sur **Configuration de l'itinérance des accréditations**.
3. Sélectionner **Gérer les accès utilisateur aux clients enregistrés** et cliquer sur **Suivant**.
4. Sélectionner le client enregistré à gérer dans la zone **Sélection d'un système du réseau itinérant CSS**. Les utilisateurs autorisés et non autorisés figurent dans les deux boîtes à liste.
5. Exécutez l'une des opérations suivantes :
  - Pour restreindre l'accès d'un utilisateur, sélectionnez celui-ci dans la liste **Utilisateurs autorisés** et cliquez sur **Restreindre**. Répétez cette opération autant de fois que nécessaire.
  - Pour accorder l'accès à un utilisateur, sélectionnez celui-ci dans la liste **Utilisateurs non autorisés** et cliquez sur **Autoriser**. Répétez cette opération autant de fois que nécessaire.

Les fonctions de gestion des accès du réseau itinérant requièrent la création d'un nouveau dossier dans l'archive. Le nouveau dossier, appelé Protected, doit être accessible en écriture par l'administrateur réseau et accessible en lecture seulement

par les autres utilisateurs. Si des utilisateurs disposent d'un accès en écriture sur ce dossier, ils peuvent manuellement réintégrer leurs systèmes ou se réintégrer eux-mêmes.

## Restauration d'un réseau itinérant

En cas de défaillance logicielle ou matérielle, il peut être nécessaire d'effectuer une restauration du réseau itinérant. Si le serveur itinérant est endommagé ou que les données utilisées par CSS sont endommagées sur un client enregistré, vous devez restaurer les données via l'utilitaire d'administration de la même manière que vous le feriez dans un environnement non itinérant. Si le sous-système de sécurité intégré IBM d'un client enregistré est défectueux ou vidé, vous devez enregistrer de nouveau le client sur le serveur itinérant. Aucune autre action n'est requise.

## Modification de la paire de clés administrateur

Il n'est pas recommandé de modifier la paire de clés administrateur dans un réseau itinérant, car cela implique le ré-enregistrement de chaque client auprès du serveur itinérant.

Cependant, si vous êtes amené à modifier la paire de clés administrateur dans un réseau itinérant, vous devez exécuter les étapes suivantes pour que cette modification soit prise en compte sur tous les ordinateurs du réseau.

1. Sur le serveur itinérant, modifiez la paire de clés administrateur via l'utilitaire d'administration.
2. Enregistrez de nouveau tous les clients du réseau.
3. Choisissez de conserver les fichiers existants chaque fois que le système vous demande si vous souhaitez les conserver.

## Modification du dossier d'archive

La méthode utilisée pour modifier le dossier d'archive dans un environnement itinérant est légèrement différente de celle utilisée dans un environnement non itinérant car chaque ordinateur du réseau accède au même emplacement d'archive.

Pour modifier le dossier d'archive dans un réseau itinérant, procédez comme suit :

1. Copiez les fichiers de l'ancien dossier d'archive vers le nouveau en procédant comme suit :
  - a. Démarrez l'utilitaire d'administration et entrez le mot de passe administrateur.
  - b. Cliquez sur **Configuration de clé**.
  - c. Sélectionnez Modification de l'emplacement d'une archive et cliquez sur **Suivant**.
  - d. Indiquez le nouveau dossier de l'archive, puis cliquez sur **Suivant**.
  - e. Cliquez sur **Oui** lorsque vous êtes invité à copier tous les fichiers de l'ancien dossier dans le nouveau dossier.
2. Effectuez la mise à jour de tous les autres ordinateurs du réseau afin qu'ils utilisent le nouveau dossier d'archive, en procédant comme suit :
  - a. Démarrez l'utilitaire d'administration et entrez le mot de passe administrateur.
  - b. Cliquez sur **Configuration de clé**.
  - c. Sélectionnez Modification de l'emplacement d'une archive et cliquez sur **Suivant**.
  - d. Indiquez le nouveau dossier de l'archive, puis cliquez sur **Suivant**.

- e. Cliquez sur **Non** lorsque vous êtes invité à copier tous les fichiers de l'ancien dossier vers le nouveau dossier.

---

## Utilitaire de chiffrement de fichiers et de dossiers (FFE)

L'utilitaire de chiffrement de fichiers et de dossiers n'est pas affecté par l'environnement itinérant. Cependant, les dossiers protégés sont gérés ordinateur par ordinateur. Ainsi, si un dossier est protégé par l'utilisateur A sur un système A, un dossier portant le même nom sur le système B (le cas échéant) n'est pas protégé si l'utilisateur ne le protège pas de façon effective sur le système B.

---

## IBM Password Manager

Tous les mots de passe protégés via IBM Password Manager sont disponibles sur tous les ordinateurs du réseau itinérant.

---

## Termes et définitions relatifs à l'itinérance

Il est utile de connaître les termes suivants lorsque l'on aborde les concepts et procédures de configuration d'un réseau itinérant :

**enregistrement de client itinérant**

Procédure consistant à enregistrer un ordinateur auprès du serveur itinérant.

**clients itinérants**

Tous les ordinateurs sécurisés du réseau itinérant.

**Serveur itinérant**

Ordinateur ESS utilisé pour initier le réseau itinérant.

**mot de passe d'enregistrement de client itinérant**

Mot de passe utilisé pour enregistrer l'ordinateur auprès du serveur itinérant.



---

## Partie 3. Informations administrateur

<b>Chapitre 5. Utilisation du logiciel Client Security</b>	39	<b>Chapitre 8. Gestion d'une stratégie UVM.</b>	55
Exemple 1 - Un client Windows 2000 et un client Windows XP utilisant tous deux Outlook Express	39	Edition d'une stratégie UVM	55
Exemple 2 - Deux clients CSS Windows 2000 utilisant Lotus Notes	40	Sélection d'objet	56
Exemple 3 - Plusieurs clients CSS Windows 2000 gérés par Tivoli Access Manager et utilisant Netscape pour le courrier électronique	41	Eléments d'authentification	57
		Utilisation de l'éditeur de stratégie UVM	58
		Edition et utilisation d'une stratégie UVM	59
<b>Chapitre 6. Autorisation d'utilisateurs</b>	43	<b>Chapitre 9. Autres fonctions de l'utilitaire d'administration</b>	61
Authentification pour les utilisateurs client	43	Utilisation de la console d'administration	61
Eléments d'authentification	43	Modification de l'emplacement de l'archive de clés	62
Opérations préalables à l'autorisation d'utilisateurs	44	Modification de la paire de clés d'archive	62
Autorisation d'utilisateurs	44	Restauration de clés à partir d'une archive	63
Suppression d'utilisateurs	45	Conditions requises pour la restauration de clé	64
Création de nouveaux utilisateurs	46	Scénarios de restauration	64
		Remplacement de la carte principale	64
		Remplacement du système	65
		Remplacement de l'unité de disque dur	65
<b>Chapitre 7. Fonctions UVM supplémentaires</b>	47	Réinitialisation du compteur d'échecs d'authentification	66
Authentification Windows améliorée	47	Modification des paramètres de Tivoli Access Manager	66
Planification de la la protection de connexion UVM	47	Configuration des paramètres de Tivoli Access Manager sur un client	66
Configuration de la protection de connexion UVM	47	Régénération de la mémoire cache locale	67
Récupération d'un mot de passe composé UVM	48	Modification du mot de passe administrateur	67
Protection de l'authentification améliorée pour les utilisateurs Lotus Notes	49	Affichage des informations relatives au logiciel Client Security	68
Activation et configuration de la protection de connexion UVM pour un ID utilisateur Lotus Notes	49	Désactivation du sous-système de sécurité intégré IBM	68
Utilisation de la protection de connexion UVM dans Lotus Notes	50	Activation du sous-système de sécurité intégré IBM et définition d'un mot de passe administrateur	69
Configuration de la protection de connexion UVM dans Lotus Notes	50	Activation du support Entrust	69
Re-définition de votre mot de passe Lotus Notes	50		
Désactivation de la protection de connexion UVM pour un ID utilisateur Lotus Notes	50		
Configuration de la protection de connexion UVM pour un autre ID utilisateur Lotus Notes	51		
Activation des applications conformes au module PKCS 11	51		
Installation du module PKCS 11 de la puce de sécurité intégrée IBM	51		
Sélection du sous-système de sécurité intégré IBM pour générer un certificat numérique	52		
Mise à jour de l'archive de clés	52		
Utilisation du certificat numérique du module PKCS 11	52		
Réinitialisation d'un mot de passe composé	52		
Réinitialisation à distance d'un mot de passe composé	53		
Réinitialisation manuelle d'un mot de passe composé	53		
Enregistrement des empreintes digitales de l'utilisateur	53		





---

## Chapitre 5. 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 CSS. Utilisez les exemples fournis ci-après pour planifier votre stratégie et votre configuration Client Security. En environnement Windows 2000 et Windows XP, par exemple, les utilisateurs peuvent définir une protection UVM pour la connexion système qui empêche la connexion d'utilisateurs non autorisés sur le client CSS.

---

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

Dans cet exemple, un client CSS (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 sera éditée et utilisée sur chaque client.

Pour configurer la sécurité client, procédez comme suit :

1. Installez le logiciel Client Security 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/us/security/secdownload.html>.

3. Configurez l'authentification utilisateur dans UVM pour chaque client. Exécutez les opérations suivantes :
  - a. Autorisez des utilisateurs pour UVM en leur affectant un mot de passe composé UVM. 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 sur le client 1. Au moins un utilisateur doit enregistrer ses empreintes digitales sur le client 2.

**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 Windows

- Acquisition d'un certificat numérique
  - Utilisation d'une signature numérique pour Outlook Express
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 CSS.

Les utilisateurs clients peuvent à présent exécuter les tâches suivantes :

- Utilisation de la protection UVM pour verrouiller et déverrouiller Windows.
- Inscription à un certificat numérique et sélection du sous-système de sécurité intégré 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 CSS Windows 2000 utilisant Lotus Notes

Dans cet exemple, les deux clients CSS (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 de connexion UVM pour la connexion système. L'administrateur a décidé d'éditer la stratégie UVM sur le client 1 et de la copier sur le client 2.

Pour configurer la sécurité client, procédez comme suit :

1. Installez le logiciel Client Security sur les clients 1 et 2. Etant donné que le même fichier de stratégie UVM sera utilisé, vous devez utiliser la même clé publique 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. Autorisez des utilisateurs pour UVM en leur affectant un mot de passe composé UVM. Le client 1 disposant de deux utilisateurs, vous devez recommencer cette opération autant de fois que nécessaire.
  - b. Configurez la protection de connexion UVM pour la connexion Windows sur chaque client.
3. Activez le support Lotus Notes de la protection UVM sur les deux clients.
4. Editez et sauvegardez une stratégie UVM 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 à Windows. Pour plus de détails, reportez-vous à la section «Edition et utilisation d'une stratégie UVM» à la page 59.
5. Redémarrez chaque client afin d'activer la protection UVM pour la connexion Windows.
6. Fournissez aux utilisateurs clients les mots de passe composés UVM ainsi que la stratégie définie pour chaque client.

---

## Exemple 3 - Plusieurs clients CSS 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 CSS disposent à la fois de Windows 2000 et de 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. Elle permettra à Tivoli Access Manager de contrôler les objets d'authentification sélectionnés pour les clients.

Dans cet exemple, un utilisateur nécessite 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 de connexion 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 va être utilisée, vous devez utiliser la même clé publique 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/us/security/index.html>.
4. Configurez l'authentification utilisateur dans UVM sur chaque client. Reportez-vous à la section «Suppression d'utilisateurs» à la page 45 pour plus de détails. Effectuez ensuite les opérations suivantes :
  - a. Autorisez des utilisateurs pour UVM en leur affectant un mot de passe composé UVM.
  - b. Configurez la protection de connexion 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 CSS, 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 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 Windows
  - Acquisition d'un certificat numérique
  - Utilisation d'une signature numérique pour Outlook Express

Pour plus de détails, reportez-vous à la section «Edition et utilisation d'une stratégie UVM» à la page 59.

7. Redémarrez chaque client afin d'activer la protection UVM pour la connexion Windows.
8. Installez le module PKCS 11 de la puce de sécurité intégrée IBM sur chaque client. Ce module offre un support cryptographique sur les clients qui utilisent Netscape pour l'envoi et la réception de courriers électroniques, et le sous-système de sécurité intégré 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 client 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 Windows
  - Utilisation de l'utilitaire de configuration utilisateur
  - Inscription à un certificat numérique qui utilise le sous-système de sécurité intégré comme fournisseur de service cryptographique associé au certificat
  - Utilisation du certificat numérique pour chiffrer les messages de courrier électronique créés dans Netscape

---

## Chapitre 6. 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 offre l'interface requise pour gérer la stratégie de sécurité d'un client CSS. 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 CSS :

- Au niveau local, à l'aide d'un éditeur de stratégie résidant sur le client CSS
- 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 CSS. 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 utilisateur sont créées pour l'utilisateur client et stockées dans un fichier géré par le sous-système de sécurité intégré IBM. Si le client CSS 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 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 de connexion UVM» à la page 47 pour plus d'informations.
- **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 panneau de configuration de Windows. Vous devez activer la protection UVM pour la connexion au système pour l'économiseur d'écran Client Security.

---

## Opérations préalables à l'autorisation d'utilisateurs

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

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

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 de Windows. Avant d'ajouter des utilisateurs client dans UVM, utilisez Windows pour créer des comptes utilisateur et des profils pour ces utilisateurs. Le logiciel Client Security est compatible avec les dispositifs de sécurité fournis par Windows.

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 Microsoft.

### Remarques :

1. Lorsque vous créez de nouveaux utilisateurs à l'aide de Windows, 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 réautoriser 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 CSS, cliquez sur **Démarrer > Paramètres > Panneau de configuration > Sous-système de sécurité intégré 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 dans Windows.

4. Cliquez sur **Autorisation**.  
L'écran Configuration de l'authentification utilisateur s'affiche.

5. Passez en revue et sélectionnez les paramètres d'expiration du mot de passe composé pour le nouvel utilisateur. Par défaut, la case **L'utilisateur doit changer le mot de passe à la prochaine utilisation** est cochée et le mot de passe composé est défini pour expirer au bout de 184 jours.

6. 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**, pour d'afficher les paramètres requis pour un mot de passe composé correct.

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

7. 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 :

- **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 via l'utilitaire de configuration utilisateur, sélectionnez le bouton d'option approprié et cliquez sur **Suivant**.
- **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 utilisateur 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 dans Windows.

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

8. Cliquez sur **OK**.
9. 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 CSS, cliquez sur **Démarrer > Paramètres > Panneau de configuration > Sous-système de sécurité intégré 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 CSS, cliquez sur **Démarrer > Paramètres > Panneau de configuration > Sous-système de sécurité intégré 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 7. Fonctions UVM supplémentaires

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

- **Authentification Windows améliorée.** Reportez-vous à la section «Planification de la la protection de connexion UVM» pour plus de détails.
- **Protection de l'authentification améliorée pour les utilisateurs Lotus Notes.**
- **Activation des applications conformes au module PKCS 11.**
- **Réinitialisation d'un mot de passe composé.**
- **Enregistrement des empreintes digitales de l'utilisateur.** Reportez-vous à la section «Enregistrement des empreintes digitales de l'utilisateur» à la page 53 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.

---

### Authentification Windows améliorée

La fonction de protection de connexion UVM vient renforcer le dispositif de sécurité par mot de passe fourni avec Windows. L'interface de connexion UVM remplace la connexion Windows de sorte que la fenêtre de connexion UVM s'ouvre à chaque tentative de connexion de l'utilisateur au système.

### Planification de la la protection de connexion UVM

Lisez les informations ci-après avant de définir et d'utiliser la protection UVM pour la connexion Windows.

- Si la stratégie UVM indique qu'une authentification par empreinte digitale est requise pour la connexion Windows 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.
- Ne videz pas la puce de sécurité intégrée IBM tant que la protection UVM est activée. Sinon, le système se verrouillera. Pour plus de détails, consultez les "Conseils pour l'administrateur" au Annexe A, «Identification des incidents», à la page 73.
- Si vous désélectionnez la case **Activation du remplacement de connexion Windows** dans l'utilitaire d'administration, le système revient à la procédure d'ouverture de session Windows sans utiliser la protection de connexion UVM.
- Si vous activez le remplacement de connexion Windows 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 de connexion UVM

Pour configurer la protection de connexion UVM pour Windows, procédez comme suit :

1. A partir du bureau Windows du client IBM, cliquez sur **Démarrer > Paramètres > Panneau de configuration > Sous-système de sécurité intégré 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. Cochez la case **Activation du remplacement de connexion Windows**.
4. Cliquez sur **OK**.
5. Cliquez sur **Sortir**.
6. Fermez toutes les applications.
7. 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 «Authentification Windows améliorée» à la page 47.

## 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 ou modifier un mot de passe composé, qui peut être perdu ou oublié, ou encore modifié par l'utilisateur client.

Pour lancer une procédure de récupération de mot de passe composé UVM, procédez comme suit :

1. A partir du bureau Windows du client IBM, cliquez sur **Démarrer > Paramètres > Panneau de configuration > Sous-système de sécurité intégré IBM**.  
La fenêtre principale de l'utilitaire d'administration s'affiche.
2. Dans la zone Utilisateurs Windows autorisés à utiliser UVM, sélectionnez un nom d'utilisateur.
3. Cliquez sur **Modification du mot de passe composé**.  
L'écran de modification du mot de passe composé s'affiche.
4. Entrez le chemin et le nom du répertoire de l'archive de clés, ou cliquez sur **Parcourir** afin de localiser le répertoire.
5. Entrez le chemin et le nom de fichier de la clé privée administrateur dans la zone Fichier de clés privées d'archive, ou cliquez sur **Parcourir** afin de localiser le fichier.
6. Cliquez sur **OK**.  
Si la clé privée 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. Entrez le nouveau mot de passe composé UVM pour l'utilisateur dans la zone Mot de passe composé UVM et confirmez ce mot de passe composé dans la zone de confirmation de mot de passe composé UVM. Cliquez sur le bouton de **visualisation des règles du mot de passe composé** afin de visualiser les règles activées par la stratégie de sécurité UVM.
8. Sélectionnez et définissez les règles de péremption de mot de passe composé disponibles dans la zone de péremption de mot de passe composé.
9. Cliquez sur **Suivant**. Un message s'affiche afin d'indiquer que l'opération a abouti.
10. Cliquez sur **Terminer**.

---

## Protection de l'authentification améliorée pour les utilisateurs Lotus Notes

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

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

Avant de pouvoir activer la protection de connexion 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 de connexion UVM pour 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 intégré 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 **Éléments 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 requise 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 de connexion 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 de connexion UVM dans Lotus Notes».

### Configuration de la protection de connexion 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.  
La fenêtre Gestionnaire de vérification d'utilisateur IBM s'affiche.
2. A partir de la barre de menus de Lotus Notes, cliquez sur **Fichier > Outils > Sécurité 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 Sécurité 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 et 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 de connexion UVM pour un ID utilisateur Lotus Notes

Si vous souhaitez désactiver la protection de connexion 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 intégré IBM**.

Une fois que vous avez tapé le mot de passe administrateur, 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 de connexion 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 de connexion UVM pour un ID utilisateur Lotus Notes» à la page 50 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 de connexion UVM dans Lotus Notes» à la page 50.

---

## Activation des applications conformes au module PKCS 11

Les instructions de la présente section sont spécifiques de l'utilisation du logiciel Client Security pour ce qui concerne l'obtention et l'utilisation de certificats numériques avec des applications prenant en charge le module PKCS 11, par exemple, un logiciel Netscape ou RSA SecurID.

Pour plus de détails concernant l'utilisation de paramètres de sécurité pour les applications Netscape, consultez la documentation fournie avec ce dernier. Seules les versions 4.8 et 7.1 de Netscape sont prises en charge par le logiciel IBM Client Security.

**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. 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 11 de la puce de sécurité intégrée IBM

Avant d'utiliser un certificat numérique, vous devez installer le module PKCS 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 le module PKCS 11 de la puce de sécurité intégrée IBM à l'aide de Netscape, procédez comme suit :

1. Ouvrez Netscape et cliquez sur **File > Open page**.

2. Recherchez le fichier d'installation `ibmpkcsinstallt.html` ou `ibmpkcsinstalls.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 d'installation `ibmpkcsinstallt.html` ou `ibmpkcsinstalls.html` dans Netscape.  
Un message vous invite à confirmer l'installation de ce module de sécurité.
4. Cliquez sur **OK**.  
La fenêtre de mot de passe composé UVM s'affiche.
5. Entrez le mot de passe composé UVM et cliquez sur **OK**.  
Un message s'affiche pour indiquer que le module est installé.

## Sélection du sous-système de sécurité intégré IBM pour générer un certificat numérique

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 **CSP amélioré du 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

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 effectuer cette mise à jour à l'aide de l'utilitaire de configuration.

## Utilisation du certificat numérique du module PKCS 11

Utilisez les paramètres de sécurité de vos applications pour visualiser, 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 de détails, 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 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, l'application se lance, mais vous ne pouvez pas utiliser le certificat numérique généré par la puce de sécurité intégrée IBM tant que l'application n'a pas été redémarrée et que vous n'avez pas indiqué le mot de passe composé et/ou les empreintes digitales qui conviennent.

---

## Réinitialisation d'un mot de passe composé

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

## Réinitialisation à distance d'un mot de passe composé

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

- **Administrateurs**

Un administrateur distant doit exécuter la procédure suivante :

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

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

- **Utilisateurs**

L'utilisateur doit exécuter la procédure suivante :

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

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

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

## Réinitialisation manuelle d'un mot de passe composé

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

---

## Enregistrement des empreintes digitales de l'utilisateur

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.

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 utilisateur de Client Security - Edition des attributs utilisateur UVM s'affiche.
3. Sélectionnez l'option **Enregistrement d'empreinte digitale et/ou de carte à puce**, puis cliquez sur **Suivant**.  
La fenêtre Modification de la configuration utilisateur 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**.



---

## Chapitre 8. Gestion d'une stratégie UVM

**Remarque :** Avant de tenter d'éditer la stratégie UVM du client local, assurez-vous que des clés ont été définies. Sinon, un message d'erreur s'affiche 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. Un fichier de stratégie UVM peut être copié sur les clients d'un réseau.

L'utilitaire d'administration intègre un éditeur de stratégie UVM grâce qui vous permet d'éditer et de sauvegarder une stratégie UVM pour un client. Les tâches exécutées au niveau du client IBM, telles que la connexion Windows 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 empreinte digitale pour se connecter à Windows.
- 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. Pour plus de détails, reportez-vous au manuel *Utilisation du logiciel Client Security avec 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 Windows, par exemple), chacun des utilisateurs autorisés à utiliser 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 45.

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

---

### Edition d'une stratégie UVM

Une stratégie UVM 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, le fichier de stratégie UVM est stocké dans le répertoire `\Program Files\IBM\Security\UVM_Policy\globalpolicy.gvm`. Pour éditer et sauvegarder un fichier de stratégie UVM, utilisez l'éditeur de stratégie UVM. L'interface de cet éditeur est fournie dans l'utilitaire d'administration.

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 chaque fois que vous vous connectez 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 Windows, par exemple), chacun des utilisateurs autorisés à utiliser 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. Si vous cliquez sur **Validation**, un message vous invite à entrer la clé privée 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 l'onglet **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, puis 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 **Eléments 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 pouvoir appliquer une stratégie UVM à plusieurs clients IBM, vous devez l'éditer et la sauvegarder, 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.



---

## Chapitre 9. 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 intégré IBM**.  
L'accès à l'utilitaire d'administration étant protégé par le mot de passe administrateur, un message vous invite à entrer ce mot de passe.
2. Tapez le mot de passe administrateur 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 la clé publique d'archive.** Cette zone permet à l'administrateur de localiser la clé publique administrateur.

- **Emplacement de la clé privée d'archive.** Cette zone permet à l'administrateur de localiser la clé privée 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 l'itinérance des accréditations.** Cette fonction enregistre le système en tant que serveur itinérant CSS. Une fois enregistré, tout utilisateur autorisé UVM du réseau pourra accéder à ses données personnelles (mots de passe composés, certificat, etc.) sur le système.

---

## 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 2, «Instructions destinées à l'utilisateur client», à la page 13.

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 **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

Lorsque vous sauvegardez les clés administrateur dans un emplacement d'archive, les clés copiées sont appelées paire de clés d'archive. Elle sont généralement stockées sur une disquette ou dans un répertoire de réseau.

**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 **Modifier des clés d'archive**, puis sur **Suivant**.  
La fenêtre Modification de la configuration de clé - Clé publique s'affiche.
3. Dans la zone Nouvelles clés d'archive, entrez le nom de fichier de la nouvelle clé publique d'archive en regard de l'invite Clé publique d'archive. 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 Nouvelles clés d'archive, entrez le nom de fichier de la nouvelle clé privée d'archive en regard de l'invite Clé privée d'archive. 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 Anciennes clés d'archive, entrez le nom de fichier de l'ancienne clé publique d'archive en regard de l'invite Clé publique d'archive, ou cliquez sur **Parcourir** afin de rechercher le fichier.
6. Dans la zone Anciennes clés d'archive, entrez le nom de fichier de l'ancienne clé privée d'archive en regard de l'invite Clé privée d'archive, 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.

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 restaurer vos clés si vous remplacez une carte principale ou en cas de défaillance de l'unité de disque dur susceptible de mettre en péril l'intégrité des clés utilisateur. Lors de la restauration des clés, vous copiez les fichiers de clés utilisateur les plus récents de l'archive de clés pour les stocker dans le sous-système de sécurité intégré IBM. La restauration des clés remplace les clés qui figurent dans le sous-système de sécurité.

Si vous remplacez la carte principale d'origine de votre ordinateur par une carte principale contenant le sous-système de sécurité intégré 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 le sous-système de sécurité intégré 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 administrateur.

Pour en savoir plus sur l'activation du nouveau sous-système de sécurité et la définition d'un mot de passe administrateur, reportez-vous à la section «Activation du sous-système de sécurité intégré IBM et définition d'un mot de passe administrateur» à la page 69.

**Remarque :** La fonction de connexion UVM est activée automatiquement après une restauration de clé. Par conséquent, vous *devez*, si une procédure d'authentification par empreinte digitale était requise pour la connexion UVM au système restauré, 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.

## Conditions requises pour la restauration de clé

Les opérations de restauration de clés ne peuvent être effectuées que si les conditions suivantes sont remplies :

- Le nom d'ordinateur du système restauré doit correspondre au nom d'ordinateur du système d'origine.
- Le système restauré doit avoir accès à la paire de clés administrateur CSS et à l'emplacement d'archive du système d'origine.
- Le système restauré doit être doté d'un sous-système de sécurité IBM vide et activé. (Utilisez BIOS pour activer et vider la puce.)
- Le niveau de sous-système de sécurité intégré IBM du système restauré doit être équivalent à celui du système d'origine (par exemple, TCG ou non TCG).

## Scénarios de restauration

Voici trois scénarios de restauration du logiciel IBM Client Security :

- **Remplacement de la carte principale.** Si la carte principale d'origine du système doit être remplacée ou si l'unité de disque dur doit être déplacée sur un autre système, vous devez restaurer le sous-système de sécurité intégré IBM avec les clés figurant dans l'archive de clés du système d'origine.
- **Remplacement du système.** Si le système d'origine a été perdu ou volé, il est nécessaire de restaurer le sous-système de sécurité IBM et le logiciel IBM Client Security à partir des données stockées dans l'emplacement d'archive.
- **Remplacement de l'unité de disque dur.** Si l'unité de disque dur est défectueuse sur le système d'origine et qu'une nouvelle unité doit être installée, vous devez restaurer le logiciel IBM Client Security à partir de l'emplacement d'archive.

### Remplacement de la carte principale

Pour remplacer la carte principale d'un ordinateur qui contient un sous-système de sécurité intégré IBM, procédez comme suit :

1. Cliquez sur l'icône **Sous-système de sécurité client IBM** dans le panneau de configuration de Windows.

2. Entrez et confirmez le mot de passe administrateur, puis cliquez sur **OK**.
3. Indiquez l'emplacement d'archive et celui de la clé administrateur du système d'origine dans les zones appropriées, puis cliquez sur **OK**.
4. Cliquez sur **OK**.
5. Cliquez sur **Sortir** pour fermer l'utilitaire d'administration.  
L'ordinateur est désormais complètement restauré. Redémarrez-le avant de continuer.

## Remplacement du système

Une fois que vous avez installé le logiciel IBM Client Security sur un nouveau système, l'assistant de configuration CSS s'exécute automatiquement lorsque le système redémarre. Pour remplacer un système et restaurer les données stockées dans l'emplacement d'archive, procédez comme suit :

1. Cliquez sur **Suivant** sur la première page de l'assistant de configuration CSS.
2. Entrez et confirmez le mot de passe administrateur du nouveau système, puis cliquez sur **Suivant**.
3. Sélectionnez le bouton d'option vous permettant **d'utiliser une clé de sécurité existante** et indiquez l'emplacement de la clé publique administrateur archivée et de la clé privée administrateur du système d'origine dans les zones appropriées.
4. Dans la zone de sauvegarde des données de sécurité, entrez un emplacement d'archive temporaire.

### Remarques :

- a. Vous pourrez supprimer ultérieurement cet emplacement une fois que le système sera complètement restauré à partir de l'archive système d'origine.
  - b. Le reste des données est remplacé lors de la restauration de l'archive système d'origine. Par conséquent, utilisez les valeurs par défaut.
5. Cliquez sur **Suivant**.
  6. Cliquez sur **Suivant** sur la page de protection des applications avec IBM Client Security.
  7. Cliquez sur **Suivant** sur la page Autorisation des utilisateurs.
  8. Cliquez sur **Suivant** sur la page Sélection du niveau de sécurité du système.
  9. Cliquez sur **Terminer** sur la page de vérification des paramètres de sécurité.
  10. Cliquez sur **OK**.
  11. Poursuivez en exécutant la procédure «Remplacement de l'unité de disque dur».

## Remplacement de l'unité de disque dur

Pour restaurer le logiciel IBM Client Security à partir de l'emplacement d'archive après le remplacement d'une unité de disque dur, procédez comme suit :

1. Cliquez sur l'icône **Sous-système de sécurité client IBM** dans le panneau de configuration de Windows.
2. Entrez le mot de passe administrateur qui a été défini dans l'assistant de configuration CSS et cliquez sur **OK**.
3. Cliquez sur **Configuration de clé**.
4. Cliquez sur le bouton d'option **Restauration des clés du sous-système de sécurité IBM à partir d'une archive**, puis sur **Suivant**.
5. Indiquez l'emplacement d'archive et celui de la clé administrateur du système d'origine dans les zones appropriées, puis cliquez sur **Suivant**.
6. Cliquez sur **OK**.

7. Cliquez sur **Terminer** pour revenir sur la page de configuration principale.
8. Cliquez sur **Sortir** pour fermer l'utilitaire d'administration.  
L'ordinateur est désormais complètement restauré. Redémarrez-le avant de continuer.

---

## 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. Tapez l'emplacement d'archive du sous-système de sécurité IBM dans la zone appropriée ou cliquez sur **Parcourir** pour sélectionner l'emplacement d'archive du sous-système de sécurité IBM pour l'utilisateur sélectionné.
4. Tapez le nom du fichier de clés privées d'archive dans la zone appropriée ou cliquez sur **Parcourir** pour sélectionner le fichier de clés privées d'archive pour l'utilisateur sélectionné.
5. Cliquez sur **OK**.  
Un message s'affiche pour indiquer que l'opération a abouti.
6. 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*.

### Configuration des paramètres de Tivoli Access Manager sur un client

Une fois que Tivoli Access Manager est installé sur le client local, vous pouvez en configurer les paramètres à l'aide de l'utilitaire d'administration. Pour configurer les paramètres 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 configurer les paramètres de Tivoli Access Manager sur un client, procédez comme suit à l'aide de 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. Cochez la case **Activation du remplacement de connexion Windows**.
3. Cliquez sur le bouton **Stratégie d'application**. L'écran Modification de la configuration de stratégie de Client Security s'affiche.
4. Dans la zone des paramètres de Tivoli Access Manager, sélectionnez le chemin d'accès complet au fichier de configuration TAMCSS.conf. (Par exemple, C:\TAMCSS\TAMCSS.conf.) Tivoli Access Manager doit être installé sur le client

pour que cette zone soit activée. Vous pouvez également cliquer sur **Parcourir** pour rechercher le fichier de configuration.

5. Cliquez sur le bouton **Edition de la stratégie** et entrez le mot de passe administrateur.
6. Sélectionnez dans le menu déroulant Actions les actions qui doivent être contrôlées par Tivoli Access Manager.
7. Sélectionnez l'option **Access Manager contrôle l'objet sélectionné** de sorte que la case soit cochée.
8. Cliquez sur le bouton **Appliquer**. Les modifications sont prises en compte lors de la régénération de la mémoire cache. Si vous souhaitez que les modifications soient appliquées immédiatement, cliquez sur le bouton **Régénérer la mémoire cache locale** de l'écran Modification de la configuration de la stratégie de sécurité client.

## 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. Cliquez sur le bouton **Stratégie d'application**. L'écran Modification de la configuration de stratégie de Client Security s'affiche.
3. 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.

---

## Modification du mot de passe administrateur

Vous devez définir un mot de passe administrateur afin d'activer le sous-système de sécurité intégré IBM pour un client. Une fois que vous avez défini un mot de passe administrateur, 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 administrateur. Un mot de passe qui demeure inchangé pendant longtemps devient plus vulnérable pour l'extérieur. Protégez le mot de passe administrateur afin d'empêcher les utilisateurs non autorisés de modifier les paramètres de l'utilitaire d'administration. Pour toute information sur les règles de mot de passe administrateur, reportez-vous à la section Annexe B, «Informations relatives aux mots de passe et mots de passe composés», à la page 93.

Pour modifier le mot de passe administrateur, 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 ci-après concernant le sous-système de sécurité intégré 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 du sous-système de sécurité intégré IBM

L'utilitaire d'administration permet de désactiver le sous-système de sécurité intégré IBM. Le mot de passe administrateur étant requis pour lancer l'utilitaire d'administration et désactiver le sous-système de sécurité, vous devez le protéger afin d'empêcher des utilisateurs non autorisés de désactiver le sous-système.

**Important** : N'effectuez pas un vidage du sous-système de sécurité intégré IBM pendant que la protection UVM est activée. Sinon, le système se verrouillera. Pour annuler la protection UVM, ouvrez l'utilitaire d'administration et désélectionnez la case à cocher **Activation du remplacement de connexion Windows**. Vous devez ensuite redémarrer l'ordinateur pour que la protection UVM de connexion système soit désactivée.

Pour désactiver le sous-système de sécurité intégré, 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 BIOS qui a été défini dans l'utilitaire de configuration pour pouvoir désactiver la puce.

Après désactivation du sous-système, il n'est pas possible de réutiliser le sous-système de sécurité intégré IBM et les clés de chiffrement. Une réactivation du sous-système de sécurité est nécessaire pour cela.

---

## Activation du sous-système de sécurité intégré IBM et définition d'un mot de passe administrateur

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

Vous pouvez également être amené à activer le sous-système de sécurité intégré IBM pour restaurer l'archive de clés après le remplacement d'une carte principale ou la désactivation du sous-système.

Pour activer le sous-système de sécurité et définir un mot de passe administrateur, procédez comme suit :

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

Un message s'affiche afin de vous demander si vous souhaitez activer le sous-système de sécurité intégré 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 le sous-système de sécurité intégré IBM puisse être activé. Si la sécurité avancée a été activée sur votre ordinateur, vous devrez peut-être saisir le mot de passe administrateur BIOS 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 intégré IBM**.

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

5. Entrez un nouveau mot de passe administrateur 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 intégré 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.



---

## Partie 4. Annexes



---

## Annexe A. Identification des incidents

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

---

### Fonctions d'administrateur

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

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

### Autorisation d'utilisateurs

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

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

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

### Suppression d'utilisateurs

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

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

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

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

**Important :**

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

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

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

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

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

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

## Définition d'un mot de passe superviseur (ThinkPad)

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

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

### Important :

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

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

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

### Exemple 1

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

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

### Exemple 2

1. Arrêtez et redémarrez l'ordinateur.
2. Lorsque le message "Pour interrompre le démarrage normal, appuyez sur le bouton bleu Access IBM" s'affiche, appuyez sur le bouton bleu Access IBM. La zone Access IBM Predesktop Area s'affiche.
3. Cliquez deux fois sur **Start setup utility**.
4. Sélectionnez **Security** à l'aide des touches directionnelles (vers le bas du menu).
5. Sélectionnez **Password**.
6. Sélectionnez **Supervisor Password**.
7. Tapez votre mot de passe et appuyez sur Entrée.
8. Retapez votre mot de passe et appuyez sur Entrée.
9. Cliquez sur **Continuer**.
10. Appuyez sur F10 pour sauvegarder et sortir.

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

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

## Protection du mot de passe administrateur

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

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

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

### Important :

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

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

1. Arrêtez et redémarrez l'ordinateur.
2. Lorsque l'invite du programme de configuration s'affiche, appuyez sur F1. Le menu principal du programme de configuration s'affiche.
3. Sélectionnez **Security**.
4. Sélectionnez **IBM TCPA Security Feature** et appuyez sur Entrée.
5. Cliquez sur **Yes**.
6. Appuyez sur Entrée pour confirmer votre choix.

7. Appuyez sur F10 pour sauvegarder vos modifications et sortir du programme de configuration.
8. Sélectionnez **Yes** et appuyez sur Entrée. L'ordinateur redémarre.

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

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

### Important :

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

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

1. Arrêtez et redémarrez l'ordinateur.
2. Lorsque l'invite du programme de configuration s'affiche, appuyez sur F1. Le menu principal du programme de configuration s'affiche.
3. Sélectionnez **Security**.
4. Sélectionnez **IBM Security Chip** et appuyez sur Entrée.
5. Appuyez sur Entrée et sélectionnez **Disabled**.
6. Appuyez sur Entrée pour confirmer votre choix.
7. Appuyez sur Entrée pour continuer.
8. Appuyez sur F10 pour sauvegarder vos modifications et sortir du programme de configuration.
9. Sélectionnez **Yes** et appuyez sur Entrée. L'ordinateur redémarre.

---

## Incidents ou limitations connus concernant CSS version 5.4

Les informations ci-après pourront vous être utiles lorsque vous utiliserez les fonctions du logiciel IBM Client Security version 5.4.

### Limitations relatives à l'itinérance

#### Utilisation d'un serveur itinérant CSS

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

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

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

#### Délais de régénération d'itinérance et certificats Internet Explorer

Les certificats Internet Explorer sont régénérés dans l'archive toutes les 20 secondes. Lorsqu'un nouveau certificat Internet Explorer est généré par un

utilisateur itinérant, celui-ci doit attendre au moins 20 secondes avant d'importer, de restaurer ou de modifier sa configuration CSS sur un autre système. S'il tente d'exécuter l'une ou l'autre de ces opérations avant le délai de 20 secondes, l'intervalle de régénération entraîne la perte du certificat. En outre, si l'utilisateur n'était pas connecté à l'archive au moment de la création du certificat, il doit attendre 20 secondes après s'être connecté à l'archive afin d'être certain que le certificat est mis à jour dans l'archive.

### **Mot de passe Lotus Notes et itinérance d'accréditation**

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

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

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

### **Disponibilité des accréditations lors de la connexion dans un environnement itinérant**

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

## **Restauration de clés**

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

## Noms d'utilisateurs de domaine et locaux

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

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

## Réinstallation du logiciel d'empreinte digitale Targus

Si le logiciel d'empreinte digitale Targus est enlevé et réinstallé, les entrées de registre nécessaires pour l'activation de la fonction d'empreinte digitale dans le logiciel Client Security doivent être ajoutées manuellement. Téléchargez le fichier de registre contenant les entrées nécessaires (atplugin.reg) et cliquez deux fois dessus de sorte que ces entrées soient fusionnées dans le registre. Cliquez sur Yes lorsque le système vous invite à confirmer cette opération. Vous devez relancer le système pour que le logiciel Client Security reconnaisse ces modifications et active la fonction d'empreinte digitale.

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

## Mot de passe composé superviseur BIOS

La version 5.4 et les versions antérieures du logiciel IBM Client Security ne prennent pas en charge la fonction de mot de passe composé superviseur BIOS disponible sur certains systèmes ThinkPad. Si vous activez l'utilisation du mot de passe composé superviseur BIOS, toute opération d'activation ou de désactivation du sous-système de sécurité doit être effectuée à partir du programme de configuration BIOS.

## Utilisation de Netscape 7.x

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

## Utilisation d'une disquette pour l'archivage

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



## Limitations relatives aux cartes à puce

### Enregistrement de cartes à puce

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

### Authentification des cartes à puce

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

## Affichage du caractère + devant les dossiers après le chiffrement

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

## Limites relatives aux utilisateurs limités de Windows XP

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

---

## Autres limites

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

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

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

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

## Utilisation du logiciel Client Security avec des applications Netscape

**Netscape s'ouvre après un échec d'autorisation :** Si la fenêtre de mot de passe composé UVM s'affiche, vous devez taper le mot de passe composé UVM et

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

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

- SHA-1
- MD5

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

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

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

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

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

## **Utilisation de la protection UVM pour un ID utilisateur Lotus Notes**

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

1. Quittez Notes.
2. Désactivez la protection UVM pour l'ID utilisateur en cours.

3. Ouvrez Notes et changez d'ID utilisateur. Consultez la documentation Lotus Notes pour plus d'informations sur le changement d'ID utilisateur.  
Pour configurer la protection UVM pour le nouvel ID utilisateur choisi, passez à l'étape 4.
4. Ouvrez l'outil de configuration Lotus Notes fourni par le logiciel Client Security et configurez la protection UVM.

## Limites de l'utilitaire de configuration utilisateur

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

### Windows XP Professionnel

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

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

Dans les situations ci-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

### Windows XP Edition familiale

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

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

## Limites relatives à Tivoli Access Manager

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

## Messages d'erreur

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

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

## Tableaux d'identification des incidents

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

### Identification des incidents liés à l'installation

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

Incident	Solution possible
<b>Un message d'erreur s'affiche lors de l'installation du logiciel</b>	<b>Action</b>
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 <b>OK</b> pour sortir de la fenêtre. Relancez le processus d'installation pour installer la nouvelle version du logiciel Client Security.
Un message s'affiche pendant l'installation pour signaler qu'une mise à niveau ou un retrait du programme est nécessaire.	Exécutez l'une des opérations suivantes : <ul style="list-style-type: none"> <li>• Si une version antérieure à la version 5.0 du logiciel Client Security est installée, sélectionnez <b>Remove</b> pour la supprimer. Redémarrez l'ordinateur et videz le sous-système de sécurité à l'aide de l'utilitaire de configuration BIOS d'IBM.</li> <li>• Sinon, sélectionnez <b>Upgrade</b> et poursuivez l'installation.</li> </ul>
<b>L'accès à l'installation est refusé car le mot de passe administrateur est inconnu</b>	<b>Action</b>
Lorsque vous installez le logiciel sur un client IBM sur lequel un sous-système de sécurité intégré IBM est activé, le mot de passe administrateur pour ce dernier est inconnu.	Videz le sous-système de sécurité afin de poursuivre l'installation.

## Identification des incidents liés à l'utilitaire d'administration

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

Incident	Solution possible
<b>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</b>	<b>Action</b>
Lorsque vous ajoutez des utilisateurs à UVM, le bouton <b>Suivant</b> 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 <b>Information</b> dans la Barre des tâches Windows et continuez la procédure.
<b>Un message d'erreur s'affiche lorsque vous modifiez la clé publique administrateur</b>	<b>Action</b>
Lorsque vous videz le sous-système de sécurité intégré et que vous restaurez ensuite l'archive de clés, un message d'erreur peut s'afficher si vous modifiez la clé publique administrateur.	Ajoutez les utilisateurs à UVM et demandez de nouveaux certificats, le cas échéant.
<b>Un message d'erreur s'affiche lorsque vous tentez de récupérer un mot de passe composé UVM</b>	<b>Action</b>
Lorsque vous modifiez la clé publique administrateur et que vous tentez ensuite de récupérer un mot de passe composé UVM pour un utilisateur, un message d'erreur peut s'afficher.	Exécutez l'une des opérations suivantes : <ul style="list-style-type: none"> <li>• Si le mot de passe composé UVM pour l'utilisateur n'est pas nécessaire, aucune action n'est requise.</li> <li>• 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.</li> </ul>
<b>Un message d'erreur s'affiche lorsque vous tentez de sauvegarder le fichier de stratégie UVM</b>	<b>Action</b>
Lorsque vous tentez de sauvegarder un fichier de stratégie UVM (globalpolicy.gvm) en cliquant sur <b>Validation</b> ou <b>Sauvegarde</b> , un message d'erreur s'affiche.	Sortez du message d'erreur, éditez à nouveau le fichier de stratégie UVM pour apporter les modifications souhaitées, puis sauvegardez le fichier.
<b>Un message d'erreur s'affiche lorsque vous tentez d'ouvrir l'éditeur de stratégie UVM</b>	<b>Action</b>
Lorsque l'utilisateur en cours (connecté au système d'exploitation) n'a pas été ajouté à UVM, l'éditeur de stratégie UVM ne s'ouvre pas.	Ajoutez l'utilisateur à UVM et ouvrez l'éditeur de stratégie UVM.
<b>Un message d'erreur s'affiche lorsque vous utilisez l'utilitaire d'administration</b>	<b>Action</b>

Incident	Solution possible
<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 au sous-système de sécurité intégré IBM. Cet incident peut être résolu par un réamorçage.</p>	Sortez du message d'erreur et redémarrez l'ordinateur.
<b>Un message de désactivation de la puce s'affiche lors de la modification du mot de passe administrateur</b>	<b>Action</b>
<p>Lorsque vous tentez de modifier le mot de passe administrateur et que vous appuyez sur Entrée ou Tabulation &gt; Entrée après avoir tapé le mot de passe de confirmation, le bouton <b>Désactivation de la puce</b> 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"> <li>1. Sortez de la fenêtre de confirmation de la désactivation de la puce.</li> <li>2. Pour modifier le mot de passe administrateur, tapez le nouveau mot de passe, tapez le mot de passe de confirmation, puis cliquez sur <b>Modification</b>. N'appuyez ni sur Entrée, ni sur la touche de tabulation &gt; Entrée après avoir tapé les informations dans la fenêtre de confirmation.</li> </ol>

## 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
<b>Les utilisateurs limités ne peuvent pas exécuter certaines fonctions de l'utilitaire de configuration utilisateur sous Windows XP Professionnel</b>	<b>Action</b>
<p>Les utilisateurs limités de Windows XP Professionnel risquent de ne pas pouvoir exécuter les tâches suivantes de l'utilitaire de configuration utilisateur :</p> <ul style="list-style-type: none"> <li>• Modifier leur mot de passe composé UVM</li> <li>• Mettre à jour le mot de passe Windows enregistré à l'aide d'UVM</li> <li>• Mettre à jour l'archive de clés</li> </ul>	Il s'agit d'une limite connue de Windows XP Professional. Il n'existe pas de solution à cet incident.
<b>Les utilisateurs limités ne peuvent pas utiliser l'utilitaire de configuration utilisateur sous Windows XP Edition familiale</b>	<b>Action</b>

Incident	Solution possible
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"> <li>• Le logiciel Client Security est installé sur une partition au format NTFS.</li> <li>• Le dossier Windows se trouve sur une partition au format NTFS.</li> <li>• Le dossier d'archive se trouve sur une partition au format NTFS.</li> </ul>	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
<b>Un autre détecteur d'empreinte digitale compatible UVM ne fonctionne pas correctement</b>	<b>Action</b>
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
<b>L'écran de veille ne s'affiche que sur l'écran local</b>	<b>Action</b>
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.
<b>Client Security ne fonctionne pas correctement pour un utilisateur enregistré dans UVM</b>	<b>Action</b>
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.
<b>Remarque :</b> 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.	
<b>Incidents lors de la lecture du courrier électronique chiffré à l'aide d'Outlook Express</b>	<b>Action</b>

Incident	Solution possible
Le courrier électronique chiffré ne peut pas être déchiffré en raison des différences de chiffrement renforcé existant entre les navigateurs Web utilisés par l'expéditeur et le destinataire.	Vérifiez les points suivants : 1. Le chiffrement renforcé pour le navigateur Web utilisé par l'expéditeur est compatible avec celui utilisé par le destinataire. 2. Le chiffrement renforcé pour le navigateur Web est compatible avec celui fourni par le microcode du logiciel Client Security.
<b>Incidents lors de l'utilisation d'un certificat à partir d'une adresse à laquelle sont associés plusieurs certificats</b>	<b>Action</b>
Outlook Express peut répertorier plusieurs certificats associés à une seule adresse électronique et certains de ces certificats peuvent ne plus être valables. Un certificat peut ne plus être valable si la clé privée qui lui est associée n'existe plus sur le sous-système de sécurité intégré IBM de l'ordinateur de l'expéditeur sur lequel le certificat a été généré.	Demandez au destinataire de renvoyer son certificat numérique, puis sélectionnez ce certificat dans le carnet d'adresses d'Outlook Express.
<b>Message d'échec lors de la tentative de signature numérique d'un message électronique</b>	<b>Action</b>
Si l'auteur d'un message électronique tente de le signer numériquement alors qu'aucun certificat n'est encore associé à son compte de messagerie électronique, un message d'erreur s'affiche.	Utilisez les paramètres de sécurité d'Outlook Express pour indiquer un certificat à associer au compte de l'utilisateur. Pour plus de détails, consultez la documentation fournie pour Outlook Express.
<b>Outlook Express (128 bits) chiffre uniquement les messages électroniques avec l'algorithme 3DES</b>	<b>Action</b>
Lors de l'envoi de courrier électronique chiffré entre des clients utilisant Outlook Express avec la version 128 bits d'Internet Explorer 4.0 ou 5.0, seul l'algorithme 3DES peut être utilisé.	Consultez la documentation Microsoft pour obtenir des informations à jour sur les algorithmes de chiffrement utilisés avec Outlook Express.
<b>Les clients Outlook Express renvoient des messages électroniques avec un algorithme différent</b>	<b>Action</b>
Un message électronique chiffré avec l'algorithme RC2(40), RC2(64) ou RC2(128) est envoyé d'un client utilisant Netscape Messenger à un client utilisant Outlook Express (128 bits). Un message électronique renvoyé par le client Outlook Express est chiffré avec l'algorithme RC2(40).	Aucune action n'est requise. Une demande de chiffrement RC2(40), RC2(64) ou RC2(128) d'un client Netscape vers un client Outlook Express (128 bits) est toujours renvoyée au client Netscape avec l'algorithme RC2(40). Consultez la documentation Microsoft pour obtenir des informations à jour sur les algorithmes de chiffrement utilisés avec votre version d'Outlook Express.
<b>Message d'erreur lors de l'utilisation d'un certificat dans Outlook Express après une défaillance de l'unité de disque dur</b>	<b>Action</b>



<b>Incident</b>	<b>Solution possible</b>
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"> <li>• Obtenez de nouveaux certificats.</li> <li>• Enregistrez à nouveau l'autorité de certification dans Outlook Express.</li> </ul>
<b>Outlook Express ne met pas à jour le chiffrement renforcé associé à un certificat</b>	<b>Action</b>
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.
<b>Un message d'erreur de déchiffrement s'affiche dans Outlook Express</b>	<b>Action</b>
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.
<b>Un message d'erreur s'affiche lorsque vous cliquez deux fois sur le bouton Envoyer dans des courriers électroniques chiffrés</b>	<b>Action</b>
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 <b>Envoyer</b> .
<b>Un message d'erreur s'affiche lorsque vous demandez un certificat</b>	<b>Action</b>
Lorsque vous utilisez Internet Explorer, vous risquez de recevoir un message d'erreur si vous demandez un certificat qui utilise le fournisseur de service cryptographique du sous-système de sécurité intégré IBM.	Redemandez le certificat numérique.

## Identification des incidents relatifs aux applications Netscape

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

Incident	Solution possible
<b>Incidents lors de la lecture du courrier électronique chiffré</b>	<b>Action</b>
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"> <li>1. Le chiffrement renforcé pour le navigateur Web utilisé par l'expéditeur est compatible avec celui utilisé par le destinataire.</li> <li>2. Le chiffrement renforcé pour le navigateur Web est compatible avec celui fourni par le microcode du logiciel Client Security.</li> </ol>
<b>Message d'échec lors de la tentative de signature numérique d'un message électronique</b>	<b>Action</b>
Lorsque le certificat de sous-système de sécurité intégré IBM n'a pas été sélectionné dans Netscape Messenger et que l'auteur d'un message électronique tente de signer celui-ci avec le certificat, un message d'erreur s'affiche.	Utilisez les paramètres de sécurité de Netscape Messenger pour sélectionner le certificat. Lorsque Netscape Messenger est ouvert, cliquez sur l'icône de sécurité de la barre d'outils. La fenêtre relative aux informations de sécurité s'ouvre. Cliquez sur <b>Messenger</b> dans le panneau de gauche, puis sélectionnez le <b>certificat de la puce de sécurité intégrée IBM</b> . Pour plus de détails, consultez la documentation fournie par Netscape.
<b>Un message électronique est renvoyé au client avec un algorithme différent</b>	<b>Action</b>
Un message électronique chiffré avec l'algorithme RC2(40), RC2(64) ou RC2(128) est envoyé d'un client utilisant Netscape Messenger à un client utilisant Outlook Express (128 bits). Un message électronique renvoyé par le client Outlook Express est chiffré avec l'algorithme RC2(40).	Aucune action n'est requise. Une demande de chiffrement RC2(40), RC2(64) ou RC2(128) d'un client Netscape vers un client Outlook Express (128 bits) est toujours renvoyée au client Netscape avec l'algorithme RC2(40). Consultez la documentation Microsoft pour obtenir des informations à jour sur les algorithmes de chiffrement utilisés avec votre version d'Outlook Express.
<b>Impossible d'utiliser un certificat numérique généré par le sous-système de sécurité intégré IBM</b>	<b>Action</b>
Le certificat numérique généré par le sous-système de sécurité intégré IBM n'est pas disponible pour l'utilisation.	Vérifiez que le mot de passe composé UVM a été tapé correctement lors de l'ouverture de Netscape. Si le mot de passe composé UVM est incorrect, un message d'erreur signalant un échec d'authentification s'affiche. Si vous cliquez sur <b>OK</b> , Netscape se lance mais vous ne pouvez pas utiliser le certificat généré par le sous-système de sécurité intégré IBM. Vous devez sortir de Netscape, puis l'ouvrir à nouveau et taper le mot de passe composé UVM correct.

<b>Incident</b>	<b>Solution possible</b>
<b>De nouveaux certificats numériques provenant du même expéditeur ne sont pas remplacés dans Netscape</b>	<b>Action</b>
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.
<b>Impossible d'exporter le certificat du sous-système de sécurité intégré IBM</b>	<b>Action</b>
Le certificat du sous-système de sécurité intégré IBM ne peut pas être exporté dans Netscape. La fonction d'exportation de Netscape peut être utilisée pour effectuer des copies de sauvegarde des certificats.	Accédez à l'utilitaire d'administration ou à l'utilitaire de configuration utilisateur pour mettre à jour l'archive de clés. Lorsque vous mettez à jour l'archive de clés, des copies de tous les certificats associés au sous-système de sécurité intégré IBM sont créées.
<b>Message d'erreur lors de la tentative d'utilisation d'un certificat restauré après une défaillance de l'unité de disque dur</b>	<b>Action</b>
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.
<b>L'agent Netscape s'ouvre et provoque l'échec de Netscape</b>	<b>Action</b>
L'agent Netscape s'ouvre et provoque la fermeture de Netscape.	Mettez l'agent Netscape hors tension.
<b>Un délai s'écoule lors de la tentative d'ouverture de Netscape</b>	<b>Action</b>
Si vous ajoutez le module PKCS 11 du sous-système de sécurité intégré IBM, puis que vous ouvrez Netscape, un petit délai s'écoule avant l'ouverture de Netscape.	Aucune action n'est requise. Ces informations sont fournies uniquement à titre d'information.

## Identification des incidents relatifs à un certificat numérique

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

Incident	Solution possible
<b>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</b>	<b>Action</b>
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.
<b>Un message d'erreur VBScript ou JavaScript s'affiche</b>	<b>Action</b>
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
<b>Les paramètres de stratégie locaux ne correspondent pas à ceux du serveur</b>	<b>Action</b>
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.
<b>Les paramètres de configuration de Tivoli Access Manager ne sont pas accessibles</b>	<b>Action</b>
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.
<b>Une commande utilisateur est valide à la fois pour l'utilisateur et le groupe</b>	<b>Action</b>

<b>Incident</b>	<b>Solution possible</b>
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 <b>Traverse bit</b> 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.

<b>Incident</b>	<b>Solution possible</b>
<b>Une fois que la fonction de protection UVM pour Lotus Notes a été activée, Notes ne peut pas finir sa configuration</b>	<b>Action</b>
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.
<b>Un message d'erreur s'affiche lorsque vous tentez de modifier le mot de passe Notes</b>	<b>Action</b>
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.
<b>Un message d'erreur s'affiche une fois que vous avez généré un mot de passe de façon aléatoire</b>	<b>Action</b>
Un message d'erreur risque de s'afficher lorsque vous exécutez les opérations suivantes : <ul style="list-style-type: none"> <li>• Utilisation de l'outil de configuration de Lotus Notes pour définir la protection UVM pour un ID Notes</li> <li>• Ouverture de Notes et utilisation de la fonction fournie par Notes pour modifier le mot de passe pour un fichier d'ID Notes</li> <li>• Fermeture immédiate de Notes après la modification du mot de passe</li> </ul>	Cliquez sur <b>OK</b> pour faire disparaître le message d'erreur. Aucune autre action n'est requise.  Contrairement aux indications du message d'erreur, le mot de passe a été modifié. Le nouveau mot de passe est généré de façon aléatoire par le logiciel Client Security. Le fichier d'ID Notes est désormais chiffré à l'aide du mot de passe généré de façon aléatoire et l'utilisateur n'a pas besoin d'un nouveau fichier d'ID utilisateur. Si l'utilisateur final modifie à nouveau le mot de passe, UVM génère un nouveau mot de passe de façon aléatoire pour l'ID Notes.

## Identification des incidents relatifs au chiffrement

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

Incident	Solution possible
<b>Les fichiers précédemment chiffrés ne sont pas déchiffrés</b>	<b>Action</b>
Les fichiers chiffrés à l'aide de versions précédentes du logiciel Client Security ne peuvent pas être déchiffrés après la mise à niveau vers Client Security version 3.0 ou suivante.	Il s'agit d'une limite connue.  Vous devez déchiffrer tous les fichiers qui ont été chiffrés à l'aide de versions précédentes du logiciel Client Security <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.

## 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
<b>Un périphérique compatible UVM cesse de fonctionner correctement</b>	<b>Action</b>
Un dispositif de sécurité compatible UVM, tel qu'une carte à puce, un lecteur de carte à puce ou un scanner d'empreinte digitale, ne fonctionne pas correctement.	Vérifiez que le dispositif est correctement configuré par le système. Une fois le dispositif configuré, il peut s'avérer nécessaire de redémarrer le système pour démarrer correctement le service.  Pour plus d'informations sur la résolution des incidents liés à un dispositif, reportez-vous à la documentation fournie avec ce dernier ou prenez contact avec le fournisseur.
<b>Un périphérique compatible UVM cesse de fonctionner correctement</b>	<b>Action</b>
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 B. Informations relatives aux mots de passe et mots de passe composés

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

---

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

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

#### Règles applicables au mot de passe administrateur

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

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

- Définir ou non un nombre minimal de caractères alphanumériques autorisé (oui, 6)  
Par exemple, lorsque "6" caractères sont autorisés, 1234567xxx est un mot de passe incorrect.
- Définir ou non un nombre minimal de chiffres autorisé (oui, 1)  
Par exemple, lorsque ce nombre est défini à "1", voicimonmotdepasse est un mot de passe incorrect.
- Définir ou non le nombre minimal d'espaces autorisé (pas de minimum)  
Par exemple, lorsque ce nombre est défini à "2", je suis absent est un mot de passe incorrect.
- Autoriser ou non le mot de passe composé à commencer par un chiffre (non)  
Par exemple, par défaut, 1motdepasse est un mot de passe incorrect.
- Autoriser ou non le mot de passe composé à se terminer par un chiffre (non)  
Par exemple, par défaut, motdepasse8 est un mot de passe incorrect.

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

#### Longueur

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

#### Caractères

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

#### Propriétés

Le mot de passe administrateur est différent du mot de passe que vous

pouvez utiliser pour ouvrir une session sur un système d'exploitation. Il peut être utilisé avec d'autres dispositifs d'authentification, tels que les capteurs à empreintes digitales UVM.

#### **Tentatives infructueuses**

Si vous tapez plusieurs fois un mot de passe administrateur incorrect durant une session, l'ordinateur met à exécution une série de périodes de suspension anti-martèlement (qui vous empêchent de tenter de vous connecter de façon incessante).

## **Règles relatives aux mots de passe composés UVM**

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

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

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

- Définir ou non un nombre minimal de caractères alphanumériques autorisé (oui, 6)  
Par exemple, lorsque "6" caractères sont autorisés, 1234567xxx est un mot de passe incorrect.
- Définir ou non un nombre minimal de chiffres autorisé (oui, 1)  
Par exemple, lorsque ce nombre est défini à "1", voicimonmotdepasse est un mot de passe incorrect.
- Définir ou non le nombre minimal d'espaces autorisé (pas de minimum)  
Par exemple, lorsque ce nombre est défini à "2", je suis absent est un mot de passe incorrect.
- Autoriser ou non le mot de passe composé à commencer par un chiffre (non)  
Par exemple, par défaut, 1motdepasse est un mot de passe incorrect.
- Autoriser ou non le mot de passe composé à se terminer par un chiffre (non)  
Par exemple, par défaut, motdepasse8 est un mot de passe incorrect.
- Autoriser ou non le mot de passe composé à contenir un ID utilisateur (non)  
Par exemple, par défaut, NomUtilisateur est un mot de passe incorrect, où NomUtilisateur est un ID utilisateur.
- Vérifier ou non que le nouveau mot de passe composé est différent des x derniers mots de passe composés, où x correspond à une zone modifiable (oui, 3)  
Par exemple, par défaut, monmotdepasse est un mot de passe incorrect si l'un de vos trois derniers mots de passe était monmotdepasse.
- Autoriser ou non le mot de passe composé à contenir plus de trois caractères consécutifs, quel que soit leur emplacement, identiques au mot de passe précédent (non)  
Par exemple, par défaut, motdep est un mot de passe incorrect si votre mot de passe précédent était motde ou mdepasse.



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

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

Par exemple, par défaut, le mot de passe composé expire au bout de 184 jours. Le nouveau mot de passe composé doit respecter la stratégie de mot de passe composé établie.

- Indiquer si le mot de passe composé doit expirer (oui).

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

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

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

#### **Longueur**

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

#### **Caractères**

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

#### **Propriétés**

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

#### **Tentatives infructueuses**

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

---

## **Nombre d'échecs sur les systèmes utilisant le TPM national**

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

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

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

Les systèmes TPM nationaux ne font pas de distinction entre les mots de passe composés utilisateur et le mot de passe administrateur. Toute authentification par le biais de la puce de sécurité intégrée IBM répond à la même stratégie. Il n'existe pas de délai d'attente maximal. Chaque échec déclenche la période de suspension indiquée ci-dessus. Les périodes de suspension anti-martèlement ne prennent pas fin à la 118ème tentative ; elles continuent plutôt indéfiniment de la manière illustrée ci-dessus.

---

## Nombre d'échecs sur les systèmes utilisant le TPM Atmel

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

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

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

---

## Réinitialisation d'un mot de passe composé

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

## Réinitialisation à distance d'un mot de passe composé

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

- **Administrateurs**

Un administrateur distant doit exécuter la procédure suivante :

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

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

- **Utilisateurs**

L'utilisateur doit exécuter la procédure suivante :

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

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

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

## Réinitialisation manuelle d'un mot de passe composé

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



---

## Annexe C. 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 **Activation du remplacement de connexion Windows** dans l'utilitaire d'administration, le système revient à la procédure d'ouverture de session Windows sans protection UVM à l'ouverture de session.
- Vous pouvez indiquer le nombre maximal de tentatives d'entrée du mot de passe admises pour l'application d'ouverture de session Windows. Cette option *ne s'applique pas* à la protection d'ouverture de session UVM. Vous ne pouvez pas indiquer de valeur maximale comme nombre maximal de tentatives d'entrée du mot de passe composé UVM.



---

## **Annexe D. 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 E. Remarques

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

---

### Remarques

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

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

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

Pour le Canada, veuillez adresser votre courrier à :

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

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

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

Les licenciés souhaitant obtenir des informations permettant : (i) l'échange des données entre des logiciels créés de façon indépendante et d'autres logiciels (dont

celui-ci), et (ii) l'utilisation mutuelle des données ainsi échangées, doivent adresser leur demande à : IBM Corporation, Department 80D, P.O. Box 12195, 3039 Cornwallis, Research Triangle Park, NC 27709, U.S.A. Ces informations peuvent être soumises à des conditions particulières, prévoyant notamment le paiement d'une redevance.

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

---

## Marques

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

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

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

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



**IBM**