IBM Client Security Solutions

Password Manager Version 1.4 Benutzerhandbuch

IBM Client Security Solutions

Password Manager Version 1.4 Benutzerhandbuch

Anmerkung:

- Die IBM Homepage finden Sie im Internet unter: **ibm.com**
- IBM und das IBM Logo sind eingetragene Marken der International Business Machines Corporation.
- Das e-business-Symbol ist eine Marke der International Business Machines Corporation.
- Infoprint ist eine eingetragene Marke der IBM.
- ActionMedia, LANDesk, MMX, Pentium und ProShare sind Marken der Intel Corporation in den USA und/oder anderen Ländern.
- C-bus ist eine Marke der Corollary, Inc. in den USA und/oder anderen Ländern.
- Java und alle auf Java basierenden Marken und Logos sind Marken der Sun Microsystems, Inc. in den USA und/oder anderen Ländern.
- Microsoft Windows, Windows NT und das Windows-Logo sind Marken der Microsoft Corporation in den USA und/oder anderen Ländern.
- PC Direct ist eine Marke der Ziff Communications Company in den USA und/oder anderen Ländern.
- SET und das SET-Logo sind Marken der SET Secure Electronic Transaction LLC.
- UNIX ist eine eingetragene Marke der Open Group in den USA und/oder anderen Ländern.
- Marken anderer Unternehmen/Hersteller werden anerkannt.

Erste Ausgabe (Oktober 2004)

Diese Veröffentlichung ist eine Übersetzung des Handbuchs
IBM Client Security Solutions Password Manager Version 1.4 User's Guide,
herausgegeben von International Business Machines Corporation, USA

Informationen, die nur für bestimmte Länder Gültigkeit haben und für Deutschland, Österreich und die Schweiz nicht zutreffen, wurden in dieser Veröffentlichung im Originaltext übernommen.

Möglicherweise sind nicht alle in dieser Übersetzung aufgeführten Produkte in Deutschland angekündigt und verfügbar; vor Entscheidungen empfiehlt sich der Kontakt mit der zuständigen IBM Geschäftsstelle.

Änderung des Textes bleibt vorbehalten.

Herausgegeben von:
SW TSC Germany
Kst. 2877
Oktober 2004

Inhaltsverzeichnis

Vorwort

Dieses Handbuch enthält Informationen zum Verwenden des Programms ″IBM Client Security Password Manager″ zum Verwalten und Abrufen sensibler Anmeldedaten.

Das Handbuch ist wie folgt aufgebaut:

Kapitel 1, „Einführung zu IBM Client Security Password Manager", enthält eine Übersicht zu Merkmalen und Funktionen von IBM Password Manager.

Kapitel 2, „Prozeduren", enthält Vorgehensweisen zum Definieren, Abrufen und Verwalten Ihrer Anmeldedaten mit IBM Client Security Password Manager.

Kapitel 3, „Einschränkungen", enthält nützliche Informationen zum Beheben bekannter Einschränkungen und Fehler, die möglicherweise beim Anwenden der in diesem Handbuch enthaltenen Anweisungen auftreten.

Zielgruppe

Dieses Handbuch ist für Benutzer von Client Security Software ab Version 4.0 konzipiert, die die Übersicht über all ihre Benutzer-IDs, Kennwörter und persönlichen Daten, die zum Registrieren und Anmelden auf Websites und in Anwendungen verwendet werden, behalten möchten.

IBM Client Security Password Manager Version 1.4 unterstützt die Betriebssysteme Windows 2000 und Windows XP.

Benutzung des Handbuchs

Dieses Handbuch liefert Informationen zur Verwendung von IBM Client Security Password Manager zur Vereinfachung des Anmeldevorgangs und der Kennwortverwaltung.

Zugang zu diesem Handbuch und zur gesamten Dokumentation zu Client Security erhalten Sie auf der IBM Website unter
http://www.pc.ibm.com/us/security/index.html.

Zusätzliche Informationen

Zusätzliche Informationen sowie Aktualisierungen für Sicherheitsprodukte können Sie, wenn verfügbar, von der IBM Website unter

http://www.pc.ibm.com/us/security/index.html

herunterladen.

Kapitel 1. Einführung zu IBM Client Security Password Manager

Mit IBM Client Security Password Manager können Ihre sensiblen und leicht zu vergessenden Anmeldedaten, wie z. B. Benutzer-IDs, Kennwörter und weitere persönliche Daten, mit IBM Client Security verwaltet werden. IBM Client Security Password Manager speichert alle Informationen über das IBM Embedded Security Subsystem (ESS, integriertes IBM Sicherheits-Subsystem), so dass die UVM-Policy für Benutzerauthentifizierung den Zugriff auf Ihre sicheren Anwendungen und Websites steuert.

Dies bedeutet, dass Sie sich nicht mehr eine große Menge einzelner Kennwörter merken müssen, die alle unterschiedlichen Regeln, Ablaufdaten usw. unterliegen. Sie benötigen nur noch einen Verschlüsselungstext, Ihren Fingerabdruck oder ein Proximity Badge oder eine beliebige Kombination dieser drei Möglichkeiten.

IBM Client Security Password Manager bietet folgende Funktionen:

- **Alle gespeicherten Informationen über das IBM Embedded Security Subsystem verschlüsseln**

  IBM Password Manager verschlüsselt automatisch alle Informationen über das IBM Embedded Security Subsystem. Dadurch wird sichergestellt, dass alle sensiblen Kennwortdaten durch Chiffrierschlüssel von IBM Client Security gesichert sind.

- **Benutzer-ID und Kennwörter schnell und einfach über eine einfache Eingabe- und Übertragungsschnittstelle übertragen**

  Verwenden Sie die Eingabe- und Übertragungsschnittstelle von IBM Password Manager, um Informationen direkt in das Anmeldedialogfenster des Webbrowsers oder der Anwendung zu stellen. Dadurch werden Tippfehler minimiert, und alle Informationen können sicher über das IBM Embedded Security Subsystem gespeichert werden.

- **Benutzer-IDs und Kennwörter automatisch verschlüsseln**

  IBM Password Manager automatisiert den Anmeldeprozess, da alle Anmeldedaten automatisch eingegeben werden, wenn Sie auf Websites zugreifen, die in IBM Password Manager eingetragen sind.

- **Sensible Anmeldedaten in einen geschützten Browser exportieren**

  Mit IBM Password Manager können Sie Ihre sensiblen Anmeldedaten exportieren und sie so sicher von einem Computer auf einen anderen übertragen. Wenn Sie Ihre Anmeldedaten aus IBM Password Manager exportieren, wird eine kennwortgeschützte Exportdatei erstellt, die Sie auf einem austauschbaren Datenträger speichern können. Mit dieser Datei können Sie auf Ihre Benutzerinformationen und Ihre Kennwörter zugreifen.

- **Kennwörter per Zufallsgenerator festlegen**

  Mit IBM Password Manager können für jede Website oder Anwendung Kennwörter per Zufallsgenerator festgelegt werden. So können Sie die Datensicherheit erhöhen, da für alle Anwendungen strengerer Kennwortschutz aktiviert ist. Per Zufallsgenerator festgelegte Kennwörter sind viel sicherer als benutzerdefinierte Kennwörter, da die Erfahrung zeigt, dass die meisten Benutzer leicht zu erinnernde persönliche Daten für Kennwörter verwenden, die oft relativ leicht zu knacken sind.

- **Einträge über die Schnittstelle von Password Manager bearbeiten**

  Mit IBM Password Manager können Sie alle Kontoeinträge und alle optionalen Kennwortfunktionen über eine einfach zu bedienende Schnittstelle bearbeiten. Dadurch wird die Verwaltung der Kennwörter und persönlichen Daten vereinfacht und beschleunigt.
- **Auf Password Manager von der Symbolleiste des Windows-Desktop oder über einen einfachen Direktaufruf über die Tastatur zugreifen**

  Das Symbol für IBM Password Manager ermöglicht sofortigen Zugriff auf das Programm, wenn Sie eine weitere Anwendung zu Password Manager hinzufügen möchten, wenn Sie zum Beispiel im Web surfen. Alle Funktionen von Password Manager können auch über einen einfachen Direktaufruf über die Tastatur aufgerufen werden.
- **Anmeldedaten archivieren**

  Über die Archivierungsfunktion ″Client Security″ ermöglicht IBM Password Manager das Wiederherstellen sensibler Anmeldedaten von einem Archiv von Client Security zum Schutz gegen einen Festplattenlaufwerk- oder Systemfehler. Weitere Informationen zum Archivieren von Daten finden Sie im Benutzerhandbuch zur Software ″Client Security″.

Kapitel 2. Prozeduren

In diesem Abschnitt werden schrittweise Vorgehensweisen zum Durchführen allgemeiner Funktionen von IBM Client Security Password Manager beschrieben.

Neue Einträge erstellen

Mit IBM Client Security Password Manager können Benutzer Informationen in Websites und Anwendungen eingeben, indem sie die Schnittstelle von Password Manager verwenden. Das Programm ″IBM Password Manager″ verschlüsselt und speichert die in die entsprechenden Felder eingegebenen Informationen über das IBM Embedded Security Subsystem (ESS, integriertes IBM Sicherheitssubsystem). Wenn die Informationen in Password Manager gespeichert sind, werden diese Felder automatisch mit diesen gesicherten Informationen ausgefüllt, wenn der Zugriff auf die Website oder Anwendung in Übereinstimmung mit der UVM-Policy für Benutzerauthentifizierung erteilt wird.

Gehen Sie wie folgt vor, um in IBM Client Security Password Manager Kennwortinformationen einzugeben:

1. Öffnen Sie die Anmeldeanzeige der Anwendung oder der Website.
2. Klicken Sie mit der rechten Maustaste auf das Symbol **Password Manager** in der Windows-Symbolleiste, und wählen Sie ″Erstellen″ aus.

   Anmerkung: Auf die Funktion ″Erstellen″ von Password Manager kann auch über den Direktaufruf über die Tastatur **Strg+Umschalttaste+H** zugegriffen werden.
3. Geben Sie die Informationen für ein Feld in das Fenster ″Erstellen″ von Password Manager ein.

   Anmerkung: Die Informationen in diesem Feld dürfen nicht länger als 260 Zeichen sein.
4. Wenn Sie nicht möchten, dass der eingegebene Text angezeigt wird, klicken Sie auf das Markierungsfeld **Eingegebenen Text wegen Vertraulichkeit teilweise überlagern**.

   Anmerkung: Dieses Markierungsfeld steuert, wie der Text in Password Manager angezeigt wird. Nachdem der Text an eine Website oder Anwendung übergeben wurde, werden die Einstellungen von der jeweiligen Anwendung gesteuert.
5. Verwenden Sie das Symbol für das Auswahlfeld ″Ziel″, um den Text aus dem Dienstprogramm ″Password Manager″ in das entsprechende Feld auf der Website oder in der Anwendung zu ziehen.

   Anmerkung: Über dieses Symbol kann der Text kopiert werden, ohne dass die Zwischenablage des Computers oder eine andere, nicht gesicherte, Position verwendet werden muss.
6. Wiederholen Sie, je nach Bedarf, die Schritte 3 bis 5 für jedes Feld.
7. Klicken Sie auf **Neuen Eintrag speichern**.
8. Geben Sie einen beschreibenden Namen für den neuen Eintrag ein.

9. Klicken Sie auf das Markierungsfeld ″**Eingabe**″ **zum automatischen Übergeben des Eintrags hinzufügen**″, wenn Sie möchten, dass Password Manager die Anmeldedaten nach dem Abrufen übergibt.

   Anmerkung: Auf einigen Websites wird nicht die Eingabetaste zum Übergeben von Anmeldedaten verwendet. Wenn die Anmeldung fehlschlägt, inaktivieren Sie diese Funktion.

10. Klicken Sie auf **Neuen Eintrag speichern**, um den Vorgang abzuschließen.

Einträge abrufen

Es ist einfach, Kennwörter über IBM Client Security Password Manager abzurufen.

Gehen Sie wie folgt vor, um in IBM Client Security Password Manager gespeicherte Daten abzurufen.

1. Öffnen Sie die Anmeldeanzeige der Anwendung oder Website für die Daten, die Sie abrufen möchten.
2. Klicken Sie doppelt auf das Symbol **Password Manager** in der Windows-Symbolleiste. Password Manager füllt die Felder der Anmeldeanzeige mit den gespeicherten Daten aus.

   Anmerkung: Die Funktion ″Abrufen″ von Password Manager kann auch über den Direktaufruf über die Tastatur **Strg+Umschalttaste+G** aufgerufen werden.

3. Geben Sie den UVM-Verschlüsselungstext ein, oder erfüllen Sie die durch die UVM-Policy für Benutzerauthentifizierung angegebenen Zugriffsbedingungen.
4. Wenn das Markierungsfeld ″**Eingabe**″ **zum automatischen Übergeben des Eintrags hinzufügen** nicht ausgewählt ist, klicken Sie auf die Schaltfläche ″Übergeben″ in der Anwendung oder auf der Website.

   Wenn kein Eintrag abgerufen wird, werden Sie gefragt, ob Sie einen neuen Eintrag erstellen möchten. Klicken Sie auf **Ja**, um das Fenster ″Password Manager - Neuen Eintrag erstellen″ zu öffnen.

Einträge verwalten

IBM Client Security Password Manager ermöglicht das Arbeiten mit in Password Manager gespeicherten Informationen. Das Fenster ″Verwalten″ von Password Manager ermöglicht das Ändern der Benutzer-ID, des Kennworts und weiterer in Password Manager eingegebener Daten, die in die Felder einer Website oder Anwendung eingegeben werden.

Gehen Sie wie folgt vor, um in IBM Client Security Password Manager gespeicherte Daten zu ändern:

1. Klicken Sie mit der rechten Maustaste auf das Symbol **Password Manager** in der Windows-Systemleiste, und klicken Sie auf **Verwalten**.

   Anmerkung: Die Funktion ″Verwalten″ von Password Manager kann auch über den Direktaufruf über die Tastatur **Strg+Umschalttaste+B** aufgerufen werden.

2. Geben Sie den UVM-Verschlüsselungstext ein, oder erfüllen Sie die durch die UVM-Policy für Benutzerauthentifizierung angegebenen Zugriffsbedingungen.
3. Bearbeiten Sie Ihre Daten. Dabei können Sie aus den folgenden Optionen auswählen:

- Eingabedaten

  Gehen Sie wie folgt vor, um Eingabedaten zu bearbeiten:

  a. Klicken Sie mit der rechten Maustaste auf den Eintrag, den Sie bearbeiten möchten.
  b. Wählen Sie eine der folgenden Aktionen aus:
     – ″Eingabe″ hinzufügen

       Wählen Sie ″″Eingabe″ hinzufügen″ aus, damit die Daten automatisch in die Website oder die Anwendung eingegeben werden. Ein Markierungssymbol wird neben ″″Eingabe″ hinzufügen″ angezeigt, wenn diese Funktion aktiviert ist.
     – Löschen

       Wählen Sie ″Löschen″ aus, um einen Eintrag vollständig zu löschen.
  c. Klicken Sie auf **Änderungen speichern**.

- Eingabefelddaten

  Gehen Sie wie folgt vor, um Eingabefelddaten zu bearbeiten.

  a. Klicken Sie mit der rechten Maustaste auf das Feld, das Sie bearbeiten möchten.
  b. Wählen Sie eine der folgenden Aktionen aus:
     – Eingabefeld ändern

       Wählen Sie ″Eingabefeld ändern″ aus, um die für dieses Feld gespeicherten Daten zu ändern. Sie können das Eingabefeld auf eine der folgenden Weisen ändern:
       - Durch Erstellen eines willkürlich ausgewählten Eintrags
         Wenn Sie einen willkürlich ausgewählten Eintrag erstellen möchten, wählen Sie ″Willkürlich auswählen″ aus. Password Manager erstellt willkürlich ausgewählte Einträge mit 7, 14 oder 127 Zeichen.
       - Durch manuelles Bearbeiten eines Eingabefelds
         Wählen Sie zum manuellen Bearbeiten eines Eingabefelds ″Bearbeiten″ aus, und nehmen Sie die entsprechenden Änderungen am Feld vor.
     – Löschen

       Wählen Sie ″Löschen″ aus, um das Eintragsfeld vollständig zu löschen.

       Anmerkung: Durch Ändern eines Felds in Password Manager werden nur die Anmeldedaten innerhalb von Password Manager aktualisiert. Wenn Sie die Sicherheit der Kennwörter erhöhen möchten, indem Sie die Funktion ″Willkürlich auswählen″ von Password Manager verwenden, müssen Sie die Anwendung oder Website mit dem neuen, per Zufallsgenerator festgelegten Kennwort, das durch diese Funktion erstellt wurde, synchronisieren. Verwenden Sie das Eingabe- und Übertragungstool, um das neue, per Zufallsgenerator festgelegte Kennwort zum Formular zum Ändern des Kennworts in der Anwendung oder auf der Website zu übertragen. Stellen Sie sicher, dass das Kennwort für die Anwendung oder Website gültig ist, und verwenden Sie dann die Option ″Änderungen speichern″ im Fenster ″Verwalten″ von Password Manager. Der Eintrag mit dem neuen Kennwort muss nicht erneut erstellt werden, da alle erforderlichen Informationen gespeichert wurden.
  c. Klicken Sie auf **Änderungen speichern**.

4. Klicken Sie auf **Änderungen speichern**.

Anmeldedaten exportieren

Mit IBM Password Manager können Sie Ihre sensiblen Anmeldedaten exportieren und sie so sicher von einem Computer auf einen anderen übertragen. Wenn Sie Ihre Anmeldedaten aus IBM Password Manager exportieren, wird eine kennwortgeschützte Exportdatei erstellt, die Sie auf einem austauschbaren Datenträger speichern können. Mit dieser Datei können Sie auf Ihre Benutzerinformationen und Ihre Kennwörter zugreifen.

Gehen Sie wie folgt vor, um in IBM Client Security Password Manager gespeicherte Anmeldedaten zu exportieren:

1. Klicken Sie mit der rechten Maustaste auf das Symbol **Password Manager** in der Windows-Systemleiste, und klicken Sie auf **Verwalten**.

   Anmerkung: Die Funktion ″Verwalten″ von Password Manager kann auch über den Direktaufruf über die Tastatur **Strg+Umschalttaste+B** aufgerufen werden.
2. Geben Sie den UVM-Verschlüsselungstext ein, oder erfüllen Sie die durch die UVM-Policy für Benutzerauthentifizierung angegebenen Zugriffsbedingungen.
3. Klicken Sie auf **Exportieren**. Das Fenster ″Speichern als″ wird mit dem Standardpfad und dem Dateinamen `PwMgrExportReader` angezeigt.
4. Wählen Sie die Position aus, an der Sie die Exportdatei speichern möchten.
5. Klicken Sie auf **Speichern**, um die angegebene Position und den Dateinamen zu akzeptieren. Eine Anzeige erscheint, in der Sie aufgefordert werden, einen Verschlüsselungstext für die Exportdatei anzugeben.
6. Geben Sie einen Verschlüsselungstext für die Exportdatei an, und klicken Sie auf **OK**. Dieser Verschlüsselungstext ist erforderlich, um auf die exportierten Daten zuzugreifen. Es erscheint eine Nachricht, die anzeigt, dass der Exportvorgang erfolgreich beendet wurde.
7. Klicken Sie auf **OK**.
8. Schließen Sie IBM Password Manager.
9. Rufen Sie die erstellte Exportdatei von der angegebenen Position ab, und kopieren Sie sie auf einen austauschbaren Datenträger.

Bevor Sie die Datei auf einem anderen Computer öffnen können, werden Sie aufgefordert, den Verschlüsselungstext für die Exportdatei einzugeben, den Sie wie oben beschrieben angegeben haben. IBM Password Manager zeigt Ihre sensiblen Daten in einer gesicherten Leseeinheit an. Diese Daten können nicht ausgedruckt oder auf der Festplatte des Computers gespeichert werden. Klicken Sie auf **OK**, um die Export-Leserdatei zu schließen.

Kapitel 3. Einschränkungen

Dieser Abschnitt enthält Informationen zu bekannten Einschränkungen in Zusammenhang mit IBM Client Security Password Manager.

IBM Client Security Password Manager unterstützt Netscape Navigator nicht. Sie müssen Microsoft Internet Explorer verwenden, um die Funktionen des Programms ″IBM Password Manager″ verwenden zu können. Die Software ″Password Manager″ unterstützt Netscape Navigator nicht.

Anhang. Bemerkungen und Marken

Dieser Anhang enthält rechtliche Hinweise zu IBM Produkten und Informationen zu Marken.

Bemerkungen

Die vorliegenden Informationen wurden für Produkte und Services entwickelt, die auf dem deutschen Markt angeboten werden.

Möglicherweise bietet IBM die in diesem Dokument beschriebenen Produkte, Services oder Funktionen in anderen Ländern nicht an. Informationen über die gegenwärtig im jeweiligen Land verfügbaren Produkte und Services sind beim IBM Ansprechpartner erhältlich. Hinweise auf IBM Lizenzprogramme oder andere IBM Produkte bedeuten nicht, dass nur Programme, Produkte oder Dienstleistungen von IBM verwendet werden können. Anstelle der Produkte, Programme oder Dienstleistungen können auch andere, ihnen äquivalente Produkte, Programme oder Dienstleistungen verwendet werden, solange diese keine gewerblichen oder andere Schutzrechte von IBM verletzen. Die Verantwortung für den Betrieb von Fremdprodukten, Fremdprogrammen und Fremddienstleistungen liegt beim Kunden.

Für in diesen Dokument beschriebene Erzeugnisse und Verfahren kann es IBM Patente oder IBM Patentanmeldungen geben. Mit der Auslieferung dieses Handbuchs ist keine Lizenzierung dieser Patente verbunden. Lizenzanfragen sind schriftlich an folgende Adresse zu richten (Anfragen an diese Adresse müssen auf Englisch formuliert werden):

IBM Europe
Director of Licensing
92066 Paris
La Defense Cedex
France

Trotz sorgfältiger Bearbeitung können technische Ungenauigkeiten oder Druckfehler in dieser Veröffentlichung nicht ausgeschlossen werden. Die Angaben in diesem Handbuch werden in regelmäßigen Zeitabständen aktualisiert. Die Änderungen werden in Überarbeitungen oder in Technical News Letters (TNLs) bekannt gegeben. IBM kann jederzeit ohne Vorankündigung Verbesserungen und/oder Änderungen an den in dieser Veröffentlichung beschriebenen Produkten und/oder Programmen vornehmen.

Lizenznehmer des Programms, die Informationen zu diesem Produkt wünschen mit der Zielsetzung: (i) den Austausch von Informationen zwischen unabhängigen, erstellten Programmen und anderen Programmen (einschließlich des vorliegenden Programms) sowie (ii) die gemeinsame Nutzung der ausgetauschten Informationen zu ermöglichen, wenden sich an folgende Adresse: IBM Corporation, Department 80D, P.O. Box 12195, 3039 Cornwallis, Research Triangle Park, NC 27709, U.S.A. Die Bereitstellung dieser Informationen kann unter Umständen von bestimmten Bedingungen - in einigen Fällen auch von der Zahlung einer Gebühr - abhängig sein.

Die Lieferung des in diesem Dokument aufgeführten Lizenzprogramms sowie des zugehörigen Lizenzmaterials erfolgt im Rahmen der Allgemeinen Geschäftsbedingungen der IBM, der Internationalen Nutzungsbedingungen der IBM für Programmpakete oder einer äquivalenten Vereinbarung.

Marken

IBM und SecureWay sind in gewissen Ländern Marken der IBM Corporation.

Tivoli ist in gewissen Ländern eine Marke von Tivoli Systems Inc.

Microsoft, Windows und Windows NT sind in gewissen Ländern Marken der Microsoft Corporation.

Andere Namen von Unternehmen, Produkten und Dienstleistungen können Marken oder Dienstleistungsmarken anderer Unternehmen sein.