Solutions IBM Client Security

Utilisation du logiciel Client Security version 5.1 avec Tivoli Access Manager

Solutions IBM Client Security

Utilisation du logiciel Client Security version 5.1 avec Tivoli Access Manager

Important

Avant d'utiliser le présent document et le produit associé, prenez connaissance des informations générales figurant à l'Annexe A, «Réglementation américaine relative à l'exportation du logiciel Client Security», à la page 33 et à l'Annexe D, «**Remarques**», à la page 41.

Première édition - (avril 2003)

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

Table des matières

Avis aux lecteurs canadiens

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

Illustrations

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

Terminologie

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

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

Claviers

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

OS/2 et Windows - Paramètres canadiens

Au Canada, on utilise :

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

Nomenclature

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

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

Brevets

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

Assistance téléphonique

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

Avant-propos

Le présent guide contient des informations relatives à la configuration du logiciel Client Security en vue d'une utilisation avec IBM Tivoli Access Manager.

Ce guide est organisé de la façon suivante :

Le ″Chapitre 1, «**Introduction au logiciel IBM Client Security**»,″ contient une présentation des applications et des composants inclus dans le logiciel, ainsi qu'une description des fonctions de l'infrastructure PKI.

Le ″Chapitre 2, ″Installation du composant Client Security sur un serveur Tivoli Access Manager″, contient la description des conditions requises et les instructions d'installation du support Client Security sur votre serveur Tivoli Access Manager.

Le ″Chapitre 3, ″Configuration des clients IBM″, contient les informations relatives aux conditions requises et les instructions permettant de configurer les clients IBM afin qu'ils utilisent les services d'authentification offerts par Tivoli Access Manager.

Le ″Chapitre 4, «Identification des incidents»,″ contient des informations utiles à la résolution des incidents que vous pouvez rencontrer lors de l'utilisation des instructions fournies dans le présent guide.

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

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

L'″Annexe C, «**Règles d'utilisation de la protection UVM à l'ouverture de session sur le système**»,″ contient des informations relatives à la protection UVM lors de l'ouverture de session sur le système d'exploitation.

L'″Annexe D, «**Remarques**»,″ contient des remarques juridiques et des informations relatives aux marques.

A qui s'adresse ce guide

Le présent manuel est destiné aux administrateurs d'entreprises qui utiliseront Tivoli Access Manager version 3.8 ou 3.9 pour gérer les objets d'authentification définis par la stratégie de sécurité du gestionnaire de vérification d'utilisateur (UVM) sur un client IBM.

Les administrateurs doivent connaître les concepts et procédures suivants :

- Installation et gestion du protocole SecureWay Directory Lightweight Directory Access Protocol (LDAP)
- Procédures d'installation et de configuration de l'environnement d'exécution Tivoli Access Manager
- Gestion de l'espace objet Tivoli Access Manager

Comment utiliser ce guide

Ce guide vous permettra de configurer le support Client Security pour l'utiliser avec Tivoli Access Manager. Le présent guide est complémentaire des manuels *Logiciel Client Security –Guide d'installation*, *Logiciel Client Security – Guide de l'administrateur* et *Logiciel Client Security – Guide de l'utilisateur*.

Vous pouvez télécharger ce manuel ainsi que toute la documentation Client Security à partir du site Web IBM http://www.pc.ibm.com/ww/security/secdownload.html.

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

Des références au manuel *Logiciel Client Security – Guide d'installation* apparaissent dans le présent document. Après avoir défini et configuré le serveur Tivoli Access Manager et installé l'environnement d'exécution sur le client, installez le logiciel Client Security sur les clients IBM à l'aide des instructions du manuel *Logiciel Client Security – Guide d'installation*. Pour plus d'informations, reportez-vous au Chapitre 3, «Configuration des clients IBM», à la page 9.

Références au manuel *Logiciel Client Security – Guide de l'administrateur*

Des références au manuel *Logiciel Client Security – Guide de l'administrateur* apparaissent dans le présent document. Le manuel *Logiciel Client Security – Guide de l'administrateur* contient des informations relatives à la configuration de l'authentification utilisateur et de la stratégie UVM pour le client IBM. Après avoir installé le logiciel Client Security, aidez-vous de ce manuel pour configurer l'authentification utilisateur et la stratégie de sécurité. Pour plus d'informations, reportez-vous au Chapitre 3, «Configuration des clients IBM», à la page 9.

Informations complémentaires

Vous pouvez obtenir des informations complémentaires et des mises à jour du produit de sécurité, lorsqu'elles sont disponibles, à partir du site Web IBM http://www.pc.ibm.com/ww/security/securitychip.html.

Chapitre 1. Introduction au logiciel IBM Client Security

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

Applications et composants du logiciel Client Security

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

- **Utilitaire d'administration :** Cet utilitaire est l'interface que l'administrateur utilise pour activer ou désactiver la puce de sécurité intégrée et pour créer, archiver et régénérer les clés de chiffrement et les mots de passe composés. En outre, l'administrateur peut ajouter des utilisateurs dans la stratégie de sécurité fournie par le logiciel Client Security.
- **Gestionnaire de vérification d'utilisateur (UVM) :** Le logiciel Client Security utilise le gestionnaire UVM pour gérer les mots de passe composés et d'autres éléments d'authentification des utilisateurs du système. Par exemple, un lecteur d'empreintes digitales peut être utilisé par le gestionnaire UVM pour l'authentification à l'ouverture de session. Le logiciel UVM offre les fonctions suivantes :
  - **Protection de stratégie client UVM :** Le logiciel UVM permet à l'administrateur de définir la stratégie de sécurité du client, qui régit le mode d'identification de l'utilisateur client sur le système.

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

Fonctions PKI (Public Key Infrastructure)

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

- **Contrôle de l'administrateur sur la stratégie de sécurité client.** Pour des raisons de stratégie de sécurité, il est essentiel d'authentifier les utilisateurs finals au niveau du client. Le logiciel Client Security offre l'interface requise pour gérer la stratégie de sécurité d'un client IBM. Cette interface fait partie du logiciel d'authentification UVM (Gestionnaire de vérification utilisateur), composant principal du logiciel Client Security.
- **Gestion des clés de chiffrement pour la cryptographie de clés publiques.** A l'aide du logiciel Client Security, les administrateurs créent des clés de chiffrement pour le matériel informatique et les utilisateurs clients. Une fois les clés de chiffrement créées, elles sont liées à la puce de sécurité intégrée IBM par l'intermédiaire d'une hiérarchie de clés, dans laquelle la clé matériel de base permet de chiffrer les clés de niveau supérieur, y compris les clés utilisateur associées à chaque utilisateur client. Le chiffrement et le stockage des clés dans la puce de sécurité intégrée IBM ajoute un niveau supplémentaire de sécurité du client car les clés sont intimement liées au matériel informatique.
- **Création de certificats numériques et stockage protégé par la puce de sécurité intégrée IBM.** Lorsque vous faites une demande de certificat numérique à utiliser pour la signature et le chiffrement numérique d'un message électronique, le logiciel Client Security vous permet de choisir la puce de sécurité intégrée IBM comme fournisseur de service pour les applications utilisant Microsoft CryptoAPI. Il peut s'agir des applications Internet Explorer et Microsoft Outlook Express. Ainsi, la clé privée du certificat numérique est stockée sur la puce de sécurité. De même, les utilisateurs de Netscape peuvent choisir la puce de sécurité intégrée IBM comme générateur de clé privée pour les certificats numériques utilisés pour la sécurité. Les applications utilisant la norme PKCS (Public-Key Cryptography Standard) n° 11, telles que Netscape Messenger, peuvent bénéficier de la protection fournie par la puce de sécurité intégrée IBM.
- **Possibilité de transférer les certificats numériques à la puce de sécurité intégrée IBM.** L'outil de transfert de certificats du logiciel IBM Client Security vous permet de déplacer les certificats qui ont été créés avec le fournisseur de service cryptographique Microsoft par défaut vers le fournisseur de service cryptographique de la puce de sécurité intégrée IBM. Cela augmente fortement le niveau de protection des clés privées associées aux certificats car elles sont maintenant stockées en toute sécurité sur la puce de sécurité intégrée IBM plutôt que dans un logiciel vulnérable.
- **Archive de clés et solutions de reprise.** L'une des fonctions importantes de l'architecture PKI est de permettre la création d'une archive de clés, à partir de laquelle des clés peuvent être restaurées en cas de perte des clés d'origine ou si celles-ci sont endommagées. Le logiciel Client Security offre une interface permettant de générer une archive pour les clés et les certificats numériques créés à l'aide de la puce de sécurité intégrée IBM et de les restaurer si nécessaire.
- **Chiffrement des fichiers et des dossiers.** La fonction de chiffrement des fichiers et des dossiers permet à l'utilisateur client de chiffrer ou de déchiffrer rapidement et simplement des fichiers ou des dossiers. Cette fonction s'ajoute aux mesures de sécurité du système CSS pour améliorer le niveau de sécurité des données.
- **Authentification des empreintes digitales.** Le logiciel IBM Client Security prend en charge les lecteurs d'empreintes digitales Targus PC Card et Targus

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

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

Chapitre 2. Installation du composant Client Security sur un serveur Tivoli Access Manager

Pour des raisons 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 Gestionnaire de vérification utilisateur, composant principal du logiciel Client Security.

Pour un client IBM, la stratégie de sécurité UVM peut être gérée de deux façons :

- Localement, à l'aide de l'éditeur de stratégie qui réside sur le client IBM
- Sur l'ensemble de l'entreprise, à l'aide de Tivoli Access Manager

Pour que Client Security puisse être utilisé avec Tivoli Access Manager, le composant Client Security de Tivoli Access Manager doit être installé. Vous pouvez le télécharger à partir du site Web IBM http://www.pc.ibm.com/ww/security/secdownload.html.

Conditions requises

Pour qu'une connexion sécurisée puisse être établie entre le client IBM et le serveur Tivoli Access Manager, vous devez installer les composants suivants sur le client IBM :

- IBM Global Security Toolkit
- IBM SecureWay Directory Client
- Tivoli Access Manager Runtime Environment

Pour plus de détails sur l'installation et l'utilisation de Tivoli Access Manager, consultez la documentation présente sur le site Web http://www.tivoli.com/products/index/secureway_policy_dir/index.htm.

Téléchargement et installation du composant Client Security

Le composant Client Security peut être téléchargé gratuitement du site Web IBM.

Pour télécharger et installer Client Security sur le serveur Tivoli Access Manager et sur le client IBM, procédez comme suit :

1. A partir des informations figurant sur le site Web, assurez-vous que la puce de sécurité intégrée IBM figure sur votre système en vérifiant la correspondance de votre numéro de modèle avec celui fourni dans le tableau des composants système requis, puis cliquez sur **Poursuite**.
2. Sélectionnez le bouton d'option qui correspond à votre type de machine et cliquez sur **Poursuite**.
3. Créez un ID utilisateur, enregistrez-le auprès d'IBM en remplissant le formulaire en ligne, puis lisez le Contrat de licence et cliquez sur **Oui** pour accepter la licence.

   Vous serez automatiquement redirigé vers la page de téléchargement de Client Security.
4. Suivez les étapes indiquées dans la page de téléchargement pour installer les pilotes de périphérique nécessaires, fichiers readme, logiciels, documents de référence et autres utilitaires complémentaires.

5. Installez le Logiciel Client Security Software en procédant comme suit :
   a. A partir du bureau Windows, cliquez sur **Démarrer > Exécuter**.
   b. Dans la zone Exécuter, entrez `d:\directory\csec50.exe`, où d:\directory\ est l'indicatif d'unité et le répertoire où se trouve le fichier.
   c. Cliquez sur **OK**.

      La fenêtre de bienvenue de l'assistant d'installation InstallShield pour IBM Client Security s'affiche.
   d. Cliquez sur **Suivant**.

      L'assistant extrait les fichiers et installe le logiciel. Une fois l'installation terminée, vous avez le choix entre redémarrer l'ordinateur immédiatement ou ultérieurement.
   e. Sélectionnez le bouton d'option approprié et cliquez sur **OK**.
6. Une fois le système redémarré, à partir du bureau Windows, cliquez sur **Démarrer > Exécuter**.
7. Dans la zone Exécuter, entrez `d:\directory\TAMCSS.exe`, où d:\directory\ est l'indicatif d'unité et le répertoire où se trouve le fichier. Vous pouvez aussi cliquer sur **Parcourir** afin de localiser le fichier.
8. Cliquez sur **OK**.
9. Indiquez un dossier cible et cliquez sur **Unzip**.

   L'assistant extrait les fichiers dans le dossier indiqué. Un message indique que les fichiers ont été décompressés.
10. Cliquez sur **OK**.

Ajout des composants Client Security sur le serveur Tivoli Access Manager

L'utilitaire pdadmin est un outil de ligne de commande que l'administrateur peut utiliser pour effectuer la plupart des tâches d'administration de Tivoli Access Manager. L'exécution de plusieurs commandes permet à l'administrateur d'utiliser un fichier contenant plusieurs commandes pdadmin pour exécuter une tâche entière ou une série de tâches. La communication entre l'utilitaire pdadmin et le serveur de gestion (pdmgrd) est sécurisée via SSL. L'utilitaire pdadmin est installé avec le progiciel Tivoli Access Manager Runtime Environment.

L'utilitaire pdadmin accepte un argument de nom de chemin qui identifie l'emplacement de ce fichier, par exemple :

```
MSDOS>pdadmin [-a <admin-util >][-p <mot-de-passe>]<chemin-fichier >
```

La commande ci-après illustre le mode de création de l'espace objet IBM Solutions, d'actions Client Security et d'entrées ACL individuelles sur le serveur Tivoli Access Manager.

```
MSDOS>pdadmin -a resp_sécurité -p mot_de_passe
C:\TAM_Add_ClientSecurity.txt
```

Pour plus d'informations sur l'utilitaire pdadmin et sa syntaxe de commande, reportez-vous au manuel *Tivoli Access Manager Guide*.

Etablissement d'une connexion sécurisée entre le client IBM et le serveur Tivoli Access Manager

Le client IBM doit définir sa propre identité authentifiée au sein du domaine sécurisé Tivoli Access Manager afin de demander des décisions d'autorisation au service Tivoli Access Manager Authorization.

Une identité unique doit être créée pour l'application dans le domaine sécurisé Tivoli Access Manager. Pour que l'identité authentifiée effectue des vérifications d'authentification, l'application doit être membre du groupe d'utilisateurs ACL éloignés. Lorsque l'application veut prendre contact avec l'un des services du domaine sécurisé, elle doit d'abord ouvrir une session sur le domaine.

L'utilitaire svrsslcfg permet aux applications IBM Client Security de communiquer avec le serveur de gestion Tivoli Access Manager et avec le serveur d'autorisation.

L'utilitaire svrsslcfg permet aux applications IBM Client Security de communiquer avec le serveur de gestion Tivoli Access Manager et avec le serveur d'autorisation.

Il permet d'exécuter les tâches suivantes :

- Création d'une identité utilisateur pour l'application. Par exemple, UtilDémo/NOMHOTE
- Création d'un fichier de clés SSL pour cet utilisateur. Par exemple, UtilDemo.kdb et UtilDemo.sth
- Ajout de l'utilisateur dans un groupe d'utilisateurs ACL éloignés

Les paramètres suivants sont nécessaires :

- **-f fichier_cfg** Chemin et nom du fichier de configuration. Utilisez TAMCSS.conf.
- **-d rép_kdb** Répertoire devant contenir les fichiers de base de données de fichiers de clés pour le serveur.
- **-n nom_serveur** Nom réel Windows/UVM de l'utilisateur client IBM voulu.
- **-P mdp_admin** Mot de passe de l'administrateur de Tivoli Access Manager.
- **-s type_serveur** Vous devez indiquer qu'il s'agit d'un serveur éloigné.
- **-S mdp_serveur** Mot de passe du nouvel utilisateur. Ce paramètre est obligatoire.
- **-r n°_port** Définit le numéro de port d'écoute pour le client IBM. Il s'agit du paramètre indiqué comme port du serveur SSL variable de Tivoli Access Manager Runtime pour le serveur de gestion de Tivoli Access Manager.
- **-e pwd_life** Définit le délai d'expiration (en nombre de jours) du mot de passe.

Pour établir une connexion sécurisée entre le client IBM et le serveur Tivoli Access Manager, procédez comme suit :

1. Créez un répertoire et placez-y le fichier TAMCSS.conf.

   Par exemple, `MSDOS> mkdir C:\TAMCSS MSDOS> move C:\TAMCSS.conf C:\TAMCSS\`
2. Exécutez svrsslcfg pour créer l'utilisateur.

   MSDOS> svrsslcfg -config -f C:\TAMCSS\TAMCSS.conf -d C:\TAMCSS\ -n <nom_serveur> - s remote -S <mdp_serveur> -P <mdp_admin> -e 365 -r 199

   Remarque : Remplacez <nom_serveur> par le nom d'utilisateur et le nom d'hôte UVM du client IBM. Par exemple : –n UtilDémo/NomHôte. Pour trouver le nom d'hôte du client IBM, vous pouvez taper la

commande “hostname” à l’invite MSDOS. L’utilitaire svrsslcfg va créer une entrée correcte sur le serveur Tivoli Access Manager et fournir un fichier de clés SSL unique pour les communications chiffrées.

3. Exécutez svrsslcfg pour ajouter l’emplacement de ivacld dans le fichier TAMCSS.conf.

   Par défaut, le serveur Tivoli Access Manager Authorization écoute sur le port 7136. Vous pouvez le vérifier en recherchant la valeur du paramètre tcp_req_port dans le paragraphe ivacld du fichier ivacld.conf sur le serveur Tivoli Access Manager. Il est important que vous disposiez du nom d’hôte ivacld correct. Pour obtenir cette information, utilisez la commande de liste de serveurs pdadmin. Les serveurs portent le nom : <nom_serveur>-<nom_hôte>. Voici un exemple d’exécution de commande de liste de serveurs pdadmin :

```
MSDOS> pdadmin server list ivacld-MonHôte.ibm.com
```

La commande ci-après permet ensuite d’ajouter une entrée réplique pour le serveur ivacld affiché précédemment. Il est entendu que ivacld écoute sur le port par défaut 7136.

```
svrsslcfg -add_replica  -f <chemin fichier config> -h <nom_hôte>
MSDOS>svrsslcfg -add_replica  -f C:\TAMCSS\TAMCSS.conf -h MonHôte.ibm.com
```

Chapitre 3. Configuration des clients IBM

Avant de pouvoir utiliser Tivoli Access Manager afin de contrôler les objets d'authentification pour les clients IBM, vous devez configurer chaque client à l'aide de l'utilitaire d'administration, composant fourni avec le logiciel Client Security. Dans la présente section, sont décrites les conditions requises et les instructions relatives à la configuration des clients IBM.

Conditions requises

Vérifiez que les logiciels ci-après sont installés sur le client IBM, dans l'ordre suivant :

1. **Système d'exploitation Microsoft Windows pris en charge.** Vous pouvez utiliser Tivoli Access pour contrôler les conditions d'authentification des clients IBM dotés de Windows XP, Windows 2000 ou Windows NT Workstation 4.0.
2. **Logiciel Client Security version 3.0 ou supérieure.** Après avoir installé le logiciel et activé la puce de sécurité intégrée IBM, vous pouvez utiliser l'utilitaire d'administration de la sécurité client pour configurer l'authentification d'utilisateur et éditer la stratégie de sécurité UVM. Pour connaître toutes les instructions d'installation et d'utilisation du logiciel Client Security, reportez-vous aux manuels *Logiciel Client Security – Guide d'installation* et *Logiciel Client Security – Guide de l'administrateur*.

Définition des informations de configuration de Tivoli Access Manager

Une fois Tivoli Access Manager installé sur le client local, vous pouvez définir les informations de configuration d'Access Manager à l'aide de l'utilitaire d'administration, composant fourni par le logiciel Client Security. Ces informations sont constituées des éléments suivants :

- Choix du chemin d'accès complet aux fichiers de configuration.
- Choix de la fréquence de régénération de la mémoire cache locale.

Pour définir les informations de configuration de Tivoli Access Manager sur le client IBM, suivez la procédure ci-après :

1. Cliquez sur **Démarrer > Paramètres > Panneau de configuration > Sous-système de sécurité client IBM**.
2. Tapez le mot de passe administrateur et cliquez sur **OK**.

   Une fois le mot de passe saisi, la fenêtre principale de l'utilitaire d'administration s'ouvre.
3. Cliquez sur le bouton **Configuration du support d'application et des stratégies**.

   L'écran Configuration des applications UVM et des stratégies s'affiche.
4. Sélectionnez la case à cocher **Remplacement de la fenêtre de connexion standard de Windows par la fenêtre de connexion sécurisée UVM**.
5. Dans la zone d'information de configuration de Tivoli Access Manager, sélectionnez le chemin d'accès complet au fichier de configuration TAMCSS.conf. Exemple : `C:\TAMCSS\TAMCSS.conf`

   Tivoli Access Manager doit être installé sur le client pour que cette zone soit disponible.
6. Cliquez sur le bouton **Stratégie d'application**.
7. Cliquez sur le bouton **Edition de la stratégie**.

L'écran Saisie du mot de passe administrateur s'affiche.

8. Tapez le mot de passe administrateur dans la zone prévue à cet effet et cliquez sur **OK**.

   L'écran Stratégie UVM s'affiche.

9. Sélectionnez les actions que vous voulez voir contrôlées par Tivoli Access Manager à partir du menu déroulant Actions.
10. Cochez la case en regard de l'option Access Manager contrôle l'objet sélectionné.
11. Cliquez sur **Validation**.

    Les modifications entrent en vigueur à la régénération suivante de la mémoire cache. Si vous souhaitez que les modifications soient immédiatement appliquée, cliquez sur le bouton **Régénération de la mémoire cache locale**.

Configuration et utilisation du dispositif de mémoire cache locale

Après avoir sélectionné le fichier de configuration de Tivoli Access Manager, vous pouvez définir la fréquence de régénération de la mémoire cache locale. Une réplique locale des informations de stratégie de sécurité, telles qu'elles sont gérées par Tivoli Access Manager, est conservée sur le client IBM. Vous pouvez planifier une régénération automatique de la mémoire cache locale par incréments de mois (0-12) ou de jours (0-30).

Pour définir ou régénérer la mémoire cache locale, suivez la procédure ci-après.

1. Cliquez sur **Démarrer > Programmes > Utilitaires du logiciel Client Security > Utilitaire d'administration**.
2. Tapez le mot de passe matériel et cliquez sur **OK**.

   La fenêtre Utilitaire d'administration s'ouvre. Pour connaître les informations relatives à l'utilisation de l'utilitaire d'administration, reportez-vous au manuel *Logiciel Client Security – Guide de l'administrateur*.

3. Dans l'utilitaire d'administration, cliquez sur le bouton **Configuration du support d'application et des stratégies**.

   L'écran Modification de la configuration de stratégie de Client Security s'affiche.

4. Effectuez l'une des opérations suivantes :
   - Pour régénérer la mémoire cache locale immédiatement, cliquez sur **Régénération de la mémoire cache**.
   - Pour définir la fréquence de régénération automatique, tapez le nombre de mois (de 0 à 12) et de jours (de 0 à 30) voulus dans les zones affichées et cliquez sur **Régénération de la mémoire cache locale**. La mémoire cache locale et la date de péremption du fichier seront mises a mise à jour afin d'indiquer la date de la prochaine régénération automatique.

Activation de Tivoli Access Manager pour contrôler les objets du client IBM

La stratégie UVM est contrôlée par le biais d'un fichier de stratégie globale. Le fichier de stratégie globale, appelé fichier de stratégie UVM, contient des conditions d'authentification requises pour les actions effectuées sur le système client IBM, telles que l'ouverture de session sur le système, la désactivation de l'économiseur d'écran ou la signature de messages de courrier électronique.

Pour pouvoir activer Tivoli Access Manager afin de contrôler les objets d'authentification pour un client IBM, éditez le fichier de stratégie UVM à l'aide de l'éditeur de stratégie UVM. L'éditeur de stratégie UVM fait partie de l'utilitaire d'administration.

Important : L'activation de Tivoli Access Manager pour contrôler un objet donne le contrôle sur les objets à l'espace objet Tivoli Access Manager. Si vous l'activez, vous devez réinstaller le logiciel Client Security pour rétablir le contrôle local sur cet objet.

Edition d'une stratégie UVM locale

Avant de tenter d'éditer la stratégie UVM pour le client local, vérifiez qu'un utilisateur au moins est inscrit dans le gestionnaire UVM. Dans le cas contraire, un message d'erreur s'affiche lorsque l'éditeur de stratégie tente d'ouvrir le fichier de stratégie local.

Après avoir édité une stratégie UVM locale, vous ne pouvez l'utiliser que sur le client sur lequel elle a été éditée. Si vous avez installé Client Security dans le répertoire par défaut, la stratégie UVM locale est stockée sous le nom \Program Files\IBM\Security\UVM_Policy\globalpolicy.gvm. Seul les utilisateurs ajoutés au gestionnaire UVM peuvent utiliser l'éditeur de stratégie UVM.

Remarque : Si vous définissez dans la stratégie UVM que les empreintes digitales sont obligatoires pour un objet d'authentification (tel que l'ouverture de session sur le système d'exploitation), les empreintes des utilisateurs qui sont ajoutés à UVM doivent être enregistrées pour que ceux-ci puissent utiliser cet objet.

Pour démarrer l'éditeur de stratégie UVM, suivez la procédure de l'utilitaire d'administration ci-après.

1. Cliquez sur le bouton **Configuration du support d'application et des stratégies**.

   L'écran Modification de la configuration de stratégie de Client Security s'affiche.
2. Cliquez sur le bouton **Edition de la stratégie**.

   L'écran Saisie du mot de passe administrateur s'affiche.
3. Tapez le mot de passe administrateur dans la zone prévue à cet effet et cliquez sur **OK**.

   L'écran Stratégie UVM s'affiche.
4. Cliquez sur l'onglet Sélection d'objet, puis sur **Action** ou sur **Type d'objet**, puis sélectionnez l'objet auquel vous voulez affecter des conditions d'authentification.

   Exemples d'actions admises : ouverture de session sur le système, déverrouillage du système, déchiffrement du courrier électronique ; exemple de type d'objet : acquisition de certificat numérique.
5. Pour chaque objet que vous sélectionnez, choisissez **Tivoli Access Manager contrôle l'objet sélectionné** pour activer Tivoli Access pour cet objet.

   Important : Si vous activez Tivoli Access Manager pour contrôler un objet, vous donnez le contrôle sur les objets à l'espace objet Tivoli Access Manager. Si vous voulez, par la suite, rétablir le contrôle local sur cet objet, vous devez réinstaller le logiciel Client Security.

   Remarque : Lorsque vous éditez la stratégie UVM, vous pouvez visualiser le récapitulatif de la stratégie en cliquant sur **Récapitulatif de la stratégie**.

6. Cliquez sur **Validation** pour sauvegarder vos modifications.
7. Cliquez sur **OK** pour sortir.

Edition et utilisation de stratégie UVM pour des clients éloignés

Pour utiliser une stratégie UVM sur plusieurs clients IBM, éditez et sauvegardez la stratégie UVM pour un client éloigné, puis copiez le fichier de stratégie sur les autres clients. Si vous installez Client Security dans le répertoire par défaut, le fichier de stratégie UVM est stocké sous le nom \Program Files\IBM\Security\UVM_Policy\remote\globalpolicy.gvm.

Copiez les fichiers suivants sur les autres clients IBM éloignés qui utiliseront 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 dans son répertoire par défaut, le répertoire racine pour les chemins précédents doit être le répertoire \Program Files.Copiez les deux fichiers dans le répertoire \IBM\Security\UVM_Policy\ sur les clients éloignés.

Chapitre 4. Identification des incidents

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

Fonctions d'administrateur

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

Définition d'un mot de passe administrateur (ThinkCentre)

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

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

Important :

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

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

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

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

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

   Le menu principal du programme Configuration/Setup Utility s'affiche.
3. Sélectionnez **System Security**.
4. Sélectionnez **Administrator Password**.
5. Tapez votre mot de passe et appuyez sur la flèche de défilement vers le bas de votre clavier.
6. Retapez votre mot de passe et appuyez sur la flèche de défilement vers le bas.
7. Sélectionnez **Change Administrator password** et appuyez sur Entrée ; appuyez de nouveau sur Entrée.
8. Appuyez sur **Echap** pour sortir et sauvegarder les paramètres.

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

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

Définition d'un mot de passe superviseur (ThinkPad)

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

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

Important :

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

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

  Lorsque la puce de sécurité intégrée IBM est vidée, toutes les clés de chiffrement et tous les certificats stockés sur la puce sont perdus.
- Il est nécessaire de désactiver temporairement le mot de passe superviseur sur certains modèles de ThinkPad avant d'installer ou de mettre à niveau le logiciel Client Security.

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

Pour définir un mot de passe superviseur, exécutez la procédure suivante :

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

   Le menu principal de l'utilitaire de configuration du BIOS IBM s'affiche.
3. Sélectionnez **Password**.
4. Sélectionnez **Supervisor Password**.
5. Tapez votre mot de passe et appuyez sur Entrée.
6. Retapez votre mot de passe et appuyez sur Entrée.
7. Cliquez sur **Continue**.
8. Appuyez sur F10 pour sauvegarder et sortir.

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

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

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

Protection du mot de passe matériel

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

Vidage de la puce de sécurité intégrée IBM (ThinkCentre)

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

Important :

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

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

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

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

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

Vidage de la puce de sécurité intégrée IBM (ThinkPad)

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

Important :

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

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

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

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

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

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

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

Utilitaire d'administration

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

Suppression d'utilisateurs

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

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

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

Limites connues

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

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

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

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

Utilisation du logiciel Client Security avec des applications Netscape

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

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

- SHA-1
- MD5

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

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

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

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

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

Utilisation de la protection UVM pour un ID utilisateur Lotus Notes

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

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

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

Limites de l'utilitaire de configuration utilisateur

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

Windows XP Professionnel

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

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

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

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

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

Windows XP Edition familiale

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

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

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

Messages d'erreur

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

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

Tableaux d'identification des incidents

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

Identification des incidents liés à l'installation

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

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

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

Identification des incidents liés à l'utilitaire d'administration

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

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

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

Identification des incidents relatifs à l'utilitaire de configuration utilisateur

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

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

Identification des incidents liés aux ThinkPad

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

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

Identification des incidents liés aux applications Microsoft

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

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

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

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

Identification des incidents relatifs aux applications Netscape

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

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

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

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

Identification des incidents relatifs à un certificat numérique

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

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

Identification des incidents relatifs à Tivoli Access Manager

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

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

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

Identification des incidents relatifs à Lotus Notes

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

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

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

Identification des incidents relatifs au chiffrement

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

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

Identification des incidents relatifs aux périphériques compatibles UVM

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

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

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

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

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

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

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

Règles applicables aux mots de passe matériel

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

Longueur
Le mot de passe doit contenir exactement huit caractères.

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

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

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

Règles relatives aux mots de passe composés UVM

Pour améliorer la sécurité, le mot de passe composé UVM est plus long qu'un mot de passe traditionnel. La stratégie de mot de passe composé UVM est contrôlée par l'utilitaire d'administration IBM Client Security.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Propriétés

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

Tentatives infructueuses

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

Annexe C. 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 décochez la case **Remplacement de la fenêtre de connexion standard de Windows par la fenêtre de connexion sécurisée UVM** dans l'utilitaire d'administration, le système revient au processus 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. 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.

Référence : 59P7639

(1P) P/N: 59P7639