IBM® Client Security
Solutions

IBM

Password Manager User's Guide

IBM® Client Security
Solutions

Password Manager User's Guide

First Edition (September 2002)

Contents

iii

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 1.0 supports the Windows NT,
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 downloaded from
the http://www.pc.ibm.com/ww/security/secdownload.html IBM web site.

Additional information

You can obtain additional information and security product updates, when available,
from the http://www.pc.ibm.com/ww/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 all of 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 Security Chip 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, expiration dates, etc.-- you only have to remember one passphrase, or provide your fingerprint.

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

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

  The IBM Password Manager automatically encrypts all information through the IBM embedded Security Chip. 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 Chip.

- **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.

- **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.

  Note: The IBM Password Manager does not support icon tray functionality on computers running the Windows NT operating system. If you are using a Windows NT system, use the keyboard shortcuts.

- **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 secure 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 Chip. 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.

   Notes:
   a. The Password Manager Create function can also be accessed with the keyboard shortcuts **Ctrl+Shift+H** or **Winlogo+H**.
   b. The IBM Password Manager does not support icon tray functionality on computers running the Windows NT operating system. If you are using a Windows NT system, use the keyboard shortcuts.

   Note:
3. Enter the information for a field in the Password Manager- Create New Entry window.
4. If you do not want the entered text to be displayed, click the **Obscure typed text for privacy** check box.

   Note: This checkbooks 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. Click the **Add** ″**Enter**″ **to automatically submit entry** checkbooks 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.
9. Click **Save New Entry** to complete the procedure.

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.

   Notes:

   a. The Password Manager Manage function can also be accessed with the keyboard shortcuts **Ctrl+Shift+B** or **Winlogo+B**.

   b. The IBM Password Manager does not support icon tray functionality on computers running the Windows NT operating system. If you are using a Windows NT system, use the keyboard shortcuts.

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 entirely.

> **Note:** After a field has been changed in Password Manager, it must then be transferred to the Web site or application using the IBM Password Manager type-and-transfer crosshair interface. This tool helps minimize typing errors and enables you to save all of your information securely through the IBM embedded Security Chip.

    c. Click **Save Changes**.

4. Click **Save Changes**.

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.

   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.

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.

   Notes:

   a. The Password Manager Recall function can also be accessed with the keyboard shortcuts **Ctrl+Shift+G** or **Winlogo+G**.

   b. The IBM Password Manager does not support icon tray functionality on computers running the Windows NT operating system. If you are using a Windows NT system, use the keyboard shortcuts.

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.

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.

The IBM Client Security Password Manager does not support icon tray functionality on computers running the Windows NT operating system: The IBM Password Manager does not support icon tray functionality on computers running the Windows NT operating system. If you are using a Windows NT system, use the keyboard shortcuts.

IBM ®

Printed in U.S.A.