IBM® Client Security
Solutions

Password Manager Version 1.4 User's Guide

IBM® Client Security
Solutions

Password Manager Version 1.4 User's Guide

First Edition (October 2004)

Contents

Preface

This guide contains information on using the IBM Client Security Password Manager program to manage and recall your sensitive login information.

This guide is organized as follows:

Chapter 1, “Introduction to the IBM Client Security Password Manager” contains an overview of IBM Password Manager features and functions.

Chapter 2, “Procedures” contains procedures for using the IBM Client Security Password Manager program to set up, recall, and manage your login information.

Chapter 3, “Limitations” contains helpful information for overcoming known limitations and problems you might experience while using the instructions provided in this guide.

Who should read this guide

This guide is intended for users of Client Security Software Version 4.0 or higher who want help keeping track of all their user IDs, passwords, and personal information that is used to register and login to Web sites or applications.

IBM Client Security Password Manager Version 1.4 supports the Windows 2000 and Windows XP operating systems.

How to use this guide

This guide is designed to help you use the IBM Client Security Password Manager to simplify your login process and password management.

This guide and all other documentation for Client Security can be accessed from the http://www.pc.ibm.com/us/security/index.html IBM web site.

Additional information

You can obtain additional information and security product updates, when available, from the http://www.pc.ibm.com/us/security/index.html IBM Web site.

Chapter 1. Introduction to the IBM Client Security Password Manager

The IBM Client Security Password Manager enables you to manage your sensitive and easy-to-forget login information, such as user IDs, passwords, and other personal information, with IBM Client Security. The IBM Client Security Password Manager stores all information through the IBM embedded Security Subsystem so that your UVM user authentication policy controls access to your secure applications and Web sites.

This means that rather than having to remember and provide a plethora of individual passwords-- all subject to different rules and expiration dates-- you only have to remember one passphrase, provide your fingerprint, provide your proximity badge, or any combination of identification elements.

The IBM Client Security Password Manager enables you to perform the following functions:

- **Encrypt all stored information through the IBM embedded Security Subsystem**

  The IBM Password Manager automatically encrypts all information through the IBM embedded Security Subsystem. This ensures that all your sensitive password information is secured by the IBM Client Security encryption keys.
- **Transfer user IDs and passwords quickly and easily utilizing a simple type-and-transfer interface**

  Use the IBM Password Manager type-and-transfer interface to place information directly into the logon dialog of your web browser or application. This helps minimize typing errors and enables you to save all of your information securely through the IBM embedded Security Subsystem.
- **Autokey user IDs and passwords**

  The IBM Password Manager automates your login process, entering your login information automatically when you access Web sites entered into the IBM Password Manager.
- **Export your sensitive login information to a secure browser**

  The IBM Password Manager enables you to export your sensitive login information so that you can securely carry it from computer to computer. When you export your login information from IBM Password Manager, a password-protected export file is created that can be stored on removable media. You can use this file to access your user information and passwords.
- **Generate random passwords**

  The IBM Password Manager enables you to generate random passwords for each Web site or application. This enables you to increase the security of your data because each application will have much more rigorous password protection enabled. Random passwords are far more secure than user-defined passwords because experience indicates that most users use easy-to-remember personal information for passwords that are often relatively easy to crack.
- **Edit entries using the Password Manager interface**

  The IBM Password Manager enables you to edit all of your account entries and set up all optional password features in one easy-to-use interface. This makes managing your passwords and personal information quick and easy.

- **Access Password Manager from the icon tray on your Windows desktop or with a simple keyboard shortcut**

  The IBM Password Manager icon enables you to have instant access whenever you need to add another application to Password Manager, such as when you are surfing the Web. Each Password Manager function can also be easily accessed by a simple keyboard shortcut.
- **Archive your login information**

  Using the Client Security archiving function, the IBM Password Manager enables you to restore your sensitive login information from a Client Security archive to protect against a hard drive or system failure. See the *Client Security Software User's Guide* for more information on how to archive information.

Chapter 2. Procedures

This section provides step-by-step procedures on how to perform common IBM Client Security Password Manager functions.

Creating new entries

The IBM Client Security Password Manager enables users to enter information into Web sites and applications using the Password Manager interface. The IBM Password Manager program encrypts and saves the information that is entered into the appropriate fields through the IBM embedded Security subsystem. Once the information is saved in Password Manager, these fields are automatically populated with this secure information whenever access to the Web site or application is granted according to the UVM user authentication policy.

To enter password information into the IBM Client Security Password Manager, complete the following procedure:

1. Open the application or Web site logon screen.
2. Right-click the **Password Manager** icon in the Windows icon tray and select Create.

   Note: The Password Manager Create function can also be accessed with the keyboard shortcut **Ctrl+Shift+H**.
3. Enter the information for a field in the Password Manager- Create New Entry window.

   Note: The information in this field must be less than 260 characters in length.
4. If you do not want the entered text to be displayed, click the **Obscure typed text for privacy** check box.

   Note: This check box only controls how the text is displayed within Password Manager. After the text is dropped into a Web site or application, its properties will be controlled by that application.
5. Use the Select Field ″target″ icon to drag the text from the Password Manager utility into the appropriate field on the Web site or application.

   Note: This icon enables the text to be copied without using your computer clipboard or other non-secure location.
6. Repeat step 3 through step 5 for each field, as necessary.
7. Click **Save New Entry**.
8. Type a descriptive name for the new entry.
9. Click the **Add ″Enter″ to automatically submit entry** check box if you want Password Manager to submit the login information after recalling.

   Note: Some Web sites do not use the Enter key to submit login information. If login is failing, disable this convenience feature.
10. Click **Save New Entry** to complete the procedure.

Recalling entries

Recalling passwords using the IBM Client Security Password Manager is simple and easy.

To recall information stored in the IBM Client Security Password Manager, complete the following procedure:

1. Open the application or Web site logon screen for the information that you want to recall.
2. Double-click the **Password Manager** icon in the Windows icon tray. Password Manager will populate the fields on the logon screen with the stored information.

   Note: The Password Manager Recall function can also be accessed with the keyboard shortcut **Ctrl+Shift+G**.
3. Enter your UVM passphrase, or complete the access requirements specified by the UVM user authentication policy.
4. If the **Add "Enter" to automatically submit entry** check box is not checked, click the Submit button on the application or the Web site.

   If no entry is recalled, a prompt will ask you if you would like to create a new entry. Click **Yes** to launch the Password Manager- Create New Entry window.

Managing entries

The IBM Client Security Password Manager enables users to work with information stored in the Password Manager. The Password Manager- Manage window enables you to change your user ID, password, and other information entered into Password Manager that populate the fields on a Web site or application.

To change information stored in the IBM Client Security Password Manager, complete the following procedure:

1. Right-click the **Password Manager** icon in the Windows icon tray and click **Manage**.

   Note: The Password Manager Manage function can also be accessed with the keyboard shortcut **Ctrl+Shift+B**.
2. Enter your UVM passphrase, or complete the access requirements specified by the UVM user authentication policy.
3. Edit your information. Select from the following options:
   - Entry information

     To edit entry information, complete the following procedure:

     a. Right-click the entry you want to edit.

     b. Select from the following actions:

        – Add "Enter"

          Select Add "Enter" to automatically have your entry information entered into the Web site or application. A check icon will appear next to Add "Enter" when this function is activated.

        – Delete

          Select Delete to delete the entry entirely.

     c. Click **Save Changes**.

- Entry field information

  To edit entry field information, complete the following procedure:

  a. Right-click the field you want to edit.
  b. Select from the following actions:
     – Change entry field

       Select Change Entry Field to change the information stored for this field. You can change an entry field in one of the following ways:

       - By creating a randomized entry

         To create a randomized entry, select Randomize. Password Manager will create randomized entries that are 7, 14, or 127 characters in length.

       - By manually editing an entry field

         To manually edit an entry field, select Edit and make the appropriate changes to the field.

     – Delete

       Select Delete to delete the entry field entirely.

     Note: Changing a field in Password Manager will only update the login information within Password Manager. If you want to increase the security of your passwords by using the Password Manager randomize feature, you must synchronize the application or Web site with the new random password generated by this feature. Use the convenient Password Manager Transfer Field Tool to transfer the new randomized password into application or Web site ″Change Password″ form. Verify that the new password is valid for the application or Web site and then use the Save Changes in the Password Manger - Manage Window. There is no need to re-create the entry with the new password since all the necessary information has been retained.

  c. Click **Save Changes**.

4. Click **Save Changes**.

Exporting login information

The IBM Password Manager enables you to export your sensitive login information so that you can securely carry it from computer to computer. When you export your login information from the IBM Password Manager, a password-protected export file is created that can be stored on removable media. You can use this file to access your user information and passwords.

To export the login information that is stored in the IBM Client Security Password Manager, complete the following procedure:

1. Right-click the **Password Manager** icon in the Windows icon tray and click **Manage**.

   Note: The Password Manager Manage function can also be accessed with the keyboard shortcut **Ctrl+Shift+B**.

2. Enter your UVM passphrase, or complete the access requirements specified by the UVM user authentication policy.
3. Click **Export**. The Save As window is displayed with the default path and `PwMgrExportReader` file name.
4. Select the location where you want to save your export file.

5. Click **Save** to accept the specified location and file name. A screen is displayed that prompts you to establish a passphrase for your export file.
6. Set a passphrase for your export file and click **OK**. This passphrase will be required to access the exported data. A message is displayed indicating that the export completed successfully.
7. Click **OK**.
8. Close the IBM Password Manager.
9. Retrieve the created export file from the location that you designated and copy it to a removable medium.

Before you can open this file on another computer, you will be prompted for the export passphrase that you established in the above procedure. IBM Password Manager displays your sensitive information in a secure reader. This information cannot be printed or saved to the computer hard drive. Click **OK** to close the export reader file.

Chapter 3. Limitations

This section contains information about known limitations related to the IBM Client Security Password Manager.

The IBM Client Security Password Manager does not support Netscape Navigator: You must use Microsoft Internet Explorer to utilize the functionality of the IBM Password Manager program. The Password Manager software does not support Netscape Navigator.

Appendix. Notices and Trademarks

This appendix gives legal notice for IBM products as well as trademark information.

Notices

This information was developed for products and services offered in the U.S.A.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not give you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785
U.S.A.

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law:
INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Licensees of this program who wish to have information about it for the purpose of enabling: (1) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact IBM Corporation, Department 80D, P.O. Box 12195, 3039 Cornwallis, Research Triangle Park, NC 27709, U.S.A. Such information may be available, subject to appropriate terms and conditions, including in some cases, payment of a fee.

The licensed program described in this document and all licensed material available for it are provided by IBM under terms of the IBM Customer Agreement, IBM International Program License Agreement or any equivalent agreement between us.

Trademarks

IBM and SecureWay are trademarks of the IBM Corporation in the United States, other countries, or both.

Tivoli is a trademark of Tivoli Systems Inc. in the United States, other countries, or both.

Microsoft, Windows, and Windows NT are trademarks of Microsoft Corporation in the United States, other countries, or both.

Other company, product, and service names may be trademarks or service marks of others.

Printed in USA