Solutions IBM Client Security

Password Manager version 1.4
Guide d'utilisation

Solutions IBM Client Security

Password Manager version 1.4
Guide d'utilisation

Première édition - septembre 2004

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 sur l'utilisation d'IBM Client Security Password Manager pour assurer la gestion et l'extraction des informations d'ouverture de session.

Ce guide est organisé comme suit :

Le Chapitre 1, «Présentation d'IBM Client Security Password Manager», contient la présentation des fonctions et caractéristiques d'IBM Password Manager.

Le Chapitre 2, «Procédures», contient les procédures d'utilisation d'IBM Client Security Password Manager pour définir, extraire et gérer les informations d'ouverture de session.

Le Chapitre 3, «Limitations», contient des informations utiles permettant de contourner les limitations connues d'IBM Password Manager.

A qui s'adresse ce guide ?

Ce guide est destiné aux utilisateurs du logiciel Client Security version 4.0 ou suivante qui souhaitent conserver une trace de leurs ID utilisateur, de leurs mots de passe et des informations personnelles qui sont utilisées lors de chaque enregistrement et ouverture de session sur des sites Web ou des applications.

IBM Client Security Password Manager version 1.4 prend en charge les systèmes d'exploitation Windows 2000 et Windows XP.

Utilisation du guide

Ce guide est conçu pour vous aider à utiliser IBM Client Security Password Manager afin de faciliter vos procédures d'ouverture de session et la gestion de vos mots de passe.

Ce guide, ainsi que toutes les autres documentations Client Security, sont accessibles à partir du site Web IBM http://www.pc.ibm.com/us/security/index.html.

Informations complémentaires

Pour vous procurer des informations complémentaires et des mises à jour de sécurité, le cas échéant, consultez le site Web IBM http://www.pc.ibm.com/us/security/index.html.

Chapitre 1. Présentation d'IBM Client Security Password Manager

IBM Client Security Password Manager permet de gérer, via IBM Client Security, toutes les informations d'ouverture de session sensibles et faciles à oublier, telles que les ID utilisateur, les mots de passe et les autres informations personnelles. IBM Client Security Password Manager stocke toutes ces informations via le sous-système de sécurité intégré IBM afin que votre stratégie d'authentification utilisateur UVM puisse contrôler l'accès aux applications et aux sites Web sécurisés.

Cela signifie qu'au lieu de devoir vous souvenir d'une multitude de mots de passe individuels (faisant tous l'objet de règles ou de dates d'expiration différentes), il vous suffit de vous souvenir d'un mot de passe composé, de fournir votre empreinte digitale ou votre badge de proximité, ou encore de fournir une combinaison de ces éléments d'identification.

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

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

  IBM Password Manager chiffre automatiquement toutes les informations via le sous-système de sécurité intégré IBM. Vous êtes ainsi assuré de la sécurisation de toutes les informations de mot de passe à l'aide des clés de chiffrement IBM Client Security.
- **Transfert rapide et facile des ID utilisateur et des mots de passe grâce à l'utilisation d'une interface de saisie-et-transfert**

  Utilisez l'interface de saisie-et-transfert IBM Password Manager pour placer directement les informations dans la boîte de dialogue d'ouverture de session du navigateur Web ou de l'application. Cet outil permet de minimiser les risques de faute de frappe et de sauvegarder toutes les informations en toute sécurité via le sous-système de sécurité intégré IBM.
- **Saisie automatique des ID utilisateur et des mots de passe**

  IBM Password Manager automatise le processus d'ouverture de session en saisissant automatiquement les informations d'ouverture de session lorsque vous accédez aux sites Web pris en compte dans IBM Password Manager.
- **Exportation des informations de connexion sensibles sur un navigateur sécurisé**

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

  IBM Password Manager permet de générer des mots de passe aléatoires pour chaque site Web ou application. Vous pouvez ainsi accroître la sécurité des données car chaque application disposera d'une protection par mot de passe plus rigoureuse. Les mots de passe aléatoires sont beaucoup plus sûrs que les mots de passe définis par les utilisateurs car l'expérience prouve que la plupart

des utilisateurs utilisent des informations personnelles faciles à mémoriser qui sont souvent relativement faciles à deviner.

- **Edition des entrées à l'aide de l'interface Password Manager**

  IBM Password Manager permet d'éditer toutes les entrées de compte et de définir toutes les fonctions de mot de passe facultatives à l'aide d'une interface d'utilisation facile. La gestion des mots de passe et des informations personnelles est ainsi facilitée.

- **Accès à Password Manager à partir de la barre d'icônes du bureau Windows ou à l'aide d'un simple raccourci clavier**

  L'icône IBM Password Manager vous permet d'accéder instantanément à Password Manager, chaque fois que vous souhaitez lui ajouter une autre application, en particulier à partir du Web. Vous pouvez également accéder à chaque fonction Password Manager à l'aide d'un raccourci clavier.

- **Archivage des informations d'ouverture de session**

  Grâce à la fonction d'archivage de Client Security, IBM Password Manager vous permet de restaurer les informations d'ouverture de session à partir d'une archive Client Security afin de les protéger contre une éventuelle défaillance du disque dur ou du système. Pour plus d'informations sur l'archivage des informations, reportez-vous au manuel *Logiciel Client Security - Guide de l'utilisateur*.

Chapitre 2. Procédures

Cette section vous indique pas-à-pas comment exécuter les fonctions courantes d'IBM Client Security Password Manager.

Création de nouvelles entrées

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

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

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

   Remarque : Vous pouvez également accéder à la fonction Créer de Password Manager à l'aide du raccourci clavier **Ctrl+Maj+H**.
3. Tapez les informations destinées à une zone dans la fenêtre Password Manager - Création d'une nouvelle entrée.

   Remarque : Les informations de cette zone doivent comporter moins de 260 caractères.
4. Si vous ne souhaitez pas que le texte saisi soit affiché, cochez la case **Masquer le texte saisi**.

   Remarque : Cette case à cocher permet uniquement de contrôler l'affichage du texte dans Password Manager. Une fois le texte intégré au site Web ou à l'application, c'est l'application concernée qui contrôlera les propriétés du texte.
5. Utilisez l'icône "cible" Sélection d'une zone pour transférer le texte de Password Manager dans la zone appropriée du site Web ou de l'application.

   Remarque : Cette icône permet de copier le texte sans utiliser le presse-papiers de l'ordinateur ou d'autres outils non sécurisés.
6. Répétez les étapes 3 à 5 pour chaque zone, le cas échéant.
7. Cliquez sur l'option de **sauvegarde de nouvelle entrée**.
8. Entrez un nom explicite pour la nouvelle entrée.
9. Cochez la case **Ajouter "Entrée" pour transmission automatique** si vous souhaitez que Password Manager transmette les informations d'ouverture de session après leur extraction.

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

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

Extraction d'entrées

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

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

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

   Remarque : Vous pouvez également accéder à la fonction Extraire de Password Manager à l'aide du raccourci clavier **Ctrl+Maj+G**.
3. Tapez votre mot de passe composé UVM ou exécutez les opérations d'accès requises par la stratégie d'authentification utilisateur UVM.
4. Si la case **Ajouter "Entrée" pour transmission automatique** n'est pas cochée, cliquez sur le bouton de transmission de l'application ou du site Web.

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

Gestion des entrées

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

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

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

   Remarque : Vous pouvez également accéder à la fonction Gérer de Password Manager à l'aide du raccourci clavier **Ctrl+Maj+B**.
2. Tapez votre mot de passe composé UVM ou exécutez les opérations d'accès requises par la stratégie d'authentification utilisateur UVM.
3. Modifiez les informations. Choisissez l'une des options suivantes :
   - Informations d'entrée

     Pour modifier les informations d'entrée, procédez comme suit :
     a. Cliquez à l'aide du bouton droit de la souris sur l'entrée à modifier.
     b. Sélectionnez l'une des actions suivantes :
        – Ajouter "Entrée"

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

– Supprimer

Sélectionnez Supprimer pour supprimer totalement une entrée.

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

• Informations de la zone de saisie

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

a. Cliquez à l'aide du bouton droit de la souris sur la zone à modifier.

b. Sélectionnez l'une des actions suivantes :

– Modifier la zone d'entrée

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

- Création d'une entrée aléatoire

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

- Modification manuelle d'une zone d'entrée

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

– Supprimer

Sélectionnez Supprimer pour supprimer totalement une zone d'entrée.

Remarque : La modification d'une zone de Password Manager met les informations d'ouverture de session à jour uniquement dans Password Manager. Si vous voulez améliorer la sécurité de vos mots de passe à l'aide de la fonction de génération d'entrée aléatoire de Password Manager, vous devez synchroniser l'application ou le site Web avec le nouveau mot de passe aléatoire généré par cette fonction. Utilisez l'outil de transfert de zones de Password Manager pour transférer le nouveau mot de passe aléatoire dans le formulaire de changement de mot de passe de l'application ou du site Web. Vérifiez que le nouveau mot de passe est admis pour l'application ou le site Web, puis sélectionnez l'option Enregistrer les modifications dans la fenêtre de gestion des entrées de Password Manager. Il est inutile de recréer l'entrée avec le nouveau mot de passe étant donné que toutes les informations nécessaires ont été conservées.

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

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

Exportation des informations de connexion

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

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

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

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

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

Chapitre 3. Limitations

Cette section contient des informations sur les limitations connues concernant IBM Client Security Password Manager.

Pas de prise en charge de Netscape Navigator par IBM Client Security Password Manager : Vous devez utiliser Microsoft Internet Explorer pour exploiter les fonctionnalités du programme IBM Password Manager. Password Manager ne prend pas en charge Netscape Navigator.

Annexe. Remarques

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

Remarques

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

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

IBM EMEA Director of Licensing
IBM Europe Middle-East Africa
Tour Descartes
La Défense 5
2, avenue Gambetta
92066 - Paris-La Défense CEDEX
France

Pour le Canada, veuillez adresser votre courrier à :

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

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

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

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

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

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

Marques

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

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

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

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