

Soluciones IBM[®] Client Security



Guía del usuario de Password Manager

Versión 1.4

Soluciones IBM[®] Client Security



Guía del usuario de Password Manager

Versión 1.4

Primera edición (octubre de 2004)

Esta publicación es la traducción del original inglés *IBM Client Security Solutions: Password Manager Version 1.4 User's Guide*.

© Copyright International Business Machines Corporation 2004. Reservados todos los derechos.

Contenido

Prefacio	v	Recuperación de entrada	4
A quién va dirigida esta guía	v	Gestión de entradas	4
Utilización de esta guía	v	Exportación de información de inicio de sesión	5
Información adicional	v		
Capítulo 1. Introducción a IBM Client Security Password Manager	1	Capítulo 3. Limitaciones	7
Capítulo 2. Procedimientos	3	Apéndice. Avisos y marcas registradas	9
Creación de nuevas entradas	3	Avisos	9
		Marcas registradas	10

Prefacio

Esta guía contiene información sobre la utilización del programa IBM Client Security Password Manager para gestionar y recuperar su información de inicio de sesión confidencial.

Esta guía está organizada de la forma siguiente:

El Capítulo 1, "Introducción a IBM Client Security Password Manager" contiene una visión general de las características y funciones de IBM Password Manager.

El Capítulo 2, "Procedimientos" contiene los procedimientos para utilizar el programa IBM Client Security Password Manager para definir, recuperar y gestionar su información de inicio de sesión.

El Capítulo 3, "Limitaciones" contiene información de ayuda para superar las limitaciones y problemas conocidos que podría encontrar mientras utiliza las instrucciones proporcionadas en esta guía.

A quién va dirigida esta guía

Esta guía va dirigida a los usuarios del software Client Security versión 4.0 o superior que deseen ayuda para mantener un seguimiento de todos sus ID de usuario, contraseñas e información personal utilizados para registrarse e iniciar sesiones en sitios Web y aplicaciones.

IBM Client Security Password Manager Versión 1.4 soporta los sistemas operativos Windows 2000 y Windows XP.

Utilización de esta guía

Esta guía está diseñada para ayudarle a utilizar IBM Client Security Password Manager con el fin de simplificar la gestión de los procesos de inicio de sesión y contraseñas.

Puede acceder a esta guía y a la demás documentación de Client Security desde el sitio Web de IBM en <http://www.pc.ibm.com/us/security/index.html>.

Información adicional

Puede obtener información adicional y actualizaciones de productos de seguridad, cuando estén disponibles, desde el sitio Web de IBM en <http://www.pc.ibm.com/us/security/index.html>.

Capítulo 1. Introducción a IBM Client Security Password Manager

IBM Client Security Password Manager le permite gestionar la información de inicio de sesión confidencial y fácil de olvidar, como los ID de usuario, contraseñas y otra información personal, con IBM Client Security. IBM Client Security Password Manager almacena toda la información mediante IBM Embedded Security Subsystem de tal forma que su política de autenticación de usuario UVM controla el acceso a sus aplicaciones seguras y sitios Web.

Esto significa que en lugar de tener que recordar y proporcionar una plétora de contraseñas individuales, todas sometidas a normas diferentes y fechas de caducidad, sólo tendrá que recordar una frase de paso, proporcionar su huella dactilar, su tarjeta de identificación por contacto o cualquier combinación de elementos de identificación.

IBM Client Security Password Manager le permite realizar las siguientes funciones:

- **Cifrar toda la información almacenada mediante IBM Embedded Security Subsystem**

IBM Password Manager cifra automáticamente toda la información mediante IBM Embedded Security Subsystem. Esto garantiza que toda la información de contraseñas confidenciales está protegida por las claves de cifrado de IBM Client Security.

- **Transferir los ID de usuario y contraseñas rápida y fácilmente utilizando una interfaz sencilla de escritura y transferencia**

Utilice la interfaz de escritura y transferencia de IBM Password Manager para situar información directamente en el diálogo de inicio de sesión del navegador Web o aplicación. Esto ayuda a minimizar los errores de escritura y le permite guardar toda su información de forma segura mediante IBM Embedded Security Subsystem.

- **ID de usuario y contraseñas mediante teclas automáticas**

IBM Password Manager automatiza los procesos de inicio de sesión, introduciendo automáticamente su información de inicio de sesión cuando accede a sitios Web especificados en IBM Password Manager.

- **Exportar la información de inicio de sesión confidencial a un navegador seguro**

IBM Password Manager le permite exportar su información de inicio de sesión confidencial de tal forma que pueda transportarla de forma segura de un sistema a otro. Cuando exporta la información de inicio de sesión desde IBM Password Manager, se crea un archivo de exportación protegido mediante contraseña que se puede almacenar en un soporte de almacenamiento extraíble. Puede utilizar este archivo para acceder a su información de usuario y contraseñas.

- **Generar contraseñas aleatorias**

IBM Password Manager le permite generar contraseñas aleatorias para cada sitio Web o aplicación. Esto le permite aumentar la seguridad de sus datos puesto que cada aplicación tendrá habilitada una protección mediante contraseña mucho más rigurosa. Las contraseñas aleatorias son mucho más seguras que las contraseñas definidas por el usuario porque la experiencia indica que la mayoría

de los usuarios utilizan información personal fácil de recordar para las contraseñas que suele ser relativamente fácil de descifrar.

- **Editar entradas utilizando la interfaz de Password Manager**

IBM Password Manager le permite editar todas las entradas de sus cuentas y definir características opcionales para las contraseñas con una interfaz fácil de utilizar. Esto agiliza y facilita la gestión de sus contraseñas e información personal.

- **Acceder a Password Manager desde la bandeja de iconos del escritorio de Windows o con un simple método abreviado de teclado**

El icono de IBM Password Manager le permite disponer de acceso instantáneo cada vez que necesita añadir otra aplicación a Password Manager, como cuando navega por la Web. También puede acceder fácilmente a cada función de Password Manager mediante un simple método abreviado de teclado.

- **Archivar su información de inicio de sesión**

Utilizando la función de archivo de Client Security, IBM Password Manager le permite restaurar su información de inicio de sesión confidencial desde un archivo de Client Security para protegerle frente a cualquier anomalía del disco duro o del sistema. Consulte la *Guía del usuario de Client Security Software* para obtener más información sobre cómo archivar información.

Capítulo 2. Procedimientos

Este apartado proporciona procedimientos paso a paso sobre cómo realizar las funciones comunes en IBM Client Security Password Manager.

Creación de nuevas entradas

IBM Client Security Password Manager permite a los usuarios introducir información en sitios Web y aplicaciones utilizando la interfaz de Password Manager. El programa IBM Password Manager cifra y guarda la información que se introduce en los campos apropiados mediante IBM Embedded Security Subsystem. Una vez guardada la información en Password Manager, estos campos se rellenan automáticamente con esta información segura cada vez que se otorga acceso al sitio Web o aplicación según la política de autenticación de usuario UVM.

Para introducir la información de la contraseña en IBM Client Security Password Manager, realice el procedimiento siguiente:

1. Abra la aplicación o la pantalla de inicio de sesión del sitio Web.
2. Pulse el botón derecho del ratón en el icono de **Password Manager** en la bandeja de iconos de Windows y seleccione Crear.

Nota: También puede acceder a la función Crear de Password Manager con el método abreviado de teclado **Control+Mayús+H**.

3. Introduzca la información de un campo en la ventana Password Manager - Crear nueva entrada.

Nota: La información de este campo deberá tener una longitud inferior a 260 caracteres.

4. Si no desea que se visualice el texto introducido, pulse el recuadro de selección **Ocultar texto escrito por privacidad**.

Nota: Este recuadro de selección sólo controla cómo se visualiza el texto dentro de Password Manager. Cuando el texto se deposita en un sitio Web o aplicación, es la aplicación la que controlará sus propiedades.

5. Utilice el icono de "destino" del Campo de selección para arrastrar el texto desde el programa de utilidad Password Manager al campo apropiado del sitio Web o aplicación.

Nota: Este icono permite que se copie el texto sin utilizar el portapapeles del sistema ni otra ubicación no segura.

6. Repita los pasos 3 al 5 para cada campo, según sea necesario.
7. Pulse **Guardar nueva entrada**.
8. Escriba un nombre descriptivo para la nueva entrada.
9. Pulse el recuadro de selección **Añadir "Intro" para someter automáticamente la entrada** si desea que Password Manager someta la información de inicio de sesión cuando se recupera.

Nota: Algunos sitios Web no utilizan la tecla Intro para someter la información de inicio de sesión. Si el inicio de sesión no funciona, inhabilite esta característica rápida.

10. Pulse **Guardar nueva entrada** para completar el procedimiento.

Recuperación de entrada

Recuperar contraseñas utilizando IBM Client Security Password Manager es sencillo.

Para recuperar información almacenada en IBM Client Security Password Manager, realice el procedimiento siguiente:

1. Abra la aplicación o la pantalla de inicio de sesión del sitio Web para la información que desea recuperar.
2. Efectúe una doble pulsación en el icono de **Password Manager** en la bandeja de iconos de Windows. Password Manager rellenará los campos de la pantalla de inicio de sesión con la información almacenada.

Nota: También puede acceder a la función Recuperar de Password Manager con el método abreviado de teclado **Control+Mayús+G**.

3. Introduzca su frase de paso UVM o complete los requisitos de acceso especificados por la política de autenticación de usuario UVM.
4. Si no está seleccionado el recuadro de selección **Añadir "Intro" para someter automáticamente la entrada**, pulse el botón Someter de la aplicación o sitio Web.

Si no se recupera ninguna entrada, se le preguntará si desea crear una nueva entrada. Pulse **Sí** para abrir la ventana Password Manager - Crear nueva entrada.

Gestión de entradas

IBM Client Security Password Manager permite trabajar a los usuarios con información almacenada en Password Manager. La ventana Password Manager - Gestionar le permite cambiar su ID de usuario, contraseña y otra información introducida en Password Manager que rellena los campos en un sitio Web o aplicación.

Para cambiar la información almacenada en IBM Client Security Password Manager, realice el procedimiento siguiente:

1. Pulse el botón derecho del ratón en el icono de **Password Manager** en la bandeja de iconos de Windows y pulse **Gestionar**.

Nota: También puede acceder a la función Gestionar de Password Manager con el método abreviado de teclado **Control+Mayús+B**.

2. Introduzca su frase de paso UVM o complete los requisitos de acceso especificados por la política de autenticación de usuario UVM.
3. Edite su información. Seleccione entre las opciones siguientes:

- Información de la entrada

Para editar la información de la entrada, realice el procedimiento siguiente:

- a. Pulse el botón derecho del ratón en la entrada que desea editar.
- b. Seleccione entre las acciones siguientes:
 - Añadir "Intro"

Seleccione Añadir "Intro" para que la información de la entrada se introduzca automáticamente en el sitio Web o aplicación. Cuando esta función está activada aparece un icono de marca junto a Añadir "Intro".

- Suprimir

Seleccione Suprimir para suprimir completamente la entrada.

c. Pulse **Guardar cambios**

- Información del campo de entrada

Para editar la información del campo de entrada, realice el procedimiento siguiente:

- a. Pulse el botón derecho del ratón en el campo que desea editar.

- b. Seleccione entre las acciones siguientes:

- Cambiar campo de entrada

Seleccione Cambiar campo de entrada para cambiar la información almacenada para este campo. Puede cambiar un campo de entrada de una de las formas siguientes:

- Creando una entrada aleatoria

Para crear una entrada aleatoria, seleccione Aleatoria. Password Manager creará entradas aleatorias con 7, 14 ó 127 caracteres de longitud.

- Editando manualmente un campo de entrada

Para editar manualmente un campo de entrada, seleccione Editar y realice los cambios apropiados en el campo.

- Suprimir

Seleccione Suprimir para suprimir completamente el campo de entrada.

Nota: Si cambia un campo en Password Manager sólo se actualizará la información de inicio de sesión en Password Manager. Si desea aumentar la seguridad de sus contraseñas mediante la característica aleatoria de Password Manager, deberá sincronizar la aplicación o sitio Web con la nueva contraseña aleatoria generada por esta característica. Utilice la herramienta de transferencia de campos apropiada de Password Manager para transferir la nueva contraseña aleatoria al formulario "Cambiar contraseña" de la aplicación o sitio Web. Verifique que la nueva contraseña es válida para la aplicación o sitio Web y después utilice Guardar cambios de la ventana Password Manager - Gestionar. No es necesario volver a crear la entrada con la nueva contraseña ya que se conserva toda la información necesaria.

c. Pulse **Guardar cambios**

4. Pulse **Guardar cambios**

Exportación de información de inicio de sesión

IBM Password Manager le permite exportar su información de inicio de sesión confidencial de tal forma que pueda transportarla de forma segura de un sistema a otro. Cuando exporta la información de inicio de sesión desde IBM Password Manager, se crea un archivo de exportación protegido mediante contraseña que se puede almacenar en un soporte de almacenamiento extraíble. Puede utilizar este archivo para acceder a su información de usuario y contraseñas.

Para exportar la información de inicio de sesión que está almacenada en IBM Client Security Password Manager, realice el procedimiento siguiente:

1. Pulse el botón derecho del ratón en el icono de **Password Manager** en la bandeja de iconos de Windows y pulse **Gestionar**.

Nota: También puede acceder a la función Gestionar de Password Manager con el método abreviado de teclado **Control+Mayús+B**.

2. Introduzca su frase de paso UVM o complete los requisitos de acceso especificados por la política de autenticación de usuario UVM.
3. Pulse **Exportar**. Aparece la ventana Guardar como con la vía de acceso por omisión y el nombre de archivo PwMgrExportReader.
4. Seleccione la ubicación donde desea guardar el archivo de exportación.
5. Pulse **Guardar** para aceptar la ubicación y el nombre de archivo especificados. Aparece una pantalla solicitando que establezca una frase de paso para el archivo de exportación.
6. Establezca una frase de paso para el archivo de exportación y pulse **Aceptar**. Esta frase de paso será necesaria para acceder a los datos exportados. Aparecerá un mensaje que indica que la exportación se ha completado satisfactoriamente.
7. Pulse **Aceptar**.
8. Cierre IBM Password Manager.
9. Recupere el archivo de exportación creado en la ubicación que indicó y cópielo a un soporte de almacenamiento extraíble.

Antes de abrir este archivo en otro sistema, se solicitará la frase de paso de exportación que haya establecido en el procedimiento anterior. IBM Password Manager muestra la información confidencial en un lector seguro. Esta información no se puede imprimir ni guardar en el disco duro del sistema. Pulse **Aceptar** para cerrar el lector del archivo de exportación.

Capítulo 3. Limitaciones

Este apartado contiene información sobre limitaciones conocidas relacionadas con IBM Client Security Password Manager.

IBM Client Security Password Manager no soporta Netscape Navigator: debe utilizar Microsoft Internet Explorer para hacer uso de la funcionalidad del programa IBM Password Manager. El software Password Manager no soporta Netscape Navigator.

Apéndice. Avisos y marcas registradas

Este apéndice ofrece avisos legales para los productos de IBM así como información de marcas registradas.

Avisos

Esta información se ha desarrollado para productos y servicios que se ofrecen en los Estados Unidos.

IBM quizá no ofrezca los productos, servicios o dispositivos mencionados en este documento, en otros países. Consulte al representante local de IBM para obtener información sobre los productos y servicios que actualmente pueden adquirirse en su zona geográfica. Las referencias a un producto, programa o servicio de IBM no pretenden afirmar ni implicar que sólo pueda utilizarse este producto, programa o servicio de IBM. En su lugar se puede utilizar cualquier producto, programa o servicio funcionalmente equivalente que no vulnere ningún derecho de propiedad intelectual de IBM. Sin embargo, es responsabilidad del usuario evaluar y verificar el funcionamiento de cualquier producto, programa o servicio que no sea de IBM.

IBM puede tener patentes o solicitudes de patentes en tramitación que hacen referencia a temas tratados en este documento. La posesión de este documento no otorga ninguna licencia sobre dichas patentes. Puede realizar consultas sobre licencias escribiendo a:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785
EE.UU.

El párrafo siguiente no es aplicable al Reino Unido ni a ningún otro país en el que tales disposiciones sean incompatibles con la legislación local:

INTERNATIONAL BUSINESS MACHINES CORPORATION PROPORCIONA ESTA PUBLICACIÓN "TAL CUAL" SIN GARANTÍAS DE NINGÚN TIPO, NI EXPLÍCITAS NI IMPLÍCITAS, INCLUIDAS, PERO SIN LIMITARSE A ELLAS, LAS GARANTÍAS IMPLÍCITAS DE NO VULNERACIÓN DE DERECHOS, COMERCIALIZABILIDAD O IDONEIDAD PARA UN FIN DETERMINADO. Algunos estados no autorizan la exclusión de garantías explícitas o implícitas en determinadas transacciones, por lo que es posible que este aviso no sea aplicable en su caso.

La presente publicación puede contener inexactitudes técnicas o errores tipográficos. Periódicamente se efectúan cambios en la información aquí contenida; estos cambios se incorporarán en nuevas ediciones de la publicación. IBM puede realizar mejoras y/o cambios en los productos y/o programas descritos en esta publicación cuando lo considere oportuno y sin previo aviso.

Los usuarios con licencia de este programa que deseen obtener información sobre el mismo para poder: (i) intercambiar información entre programas creados de forma independiente y otros programas (incluido éste) y (ii) utilizar de forma mutua la información intercambiada, deben ponerse en contacto con IBM Corporation, Department 80D, P.O. Box 12195, 3039 Cornwallis, Research Triangle

Park, NC 27709, EE.UU. La disponibilidad de esta información, de acuerdo con los términos y condiciones correspondientes, podría incluir en algunos casos el pago de una tarifa.

El programa bajo licencia que se describe en este documento y todo el material bajo licencia disponible para el mismo es proporcionado por IBM bajo los términos que se especifican en IBM Customer Agreement, International Programming License Agreement o en cualquier otro acuerdo equivalente acordado entre las partes.

Marcas registradas

IBM y SecureWay son marcas registradas de IBM Corporation en los Estados Unidos y/o en otros países.

Tivoli es una marca registrada de Tivoli Systems Inc. en los Estados Unidos y/o en otros países.

Microsoft, Windows y Windows NT son marcas registradas de Microsoft Corporation en los Estados Unidos y/o en otros países.

Otros nombres de empresas, productos y servicios pueden ser marcas registradas o marcas de servicio de otras empresas.

IBM