Software HP ProtectTools for Small Business Security, versión 5.10

Guía del usuario

Software HP ProtectTools for Small Business Security versión 5.10 Guía del usuario

HP Business PC

Tercera edición: julio de 2010

Número de referencia del documento: 610663-E53

Acerca de esta publicación

Esta guía proporciona información acerca del software HP ProtectTools para Seguridad de las Pequeñas Empresas.

⚠ **¡ADVERTENCIA!** El texto presentado de esta forma indica que, si no se siguen las instrucciones, se pueden producir daños físicos o pérdida de la vida.

△ **PRECAUCIÓN:** El texto presentado de esta forma indica que, si no se siguen las instrucciones, se pueden producir daños en el equipo o pérdida de información.

NOTA: El texto presentado de esta manera proporciona información importante complementaria.

Tabla de contenido

1 Introducción a seguridad 1

Recursos de HP ProtectTools 2

Descripción de productos de seguridad de HP ProtectTools y ejemplos de uso común 3

Credential Manager for HP ProtectTools 3

Drive Encryption for HP ProtectTools 4

File Sanitizer for HP ProtectTools 4

Device Access Manager for HP ProtectTools 5

2 Guía de configuración fácil para las opciones más útiles 6

Pasos iniciales 6

Credential Manager for HP ProtectTools 8

Visualización y administración de las autenticaciones guardadas en el Administrador de contraseñas 10

File Sanitizer for HP ProtectTools 13

Device Access Manager for HP ProtectTools 16

Drive Encryption for HP ProtectTools 18

3 Ventajas de HP ProtectTools for Small Business 20

Acceso al software HP ProtectTools para Seguridad de las Pequeñas Empresas 20

Logrando objetivos principales de seguridad 20

Restricción de acceso a datos sensibles 20

Prevención contra acceso no autorizado desde ubicaciones internas o externas 21

Creación de políticas sólidas de contraseña 21

Elementos adicionales de seguridad 21

Asignación de funciones de seguridad 21

Administración de contraseñas de HP ProtectTools 22

Creación de una contraseña segura 22

Copia de seguridad de sus credenciales y configuración 23

4 Consola administrativa de HP ProtectTools Security Manager 24

Acerca de la Consola administrativa de HP ProtectTools 24

Uso de Consola administrativa 24

Pasos iniciales con el asistente de configuración 25

Configuración del sistema 26

Activación de recursos de seguridad 26
Definición de las políticas de autenticación de Security Manager 26
Ficha Inicio de sesión 26
Ficha Política de Sesión 27
Definición de configuración 27
Administración de usuarios 27
Adición de un usuario 28
Eliminación de un usuario 28
Comprobación de estado de un usuario 28
Configuración de parámetros de las aplicaciones 29
Encriptado de unidades 30
Administración de Device Access 30

5 HP ProtectTools Security Manager 31
Administración de contraseñas 31
Configuración de credenciales 31
Cambio de la contraseña de Windows 31
Trituración o purificación de archivos 32
Visualización de estado de encriptación de unidad 32
Visualización de device access 32
Adición de aplicaciones 33
Configuración de preferencias 33
Copia de seguridad y restauración 33
Copias de seguridad de sus datos 34
Restauración de sus datos 34
Cambio de la imagen y del nombre de usuario de Windows 35

6 Drive Encryption for HP ProtectTools 36
Procedimientos de configuración 37
Apertura de Drive Encryption 37
Tareas generales 38
Activación de Drive Encryption 38
Desactivación de Drive Encryption 38
Inicio de sesión después de activar Drive Encryption 38
Tareas avanzadas 39
Administración de Drive Encryption (tarea de administrador) 39
Encriptado o desencriptado de unidades individuales 39
Copia de seguridad y restauración (tarea de administrador) 39
Creación de claves de copia de seguridad 39

7 Credential Manager for HP ProtectTools 40
Adición de inicios de sesión 41
Edición de inicios de sesión 42

Uso del menú inicios de sesión 42
Organización de inicios de sesión en categorías 43
Administración de inicios de sesión 43
Acceso a seguridad de la contraseña 44
Configuración del icono de Administrador de contraseñas 44

8 File Sanitizer for HP ProtectTools 45
Procedimientos de configuración 46
Apertura de File Sanitizer 46
Configuración de la programación de purificación del espacio libre 46
Configuración de una programación de trituración 46
Selección o creación de un perfil de trituración 47
Selección de un perfil de trituración predefinido 47
Personalización de un perfil de trituración de seguridad avanzada 47
Personalización de un perfil de eliminación simple 48
Tareas generales 49
Uso de una secuencia de teclas para iniciar trituración 49
Uso del icono File Sanitizer 49
Trituración manual de un activo 49
Trituración manual de todos los elementos seleccionados 50
Activación manual de purificación de espacio libre 50
Anulación de una operación de trituración o de purificación de espacio libre 51
Visualización de los archivos de registro 51

9 Device Access Manager for HP ProtectTools 52
Inicio de servicio en segundo plano 52
Configuración sencilla 52
Configuración de clases de dispositivos (avanzado) 53
Agregado de un usuario o grupo 53
Eliminación de un usuario o grupo 53
Denegación o permiso de acceso a un usuario o grupo 54
Configuraciones de acceso de usuario (avanzada) 55
Adición de un usuario o grupo 55
Eliminación de un usuario o grupo 55
Permiso o denegación de permiso 55

Glosario 57

Índice 59

1 Introducción a seguridad

HP entiende que su tiempo es extremadamente valioso, y que usted necesita concentrarse en la administración y crecimiento de su negocio – no solamente preocuparse sobre el software de seguridad adecuado para proteger su PC, sus datos y su negocio.

Es importante que considere proactivamente soluciones de seguridad que sean fáciles de utilizar pero que proporcionen una protección sólida para sus activos de negocio. Seguridad no es algo “bonito de tener” – es un “¡deber!”

HP brinda protección que es fácil de implementar y sencilla de utilizar…se llama HP ProtectTools for Small Business.

HP ProtectTools for Small Business es un software de seguridad que proporciona recursos que ayudan a proteger contra al acceso no autorizado a las computadoras y datos críticos. La funcionalidad de seguridad optimizada se suministra a través de los varios módulos de software HP ProtectTools:

HP ProtectTools for Small Business provee dos versiones que pueden utilizarse: Consola administrativa de HP ProtectTools Security Manager y HP ProtectTools Security Manager (para usuarios en general). Ambas versiones de administrador y usuario están disponibles en el menú **Inicio** > **Todos los programas**.

Función	Recursos
Consola administrativa de HP ProtectTools Security Manager	• Requiere los derechos de administrador del sistema de Microsoft Windows para acceder • Acceso a módulos que tienen que ser configurados por un administrador y que no están disponibles para los usuarios generales • Permite una configuración de seguridad inicial y configura las opciones o los requisitos para todos los usuarios
HP ProtectTools Security Manager (para usuarios en general)	• Permite a los usuarios configurar las opciones suministradas por un administrador • Puede restringir acceso y sólo permitir a un usuario controles limitados de algunos módulos de HP ProtectTools modules

Los módulos de software HP ProtectTools pueden estar preinstalados, precargados o disponibles como una opción configurable o como un producto en el mercado de accesorios. Para obtener más información, visite http://www.hp.com.

Recursos de HP ProtectTools

La tabla siguiente muestra detalles de los recursos principales de los módulos HP ProtectTools for Small Business:

Módulo	Recursos principales
Consola administrativa de HP ProtectTools Security Manager	• El asistente de configuración de Security Manager es utilizado por los administradores para instalar y configurar los niveles de seguridad y los métodos de seguridad de inicio de sesión. • Opciones de configuración ocultas para los usuarios básicos. • Configuración de los parámetros de Device Access Manager y del acceso a usuarios. • Herramientas del administrador son utilizadas para agregar y eliminar usuarios de HP ProtectTools y para visualizar el estado de usuarios.
HP ProtectTools Security Manager (para usuarios en general)	• Organización, configuración y cambios de nombres de usuario y contraseñas. • Configuración y cambio de credenciales de usuarios, como contraseña de Windows y Smart Card. • Definición y cambio de configuración, purificación y trituración de File Sanitizer. • Visualización de configuración para Device Access Manager. • Configuración de preferencias y opciones de copia de seguridad y restauración.
Credential Manager for HP ProtectTools	• Está diseñado para guardar, organizar y proteger los nombres y contraseñas de usuarios. • Le permite configurar las pantallas de inicio de sesión de sitios web y programas para proporcionar un rápido y seguro acceso. • A medida que accede varios sitios web y desee guardar su nombre y contraseña de usuario, ingréselos en el Administrador de contraseñas para que no tenga que recordarlos nuevamente. La próxima vez que visite este sitio, el Administrador de contraseñas llenará y enviará los datos automáticamente. • Le permite crear señas más difíciles que no tendrá que escribirlas o recordarlas, y mantiene sus cuentas más seguras.
Drive Encryption for HP ProtectTools	• Ofrece encriptación completa de todo el volumen de la unidad de disco duro. • Fuerza una autenticación de pre-inicialización a fin de encriptar y acceder a los datos en la unidad de disco duro. • Ayuda a cumplir los requisitos legales o del sector para proteger datos confidenciales y datos. • Protege sus datos de acceso no autorizado encriptando toda la unidad de disco duro. Si alguna vez roban la PC y extraen la unidad del sistema original y la instalan en un sistema diferente, los datos no serán comprometidos.

Módulo	Recursos principales
File Sanitizer for HP ProtectTools	• Eliminación de datos en Windows, no elimina completamente el contenido de su unidad de disco duro. Windows sólo elimina la referencia a los datos. Los datos aún permanecen en la unidad de disco duro hasta que otro archivo sobrescribe esa misma área en la unidad de disco duro con nueva información. Sin embargo, con File Sanitizer, usted puede borrar completa y automáticamente documentos, historial del navegador web, archivos temporales, etc. • Le permite borrar con seguridad (o triturar) archivos y carpetas críticos (información personal o archivos, historial de datos o relacionados con la web u otros componentes de datos) en su equipo y hace una purificación periódica (grabación sobre datos previamente eliminados) de su unidad de disco duro.
Device Access Manager for HP ProtectTools	• Puede utilizarse para controlar el acceso a unidades de multimedia, USB, y otros dispositivos de hardware basados en perfiles de usuario. • Le permite limitar la capacidad de un usuario de guardar datos críticos. • Evita que usuarios utilicen dispositivos de almacenamiento externos, como un reproductor personal de música para copiar datos de una PC o de su red. • Evita que usuarios introduzcan virus en el sistema desde multimedia externa. • Le permite desactivar selectivamente un grupo de dispositivos (como llaves USB, dispositivos de grabación, reproductores personales de música, etc.) por usuario o grupo de usuarios. La persona con una contraseña de administrador puede iniciar sesión y copiar información desde la PC, pero otros usuarios no pueden.

Descripción de productos de seguridad de HP ProtectTools y ejemplos de uso común

La mayoría de productos de seguridad de HP ProtectTools poseen una autenticación de usuario (normalmente una contraseña) y una copia de seguridad administrativa para obtener acceso si se pierden, no están disponibles o se olvidan las contraseñas o en cualquier momento que se requiera acceso a seguridad corporativa.

NOTA: Algunos de los productos de seguridad de HP ProtectTools son diseñados para restringir el acceso a datos. Los datos deben encriptarse cuando son tan importantes que el usuario opte por perder la información antes de comprometerla. Se recomienda que se realicen copias de seguridad de todos los datos en una ubicación segura.

Credential Manager for HP ProtectTools

Credential Manager (parte de Security Manager) es un depósito de nombres de usuario y contraseñas. Se utiliza más frecuentemente para guardar nombres y contraseñas de inicio de sesión para acceso a Internet o correo en la web. Credential Manager puede iniciar sesión del usuario automáticamente en un sitio web o correo.

Ejemplo 1: Un agente de compras de un pequeño fabricante realiza la mayoría de sus transacciones corporativas a través de la Internet. Ella también visita frecuentemente varios sitios web populares que requieren información de inicio de sesión. Ella tiene una gran preocupación con la seguridad, por lo que no utiliza la misma contraseña en cada cuenta. La agente de compras decidió utilizar Credential Manager para corresponder enlaces web con diferentes nombres de usuario y contraseñas. Cuando ella decide ingresar a un sitio web para iniciar sesión, Credential Manager le presenta las credenciales automáticamente. Si ella decide visualizar los nombres de usuario y contraseñas, Credential Manager puede configurarse para que las revele.

Credential Manager también puede utilizarse para administrar y organizar las autenticaciones. Esta herramienta permite que un usuario elija que activo de web o red desea seleccionar y acceder directamente ese enlace. El usuario también puede visualizar los nombres de usuario y contraseñas cuando sea necesario.

Ejemplo 2: Un contador público certificado muy trabajador de una pequeña empresa de contabilidad ha sido asignado para administrar cómo los clientes hacen inicio de sesión en su sitio web seguro para publicar actualizaciones. El contador desea controlar el acceso y compartir la información de inicio de sesión actual. El contador decide organizar todos los enlaces web, nombres de usuario y contraseñas de la compañía en Credential Manager for HP ProtectTools. Una vez completado, el contador implementa Credential Manager para que los empleados puedan trabajar en las cuentas de la web y que nunca sepan las credenciales de inicio de sesión que están utilizando.

Drive Encryption for HP ProtectTools

Drive Encryption se utiliza más frecuentemente para restringir el acceso a los datos en toda la unidad de disco duro del equipo o una unidad de disco duro secundaria.

Ejemplo 1: Un doctor desea asegurarse que sólo él puede acceder los datos en la unidad de disco duro de su equipo. El doctor activa Drive Encryption que habilita el requisito de autenticación en la preinicialización antes de iniciar sesión en Windows. Una vez definido, la unidad de disco duro no puede abrirse sin ingresar una contraseña antes de inicializar el sistema operativo.

Drive Encryption for HP ProtectTools no permitirá acceso a los datos encriptados aún cuando se extraiga la unidad, porque está vinculado a la placa madre original.

Ejemplo 2: Un administrador de una clínica pequeña, desea segura que sólo los doctores y personal autorizado puedan acceder todos los datos en su equipo local sin necesidad de compartir sus contraseñas personales. El departamento de TI agrega el administrador, los doctores y todo el personal autorizado como usuarios de Drive Encryption. Ahora sólo personal autorizado puede ingresar al equipo utilizando sus nombres de usuario y contraseñas personales.

File Sanitizer for HP ProtectTools

File Sanitizer for HP ProtectTools se utiliza para eliminar datos de forma permanente, incluyendo actividad de navegación en la Internet, archivos temporales, datos previamente eliminados y cualquier otra información. File Sanitizer puede configurarse para ejecutar manual o automáticamente en una programación definida por el usuario.

Ejemplo 1: Un abogado frecuentemente tiene acceso a información sensible de los clientes y desea asegurar que los datos en archivos eliminados no sean recuperados. El abogado utiliza File Sanitizer para “triturar” archivos eliminados para que sea casi imposible recuperarlos.

Normalmente cuando Windows elimina datos, en realidad no borra los datos de la unidad de disco duro. En su lugar, marca los sectores de la unidad de disco duro como disponibles para uso futuro. Hasta que los datos son sobrescritos, estos pueden ser fácilmente recuperados utilizando herramientas comunes disponibles en la Internet. File Sanitizer sobrescribe los sectores con datos

aleatorios (múltiples veces si es necesario), consecuentemente tornando los datos eliminados ilegibles y sin posibilidad de recuperación.

Ejemplo 2: Una investigadora desea triturar datos eliminados, archivos temporales, actividad de navegación, etc. automáticamente cuando ella cierra sesión. Ella utiliza File Sanitizer para programar la “trituración” de tal manera que ella puede seleccionar los archivos comunes o cualesquier archivos personalizados para eliminarlos de forma permanente automáticamente.

Device Access Manager for HP ProtectTools

Device Access Manager for HP ProtectTools puede utilizarse para bloquear acceso no autorizado a unidades flash USB donde los datos pueden copiarse. Un ejemplo sería una situación donde proveedores externos necesitan acceso a equipos de la compañía pero que no pueden copiar los datos a una unidad USB. Device Access Manager for HP ProtectTools permite que un administrador restrinja y gestione acceso a hardware. También puede restringir acceso a unidades de CD/DVD, control de dispositivos USB, conexiones de red, etc.

Ejemplo 1: Un gerente de una compañía de suministros médicos trabaja frecuentemente con registros personales médicos junto con la información de su compañía. Los empleados necesitan acceso a estos datos, sin embargo, es extremadamente importante que los datos no sean eliminados del equipo mediante el uso una unidad USB o cualquier otra multimedia de almacenamiento externo. La red es segura, pero los equipos tienen grabadores de CD y puertos USB que podrían permitir la copia o robo de los datos. El gerente utiliza Device Access Manager para desactivar los puertos USB y grabadores de CD para que no puedan utilizarse. Aún cuando los puertos USB estén bloqueados, el mouse y los teclados continuarán funcionando.

Ejemplo 2: Una compañía de seguros no desea que sus empleados instalen o carguen software o datos personales desde sus residencias. Algunos empleados necesitan tener acceso al puerto USB en todos los equipos. El gerente de TI utiliza Device Access Manager para permitir acceso para algunos empleados mientras que bloquea acceso externo a otros.

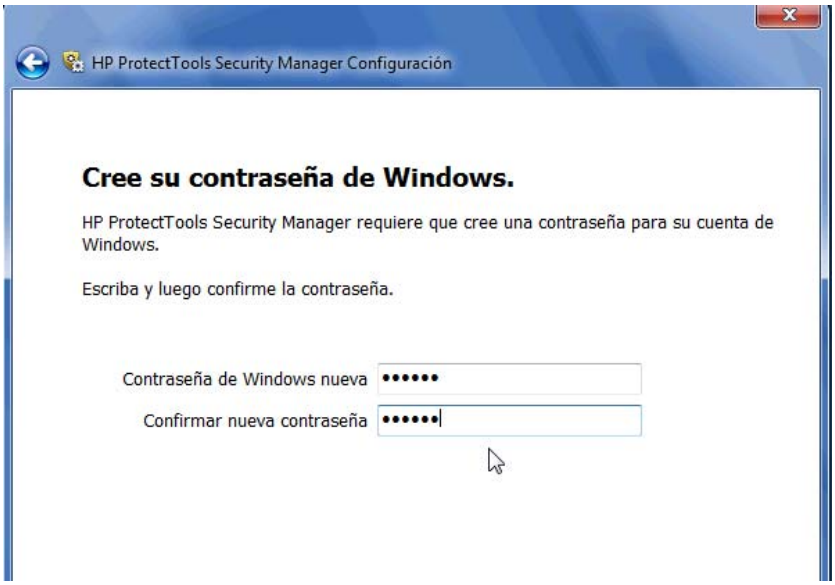
2 Guía de configuración fácil para las opciones más útiles

Esta guía de configuración fácil está proyectada para demostrar los pasos básicos para activar las opciones más comunes y útiles en HP ProtectTools for Small Business. Existen varias herramientas y opciones disponibles en este software que le permitirán ajustar sus preferencias y definir su control de acceso. La guía de configuración fácil enfocará en mantener cada módulo funcionando con el menor tiempo y esfuerzo de configuración. Para obtener más información, sólo seleccione el módulo en el cual está interesado y haga clic en el símbolo “?” o en el botón de ayuda en la esquina superior derecha. Este botón proporcionará información automáticamente para ayudarle con la ventana actualmente exhibida.

Pasos iniciales

1. Abra HP ProtectTools Security Manager desde el icono Gadget, icono en la barra de tareas (escudo dorado), o haga clic en **Inicio** > **Todos los programas** > **HP**.

2. Ingrese su contraseña de Windows o cree una contraseña de Windows.

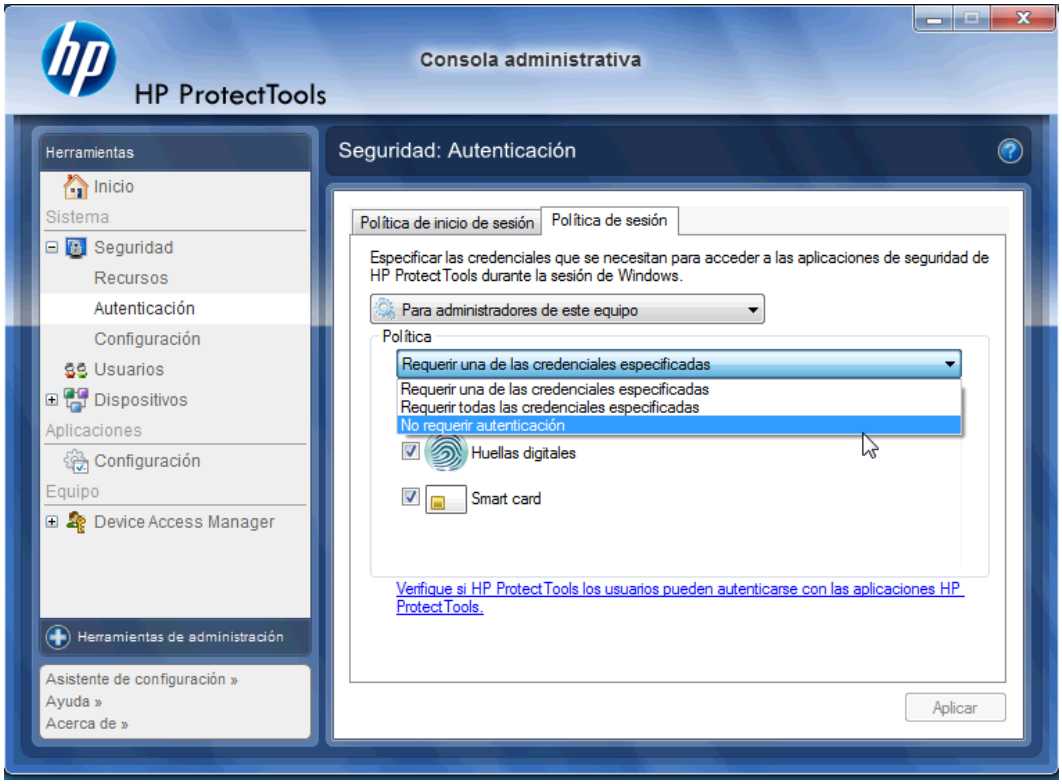


3. Finalice el asistente de configuración.

NOTA: De forma predeterminada, HP ProtectTools Security Manager está definido para política de autenticación sólida.

Esta definición está diseñada para evitar el acceso no autorizado mientras haya iniciado sesión en Windows y debe utilizarse cuando se necesita máxima seguridad o si usuarios están lejos de sus sistemas con frecuencia durante el día. Si usted gustaría cambiar esta definición, haga clic en la ficha política de sesión, y haga sus selecciones.

Para configurar HP ProtectTools Security Manager para que utilice sólo el inicio de sesión inicial de Windows para toda la sesión, cambie la siguiente configuración.



Para hacer que HP ProtectTools Security Manager autentique sólo una vez durante el inicio de sesión de Windows:

1. Haga clic en **Inicio** > **Todos los programas** > **HP** > **Consola administrativa de HP ProtectTools**.
2. En el panel izquierdo **Herramientas**, seleccione **Autenticación** desde el grupo **Seguridad**.
3. Haga clic en la ficha **Política de sesión** y seleccione **No requerir autenticación** desde el menú desplegable en **Política**.
4. Haga clic en el botón **Aplicar** cuando finalice.

Credential Manager for HP ProtectTools

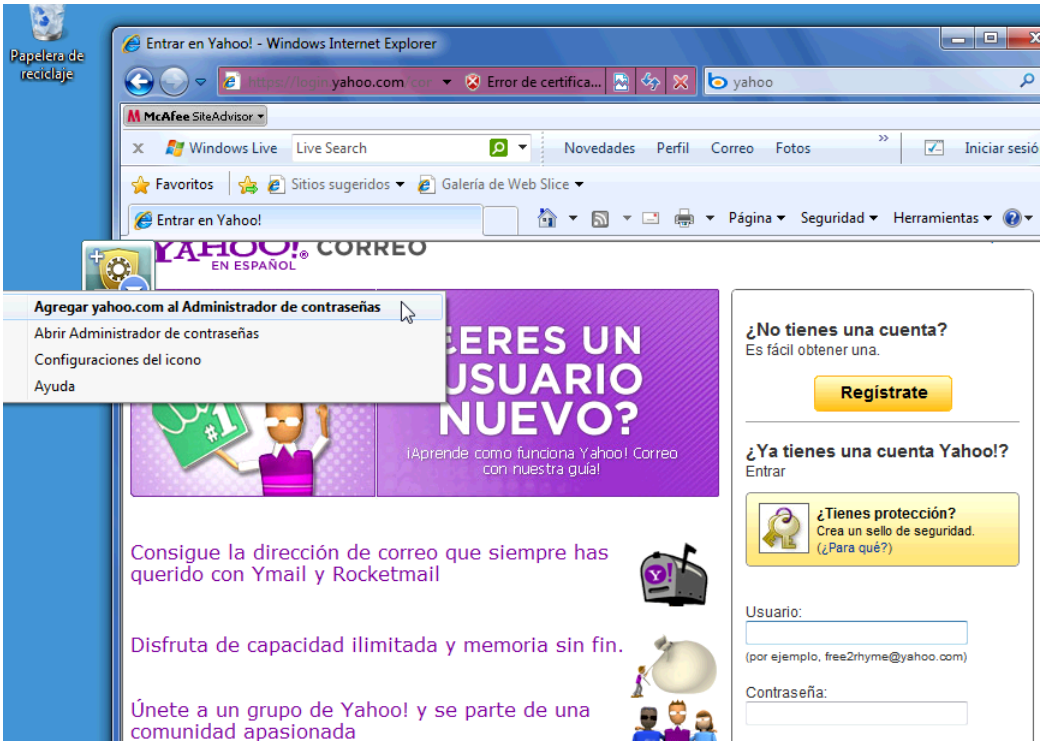
¡Contraseñas! Todos tenemos bastantes de ellas – especialmente si accede sitios web con frecuencia o utiliza aplicaciones que requieren que inicie de sesión. Un usuario normal utiliza la misma contraseña para cada aplicación o sitio web, o usa su imaginación y rápidamente se olvida cual contraseña pertenece a cual aplicación.

¿No sería estupendo que el software recordara automáticamente sus contraseñas a sitios que no son críticos o que le brindan la capacidad de distinguir cuales sitios recordar y cuales ignorar? Credential Manager for HP ProtectTools es la respuesta. Credential Manager es el Administrador de contraseñas que le brinda esa capacidad. Una vez que haga inicio de sesión en la PC, Credential Manager le suministrará sus contraseñas y credenciales según sea necesario.

Cuando accede cualquier aplicación o sitio web que requiera credenciales, el Administrador de contraseñas reconocerá automáticamente el sitio, y le preguntará si desea que el software recuerde su información. Si acepta, usted nunca más tendrá que recordar esa contraseña nuevamente. Puede rehusar la solicitud para recordar su información si desea excluir ciertos sitios.

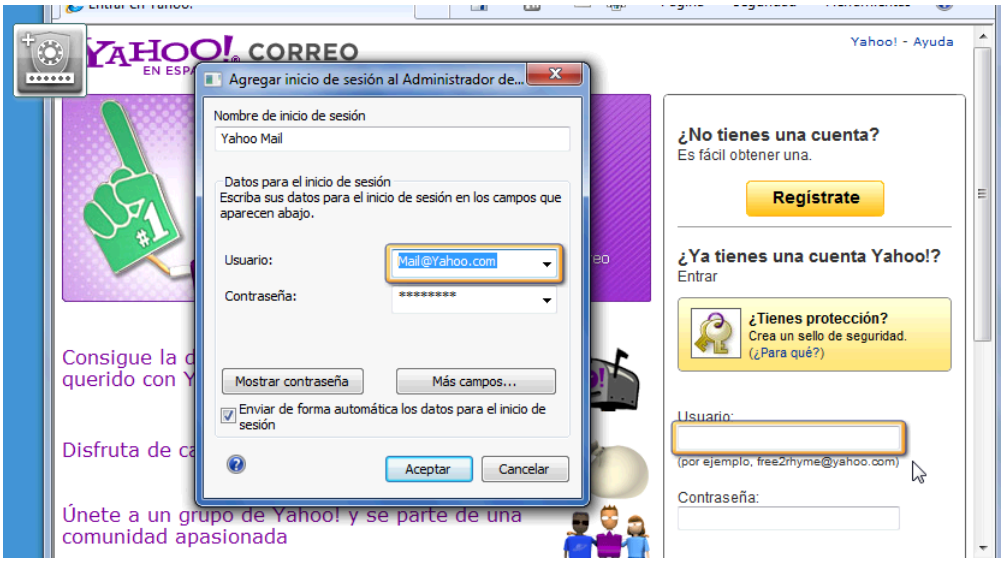
Para comenzar a guardar ubicaciones web, nombres de usuario y contraseñas:

1. Como un ejemplo, navegue a su cuenta de correo electrónico en la web y solicite al Administrador de contraseñas (haga clic en el icono) para que agregue la autenticación web.



2. Nombre el enlace (opcional) e ingrese un nombre de usuario y contraseña en Credential Manager.

NOTA: La página web destacará las áreas que el Administrador de contraseñas utilizará ahora y para visitas subsecuentes.



3. Cuando finalice, haga clic en el botón **Aceptar**.

4. Administrador de contraseñas también puede guardar su nombre de usuario y contraseñas para recursos compartidos de red o asignación de unidades en la red.

Visualización y administración de las autenticaciones guardadas en el Administrador de contraseñas

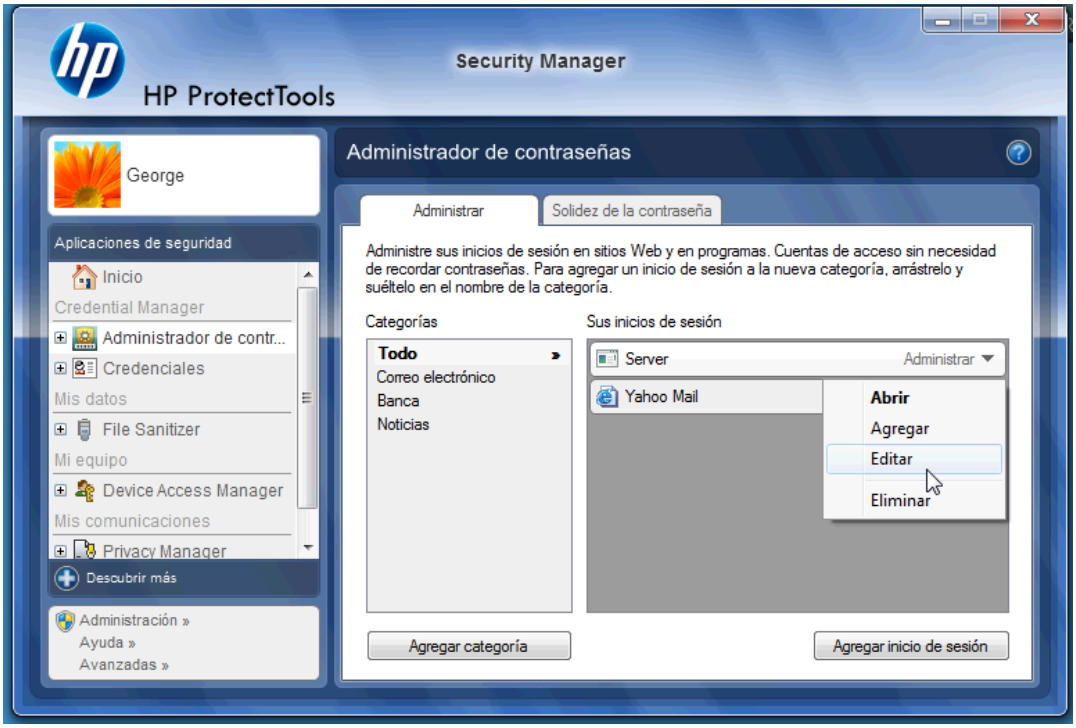
Las ventajas del Administrador de contraseñas son que usted puede visualizar, administrar, hacer copia de seguridad e iniciar sus autenticaciones desde una ubicación central. Administrador de contraseñas también soportará el inicio de sitios guardados desde Windows.

Para abrir HP Recovery Manager, utilice uno de los dos métodos siguientes:

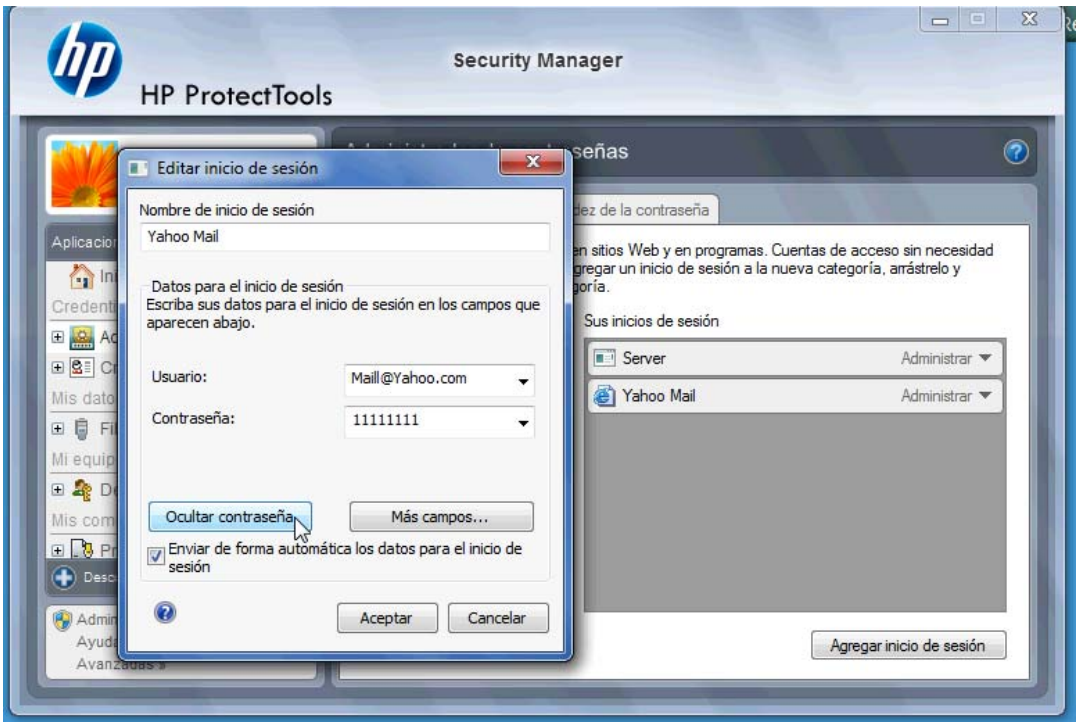
- Utilice la combinación de teclado de Ctrl + Windows + H para abrir el Administrador de contraseñas. Al seleccionar **Abrir** iniciará y autenticará rápidamente el acceso directo guardado.

O

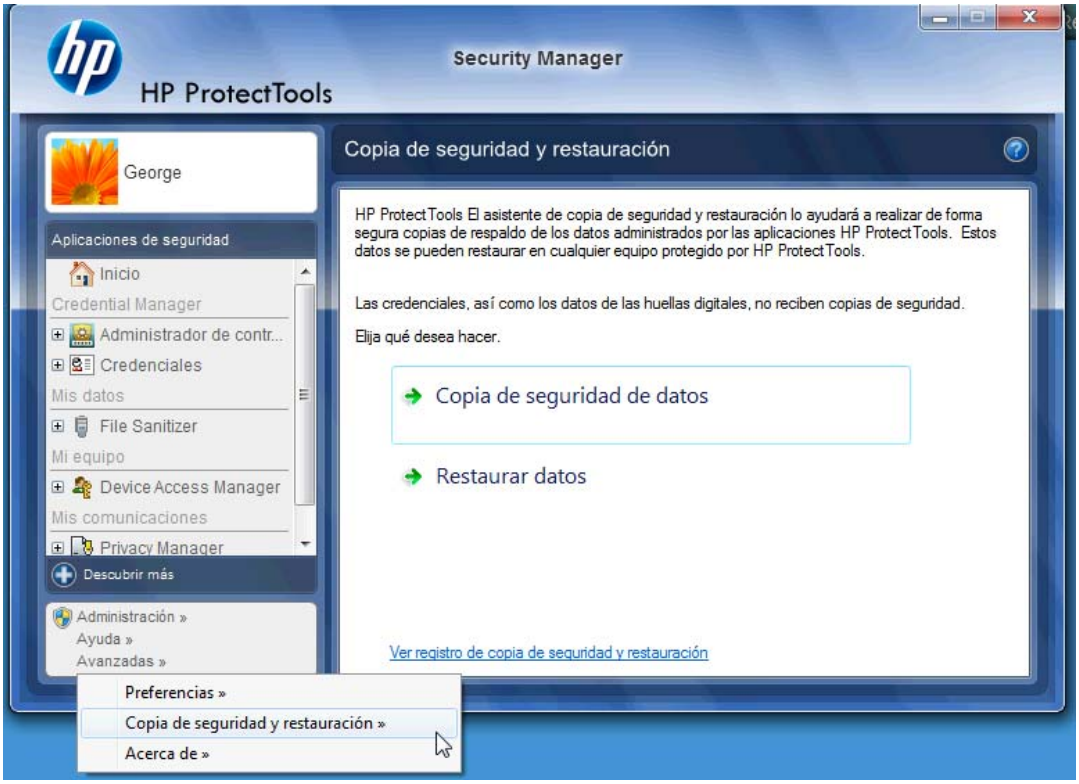
- Seleccione la ficha **Administrar** en Administrador de contraseñas para abrir HP ProtectTools Security Manager donde pueden ser editadas las credenciales.



La opción **Editar** del Administrador de contraseñas le permitirá visualizar y modificar en nombre, nombre de inicio de sesión, y aún revelar las contraseñas.



HP ProtectTools for Small Business permite hacer copia de seguridad y/o copiar todas las credenciales y configuraciones para otra PC.


HP ProtectTools
Security Manager
George
Aplicaciones de seguridad
Inicio
Credential Manager
Administrador de contr...
Credenciales
Mis datos
File Sanitizer
Mi equipo
Device Access Manager
Mis comunicaciones
Privacy Manager
Descubrir más
Administración »
Ayuda »
Avanzadas »
Preferencias »
Copia de seguridad y restauración »
Acerca de »
Copia de seguridad y restauración
HP ProtectTools El asistente de copia de seguridad y restauración lo ayudará a realizar de forma segura copias de respaldo de los datos administrados por las aplicaciones HP ProtectTools. Estos datos se pueden restaurar en cualquier equipo protegido por HP ProtectTools.
Las credenciales, así como los datos de las huellas digitales, no reciben copias de seguridad.
Elija qué desea hacer.
Copia de seguridad de datos
Restaurar datos
Ver registro de copia de seguridad y restauración

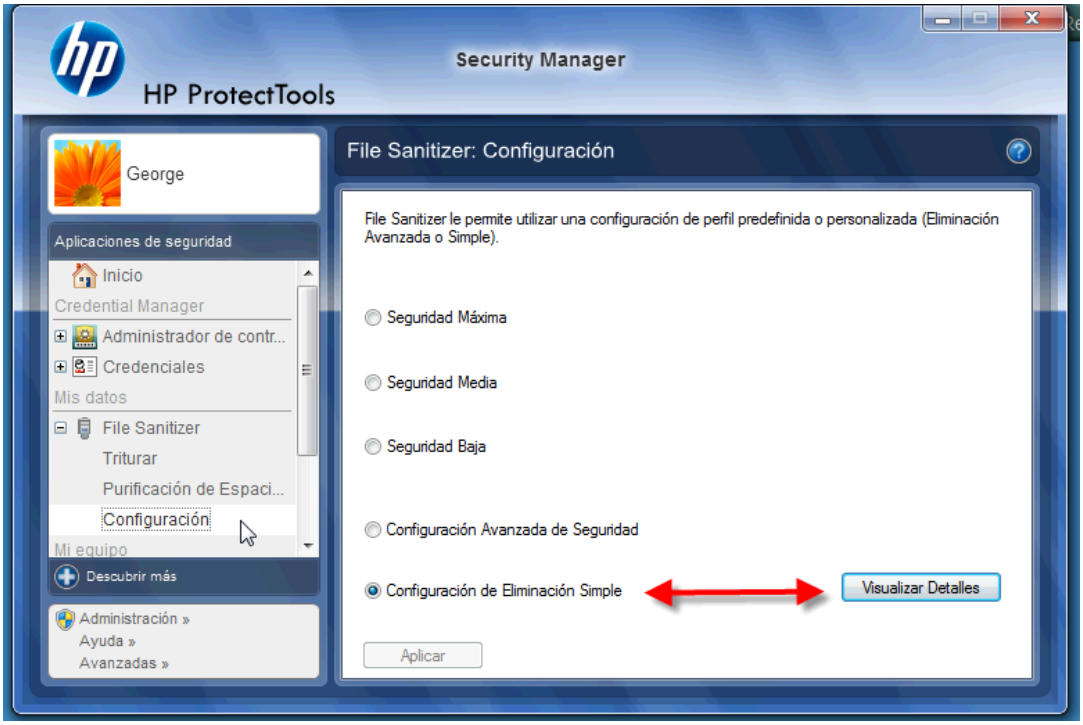
File Sanitizer for HP ProtectTools

File Sanitizer está diseñado para tornar difícil para que una persona no autorizada recupere datos que usted eliminó. Existen múltiples opciones disponibles para que usted borre manualmente o para establecer una programación regular para borrar archivos y carpetas seleccionados incluyendo el historial del navegador.

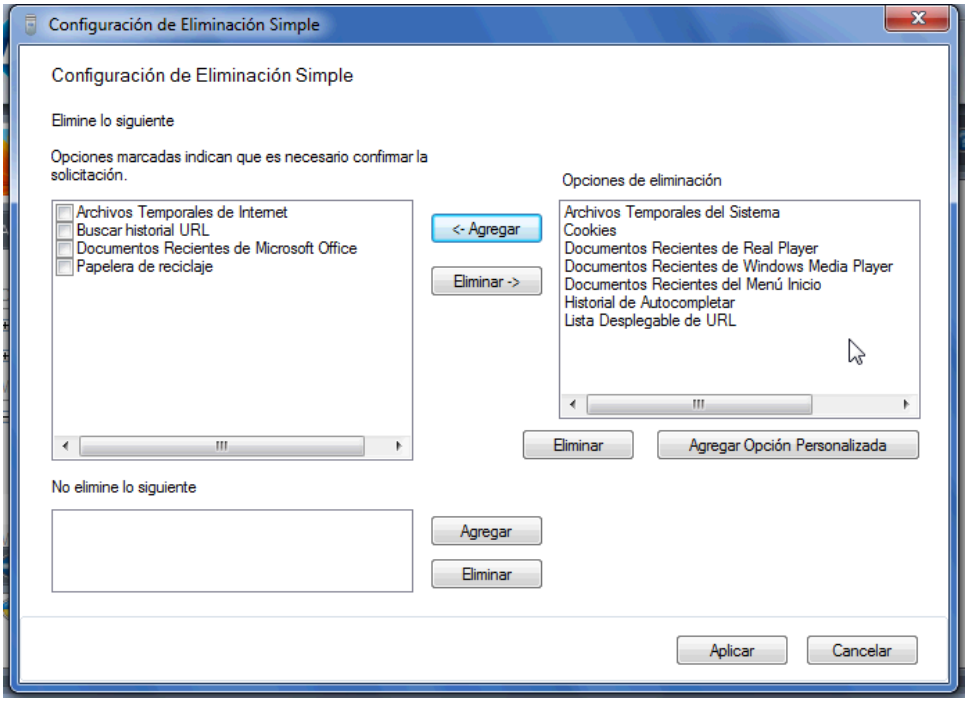
A continuación mostramos algunas definiciones simples de configuración.

Para comenzar a borrar permanentemente sus datos eliminados, seleccione el archivo o carpetas que ya no necesita.

1. Navegue para **Security Manager** > **File Sanitizer** > **Configuración**. Seleccione **Configuración de Eliminación Simple** y haga clic en el botón **Visualizar Detalles**.



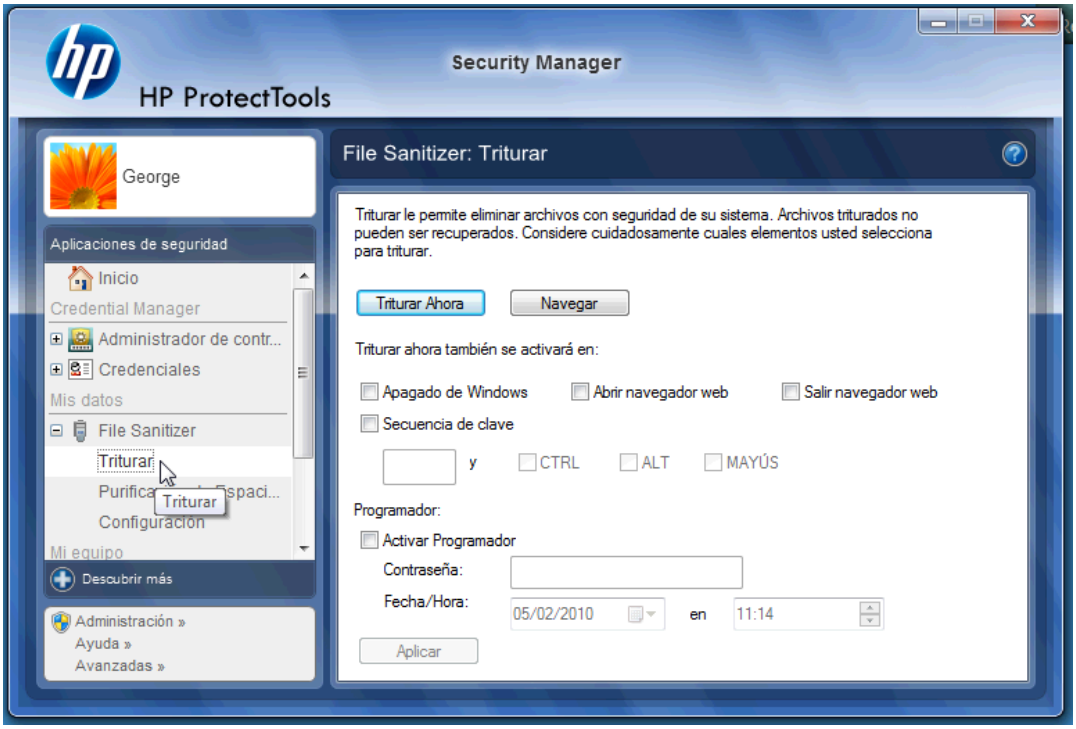
2. Seleccione los elementos en la parte lateral derecha de la ventana Configuración de Eliminación Simple que usted desea eliminar permanentemente con frecuencia y haga clic en el botón **<- Agregar** para mover los elementos seleccionados para el lado de eliminación.



3. Inicie con la papelera de reciclaje y agregue otros elementos que desee borrar a través de trituración.

4. Haga clic en el botón **Aplicar** cuando haya seleccionado todo lo que desee borrar permanentemente.

5. Navegue para la opción **Triturar** y configure cuándo desea ejecutar la acción. El botón **Triturar Ahora** borrará inmediatamente los elementos seleccionados en la ventana Configuración de Eliminación Simple que terminó de configurar.



6. Una pequeña burbuja emergente aparecerá en la barra de tareas cada vez que se inicia y se finaliza triturar.

Device Access Manager for HP ProtectTools

Device Access Manager puede utilizarse para restringir el uso de varios dispositivos de almacenamiento internos y externos para que sus datos permanezcan seguros en la unidad de disco duro y no salgan por la puerta de su negocio. Un ejemplo sería permitir el acceso de un usuario a sus datos pero bloquearlo de copiarlos a un CD, reproductor personal de música o un dispositivo de memoria USB. A continuación mostramos una manera fácil de cómo configurar esto.

1. Haga clic en **Inicio** > **Todos los programas** > **HP** > **Consola administrativa** > **Device Access Manager** > **Configuración sencilla**.

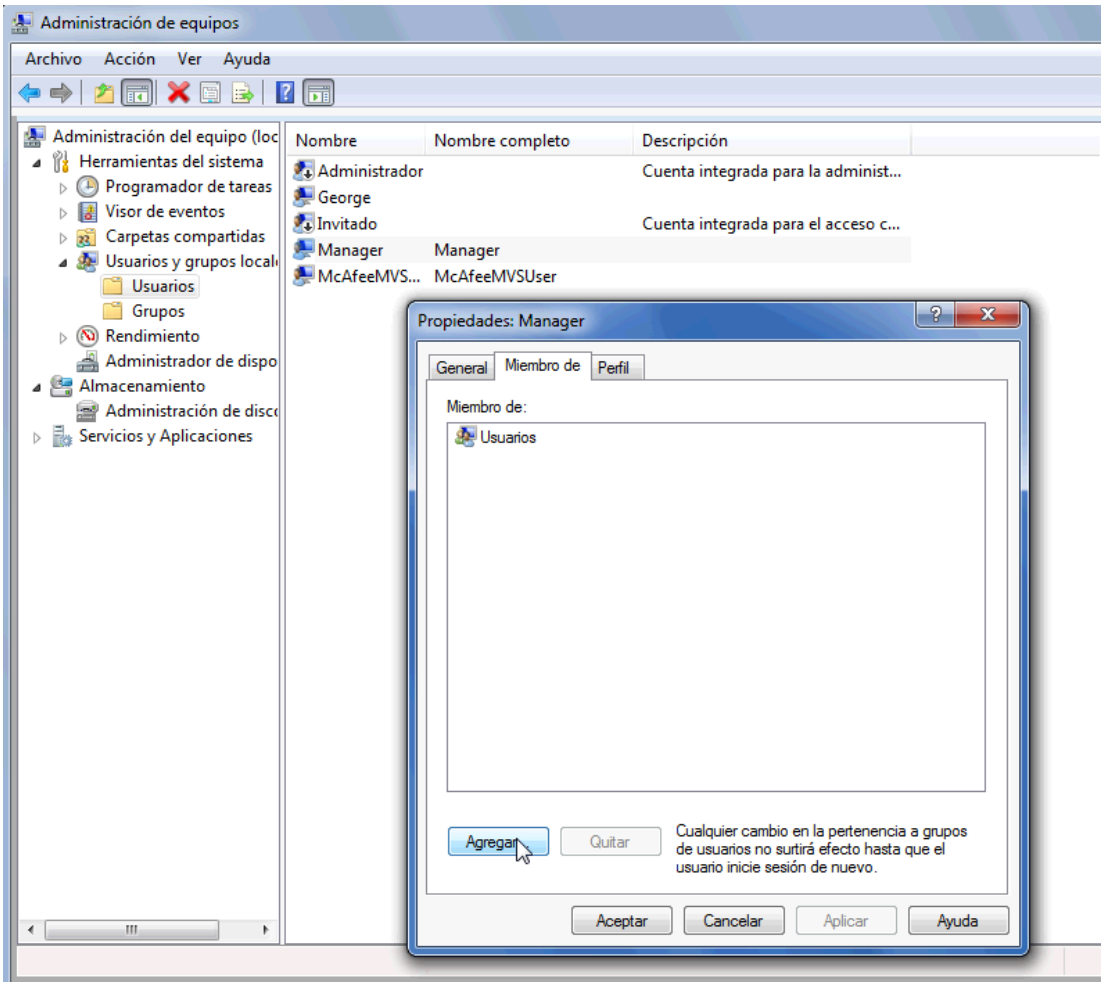
2. Seleccione los dispositivos de hardware que desea restringir y haga clic en el botón **Aplicar** para finalizar el proceso.

3. El siguiente paso a continuación es de seleccionar quién continuará a tener acceso mientras que todos los demás serán bloqueados.

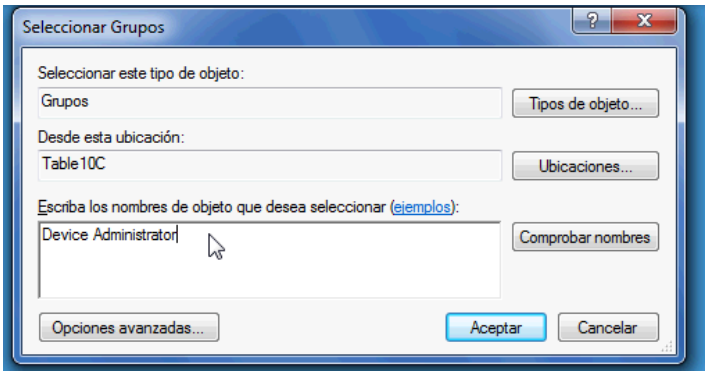
4. Navegue para y seleccione **Equipo**, haga clic con el botón derecho del mouse y seleccione **Administrar** > **Administración de equipos** > **Herramientas del sistema** > **Usuarios y grupos locales** > **Usuarios**.

5. Haga doble clic en el usuario (en este ejemplo “Administrador”) que desea que retenga acceso al hardware bloqueado.

6. En la ficha **Miembro de**, haga clic en el botón **Agregar**.



7. En la ventana **Seleccionar Grupos** puede utilizar la opción **Opciones avanzadas** o sólo escriba el grupo “Administradores de dispositivo”. Haga clic en el botón **Aceptar** y cierre las ventanas haciendo clic en los botones aceptar. Usted debe cerrar la sesión e iniciar sesión nuevamente para obtener los permisos.



Ahora todas las unidades de almacenamiento internas y externas incluyendo unidades de CD, unidades USB, reproductores personales de música, etc. no funcionarán excepto para la(s) persona(s) incluidas en el grupo “Administradores de dispositivo”.

Drive Encryption for HP ProtectTools

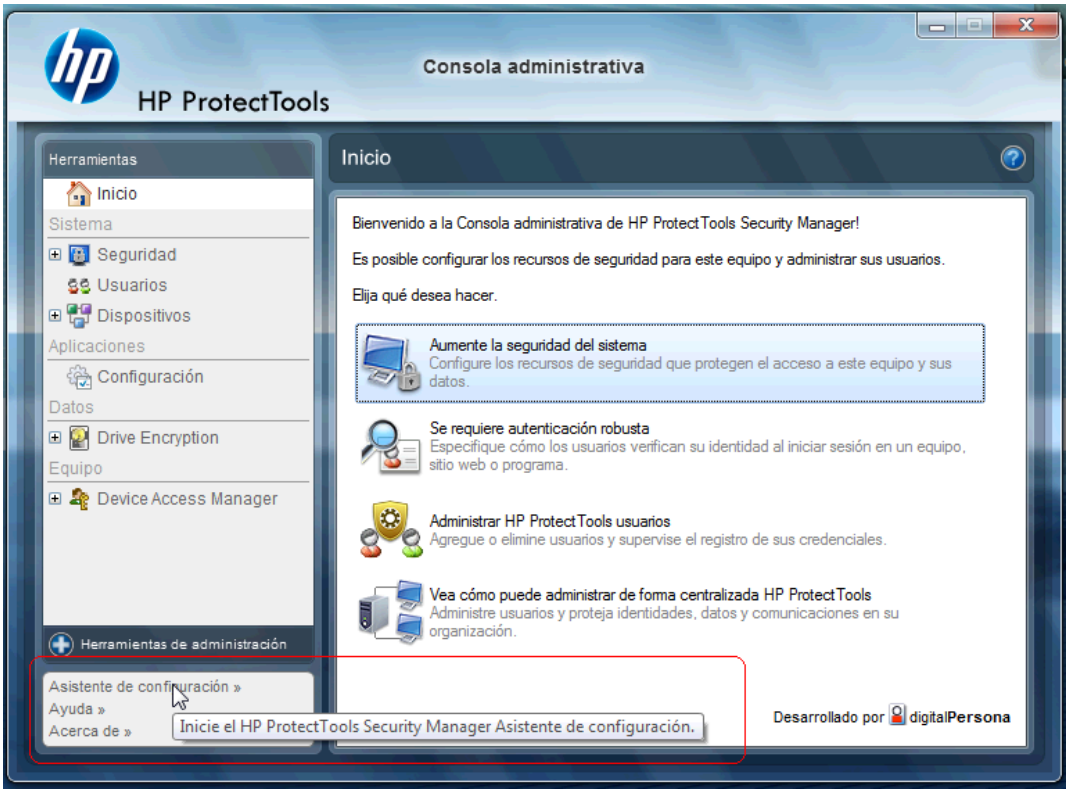
Drive Encryption for HP ProtectTools es un software que se utiliza para proteger sus datos encriptando toda la unidad de disco duro. Los datos en la unidad de disco duro se mantendrán protegidos si su alguna vez roban su PC y/o si extraen la unidad de disco duro del sistema original y la instalan en un sistema diferente.

Un beneficio de seguridad adicional es que Drive Encryption se solicitará autenticación adecuada utilizando su nombre de usuario y contraseña antes que el sistema inicialice. Este proceso se conoce como autenticación de preinicialización.

Para facilitar el proceso, los usuarios de Windows, dominios, Credential Manager for HP ProtectTools, y HP ProtectTools Security Manager todos interactúan con Drive Encryption permitiendo una fácil sincronización de contraseña.

Utilice los siguientes pasos sencillos para activar Drive Encryption for HP ProtectTools.

1. Haga clic en **Inicio** > **Todos los programas** > **HP** > **Consola administrativa de HP ProtectTools** > **Herramientas de administración** > **Asistente de configuración**. Aparece la siguiente pantalla:



2. En la pantalla ¡Bienvenido! seleccione **siguiente**.
3. Se requiere una contraseña de Windows para iniciar el asistente de activación > **Siguiente**.
4. Marque la casilla **Encriptación de unidad** y seleccione **Siguiente**.

5. La ventana de configuración Drive Encryption a continuación exhibe las unidades disponibles que pueden encriptarse y solicitará una unidad flash USB para almacenar la clave de encriptación de recuperación. Mantenga esta clave de recuperación segura y protegida porque se utiliza para recuperar datos o acceder la unidad si se pierde o falla la contraseña de preinicialización.

6. Seleccione **Siguiente**, finalice el proceso, y seleccione **Finalizar**. Cuando se le solicita, extraiga la unidad flash USB y reinicie el sistema cuando esté listo.

7. Cuando el sistema reinicialice en la unidad de disco duro, Drive Encryption solicitará su contraseña de Windows. Ingrese la contraseña y haga clic en **Aceptar**.

NOTA: El equipo puede parecer que está funcionando lentamente mientras la unidad se está encriptando. Una vez que esté totalmente encriptada volverá a un estado normal. A medida que se acceden datos en la unidad, serán encriptados o desencriptados según sea necesario.

Observe también que, la autenticación Drive Encryption “pasará” a través del inicio de sesión de Windows Credential Manager directamente al área de escritorio sin tener que ingresar dos veces su contraseña.

3 Ventajas de HP ProtectTools for Small Business

Acceso al software HP ProtectTools para Seguridad de las Pequeñas Empresas

Para acceder a HP ProtectTools Security Manager desde el menú Inicio de Windows:

- En Windows, haga clic en **Inicio**, luego en **Todos los programas** y, a continuación, en **HP ProtectTools Security Manager**.

Para acceder la Consola administrativa de HP ProtectTools Security Manager desde el menú Inicio de Windows:

- En Windows, haga clic en **Inicio**, luego en **Todos los programas** y, a continuación, en **Consola administrativa de HP ProtectTools**.

Logrando objetivos principales de seguridad

Los módulos HP ProtectTools pueden funcionar juntos suministrando soluciones para una amplia variedad de problemas de seguridad, incluyendo los siguientes objetivos principales de seguridad:

- Restricción de acceso a datos sensibles
- Prevención contra acceso no autorizado desde ubicaciones internas o externas
- Creación de políticas sólidas de contraseña

Restricción de acceso a datos sensibles

Imagine que un auditor está realizando una auditoría en una empresa y se le ha dado acceso a los equipos informáticos para que pueda revisar datos financieros confidenciales. Sin embargo, la empresa no desea que el auditor pueda imprimir archivos ni guardarlos en dispositivos de grabación como un CD. La siguiente característica permite restringir el acceso a los datos:

Device Access Manager for HP ProtectTools permite que administradores restrinjan acceso a dispositivos de grabación para que información confidencial no pueda imprimirse o copiarse desde la unidad de disco duro para una multimedia extraíble. Consulte Configuración de clases de dispositivos (avanzado) en la página 53.

Prevención contra acceso no autorizado desde ubicaciones internas o externas

El acceso no autorizado a un PC de la empresa carente de protección es un riesgo muy tangible para los datos muy importantes, como la información sobre los servicios financieros, el equipo ejecutivo o de I+D e información privada como historiales de pacientes o informes financieros personales. Los siguientes recursos contribuyen a prevenir el acceso no autorizado a la información:

- Recurso de autenticación de pre-inicialización, si está habilitado, ayuda a evitar el acceso al sistema operativo. Consulte los capítulos siguientes:
  - Credential Manager for HP ProtectTools en la página 40
  - Drive Encryption for HP ProtectTools en la página 36
- Credential Manager for HP ProtectTools ayuda a asegurar que un usuario no autorizado no obtenga contraseñas o acceso a aplicaciones protegidas por contraseña. Consulte el capítulo siguiente
  - Credential Manager for HP ProtectTools en la página 40
- Device Access Manager for HP ProtectTools permite que administradores restrinjan acceso a dispositivos de grabación para que información confidencial no pueda copiarse desde la unidad de disco duro para una multimedia extraíble. Consulte el capítulo siguiente
  - Device Access Manager for HP ProtectTools en la página 52
- File Sanitizer permite eliminar los datos de forma segura, eliminando los archivos y las carpetas vitales o realizando una purificación de la unidad de disco duro (sobrescribe datos que ya habían sido eliminados pero que siguen todavía guardados en la unidad de disco duro, para dificultar la recuperación de la información). Consulte el capítulo siguiente:
  - File Sanitizer for HP ProtectTools en la página 45

Creación de políticas sólidas de contraseña

Si usted necesita el uso de una política de contraseñas sólida (una contraseña complicada que es difícil de piratear) para docenas de aplicaciones y bases de datos con base en la web, Credential Manager for HP ProtectTools brinda un práctico depósito protegido para contraseñas e inicio único de sesión. Consulte el capítulo siguiente:

- Credential Manager for HP ProtectTools en la página 40

Elementos adicionales de seguridad

Asignación de funciones de seguridad

Para proteger adecuadamente los datos, una práctica importante es dividir responsabilidades y derechos entre varios tipos de administradores y usuarios.

NOTA: En una pequeña organización o para uso individual, estas funciones pueden ser asumidos por una misma persona.

Para HP ProtectTools for Small Business, los deberes y privilegios de seguridad pueden ser divididos en las siguientes funciones:

- Administrador—Aplica y administra los recursos de seguridad. También puede activar o desactivar algunos recursos.
- Usuario—Utiliza los recursos de seguridad.

Administración de contraseñas de HP ProtectTools

La mayoría de los recursos de HP ProtectTools Security Manager son protegidos por contraseñas. La siguiente tabla enumera las contraseñas más comúnmente utilizadas, el módulo de software donde se define la contraseña y la función de la misma.

Las contraseñas definidas y utilizadas sólo por administradores también aparecen en esta tabla. Todas las otras contraseñas las pueden definir usuarios comunes.

Contraseña de HP ProtectTools	Definida en este módulo de HP ProtectTools	Función
Contraseña de inicio de sesión en Administrador de contraseñas	Administrador de contraseñas	Esta contraseña ofrece dos opciones: • Se puede usar en un inicio de sesión independiente para acceder Administrador de contraseñas después de haber iniciado sesión en Windows. • Se puede usar en lugar del proceso de inicio de sesión en Windows, de forma que permita acceder simultáneamente a Administrador de contraseñas y a Windows.
Contraseña de Computer Setup **NOTA:** También conocida como contraseña de administrador de BIOS, configuración F10 o contraseña de configuración de seguridad	BIOS, por administrador	Protege contra el acceso no autorizado a la utilidad de configuración.
Contraseña de inicio	BIOS	Protege contra el acceso no autorizado al contenido del equipo cuando éste se enciende, se reinicia o sale de la hibernación.
Contraseña de inicio de sesión de Windows.	Panel de control de Windows	Puede utilizarse para realizar inicio de sesión manual.

Creación de una contraseña segura

Para crear contraseñas, primero debe seguir todas las especificaciones definidas por el programa. Sin embargo, considere las siguientes pautas generales para crear contraseñas seguras y reducir las posibilidades de que la contraseña sea comprometida:

- Utilice contraseñas con más de seis caracteres, preferiblemente más de ocho.
- Utilice letras mayúsculas y minúsculas en la contraseña.

- Cuando sea posible, utilice caracteres alfanuméricos e incluya caracteres especiales y signos de puntuación.
- Utilice caracteres especiales o números en lugar de algunas letras en una palabra clave. Por ejemplo, utilice el número 1 en lugar de las letras I o L.
- Combine palabras en dos o más idiomas.
- Divida una palabra o frase con números o caracteres especiales en la mitad de la palabra, por ejemplo, “Mary2-2Cat45.”
- No utilice contraseñas que puedan aparecer en el diccionario.
- No utilice su nombre ni ningún otra información personal como la fecha de nacimiento, el nombre de una mascota o el nombre de soltera de su madre, aunque los escriba al revés.
- Cambie las contraseñas regularmente. Puede cambiar sólo algunos caracteres que incrementen.
- Si anota la contraseña, no la guarde en un lugar muy visible cerca del equipo.
- No guarde la contraseña en un archivo, por ejemplo un correo electrónico, del equipo.
- No comparta cuentas ni le diga a nadie su contraseña.

Copia de seguridad de sus credenciales y configuración

Utilice la herramienta copia de seguridad y restauración en HP ProtectTools Security Manager como una ubicación central desde la cual pueda hacer copias de seguridad y restauración de credenciales de seguridad dese los módulos instalados de HP ProtectTools.

4 Consola administrativa de HP ProtectTools Security Manager

Acerca de la Consola administrativa de HP ProtectTools

Administration of HP ProtectTools Security Manager se suministra a través de Consola administrativa.

Mediante la consola, el administrador local puede:

- Habilitar o deshabilitar recursos de seguridad
- Administrar los usuarios del equipo
- Ajustar los parámetros específicos del dispositivo
- Configurar aplicaciones de Security Manager
- Agregar más aplicaciones de Security Manager

Uso de Consola administrativa

La Consola administrativa de Security Manager es la ubicación central para la administración de HP ProtectTools Security Manager.

Para abrir la consola:

- Seleccione **Inicio** > **Todos los programas** > **Consola administrativa de HP ProtectTools**, o
- Haga clic en el enlace **Administración** que se encuentra en la esquina inferior izquierda de la consola Security Manager.

La Consola administrativa consiste de dos paneles: un panel izquierdo y un panel derecho. El panel izquierdo contiene las herramientas administrativas. El panel derecho contiene el área de trabajo para configurar las herramientas.

El panel izquierdo de Consola administrativa consiste de los siguientes elementos:

- **Inicio** - Proporciona un acceso fácil a las tareas usadas con más frecuencia, entre las que se incluyen la activación de recursos de seguridad, la especificación de credenciales de seguridad y la administración de usuarios.
- **Sistema** - Administra la configuración de los recursos de seguridad, usuarios y dispositivos de autenticación, como lectores de smart card en todo el sistema.

- **Aplicaciones** - Incluye herramientas para configurar el comportamiento de Security Manager y sus aplicaciones.
- **Datos** - Proporciona herramientas para hacer copia de seguridad y recuperación de claves codificadas.
- **Equipo** - Proporciona opciones avanzadas de seguridad para rechazar de forma selectiva varios tipos de dispositivos que puedan poner en peligro la seguridad de esta PC y establecer permisos de acceso para varios usuarios y grupos.
- **Herramientas de administración** - Abre el navegador predeterminado en una página web en la que puede ver herramientas y aplicaciones de administración adicionales que amplían los recursos de Security Manager, además actúa como un medio para mantenerse informado cuando estén disponibles nuevas aplicaciones y actualizaciones.
- **Enlaces** - Proporciona lo siguiente:
  - **Asistente de configuración** - Inicia el asistente de configuración que le guía por el proceso de configuración inicial de Security Manager.
  - **Ayuda** - Abre el archivo de ayuda, que ofrece información sobre Security Manager y sus aplicaciones.
  - **Acerca de** - Exhibe información sobre Security Manager, incluyendo el número de versión y aviso de derechos autorales.

Pasos iniciales con el asistente de configuración

La administración de HP ProtectTools Security Manager requiere privilegios administrativos.

El asistente de configuración de HP ProtectTools Security Manager lo guía a través de la instalación de los recursos de seguridad. Sin embargo, existe un caudal de funcionalidad adicional disponible a través de HP ProtectTools Security Manager Console. Las mismas opciones de configuración encontradas en el asistente así como recursos de seguridad adicionales se pueden configurar en la consola, y se puede acceder a ellos desde el menú Inicio de Windows o desde un enlace dentro de Consola administrativa. Esta configuración se aplica al equipo y a todos los usuarios que compartan el equipo.

La primera vez que inicie sesión en Windows, se le solicitará que configure HP ProtectTools Security Manager. Haga clic en **Aceptar** para iniciar el asistente de configuración de Configuración de Security Manager, que le guiará por los pasos básicos de configuración del programa.

NOTA: También puede iniciar el asistente de seguridad haciendo clic en **Asistente de seguridad** que aparece en la parte inferior del panel izquierdo de Consola administrativa.

Siga las instrucciones que aparecen en la pantalla del asistente de instalación hasta finalizar la configuración.

Si no completa el asistente, se iniciará automáticamente hasta que haga clic en **No volver a mostrar este asistente**.

Para utilizar las aplicaciones de HP ProtectTools Security Manager, inicie HP ProtectTools Security Manager desde el menú **Inicio** o haciendo clic con el botón derecho del mouse en el icono **Security Manager** en el área de notificación de la barra de tareas (bandeja del sistema). La consola de Security Manager y sus aplicaciones están disponibles para todos los usuarios que compartan este equipo.

Configuración del sistema

Se puede acceder al grupo de aplicaciones del **Sistema** desde el menú **Herramientas** en la parte izquierda de Consola administrativa.

Al utilizar las aplicaciones incluidas en este grupo, puede configurar y administrar las políticas y la configuración de este equipo, sus usuarios y dispositivos.

Las siguientes aplicaciones están incluidas en el grupo del sistema.

- **Seguridad** - Administre los recursos de seguridad, políticas de autenticación y otras configuraciones que gobiernan cómo los usuarios autentican cuando hacen inicio de sesión en el equipo o en las aplicaciones de HP ProtectTools.
- **Usuarios** - Configure, administre y registre a los usuarios de este equipo.
- **Dispositivos** - Administre la configuración de los dispositivos de seguridad integrados o conectados al equipo.

Activación de recursos de seguridad

Los recursos de seguridad activados aquí se aplican a todos los usuarios de este equipo.

1. En el panel izquierdo de Consola administrativa, amplíe **Seguridad**, y haga clic en **Recursos**.
2. Para activar un recurso de seguridad, haga clic en la casilla de verificación correspondiente junto a **Política de inicio de sesión de Windows** y/o **Drive Encryption**.
   - **Política de inicio de sesión de Windows** - protege sus cuentas de Windows al solicitarle el uso de credenciales específicas de acceso.
   - **Drive Encryption** - protege sus datos al encriptar la(s) unidad(es) de disco duro, de forma que la información no sea legible por aquellos usuarios que no dispongan de la autorización adecuada.
3. Haga clic en el botón **Siguiente**.
4. Haga clic en el botón **Aplicar**.

Definición de las políticas de autenticación de Security Manager

Las políticas de autenticación de Security Manager para este equipo se definen en dos fichas, inicio de sesión y sesión, que especifica la credenciales necesarias para autenticar cada clase de usuario cuando accede el equipo y las aplicaciones de HP ProtectTools durante una sesión de usuario.

Ficha Inicio de sesión

Para especificar las credenciales necesarias para acceder el equipo e iniciar sesión en Windows:

1. En el panel izquierdo de Consola administrativa, amplíe **Seguridad**, y haga clic en **Autenticación**.
2. En la ficha **Política de inicio de sesión**, seleccione una categoría de usuario de la lista desplegable.
3. En la sección **Política**, especifique las credenciales de autenticación necesarias para la categoría de usuario seleccionada haciendo clic en la casilla o casillas de verificación que están al lado de las credenciales indicadas. Debe especificar al menos una credencial.

4. En la lista desplegable de la sección **Política**, elija si son necesarias ALGUNA (sólo una) de las credenciales especificadas, o si TODAS las credenciales son necesarias para autenticar un usuario.

5. Haga clic en el botón **Aplicar**.

Ficha Política de Sesión

Para definir políticas de administración de credenciales necesarias para autenticar un usuario cuando inicie sesión en las aplicaciones de HP ProtectTools durante una sesión de Windows:

1. En el panel izquierdo de Consola administrativa, amplíe **Seguridad**, y haga clic en **Autenticación**.

2. En la ficha **Política de sesión**, seleccione una categoría de usuario.

3. En la sección **Política**, especifique las credenciales de autenticación necesarias para la categoría de usuario seleccionada haciendo clic en la casilla o casillas de verificación que están al lado de las credenciales indicadas. Debe especificar al menos una credencial.

4. En la lista desplegable de la sección **Política**, elija si son necesarias ALGUNA (sólo una) de las credenciales especificadas, o si TODAS las credenciales son necesarias para autenticar un usuario.

5. Haga clic en el botón **Aplicar**.

Definición de configuración

Puede especificar qué configuración avanzada de seguridad desea permitir. Para editar la configuración:

1. En el panel izquierdo de Consola administrativa, amplíe **Seguridad**, y haga clic en **Configuración**.

2. Haga clic en la casilla de verificación adecuada para activar o desactivar un parámetro de configuración determinado.

3. Haga clic en el botón **Aplicar** para guardar los cambios.

NOTA: La configuración **Permitir inicio de sesión de un paso** permite que los usuarios de este equipo salten inicio de sesión en Windows si la autenticación se realizó a nivel de BIOS.

Administración de usuarios

En la aplicación de usuarios, el administrador de Windows puede administrar los usuarios de este equipo y las políticas que los afectan. Para acceder a la aplicación de usuarios de Consola administrativa, haga clic en **Usuarios**.

Los usuarios de HP ProtectTools son listados y verificados contra las políticas de autenticación definidas a través de Security Manager y contra las credenciales requeridas para cumplir esas políticas.

Para ver las políticas en vigor para un usuario específico, seleccione el usuario de la lista y haga clic en el botón **Ver políticas**.

Para supervisar a los usuarios cuando éstos registran las credenciales, seleccione el usuario de la lista y haga clic en el botón **Registrar**.

Adición de un usuario

Este proceso agrega usuarios a la lista de inicio de sesión. Antes de agregar un usuario, éste debe tener una cuenta de usuario de Windows en el equipo y debe estar presente en el siguiente procedimiento para suministrar una contraseña.

Para agregar un usuario a la lista de usuarios:

1. Haga clic en **Inicio**, luego en **Todos los programas** y, a continuación, en **Consola administrativa de HP ProtectTools**.
2. En el panel izquierdo de Consola administrativa, haga clic en **Usuario**.
3. Haga clic en el botón **Agregar**. Aparece el cuadro de diálogo **Seleccionar usuarios**.
4. Haga clic en el botón **Opciones avanzadas** y, a continuación, en **Buscar ahora** para buscar los usuarios que desea agregar.
5. Haga clic en el usuario que desee agregar a la lista y, a continuación, haga clic en **Aceptar**.
6. Haga clic en **Aceptar** en el cuadro de diálogo **Seleccionar usuarios**.
7. Escriba la contraseña de Windows para la cuenta seleccionada y haga clic en **Finalizar**.

NOTA: Debe utilizar una cuenta de Windows existente y escribirla exactamente igual. No puede modificar ni agregar una cuenta de usuario de Windows desde este cuadro de diálogo.

Eliminación de un usuario

NOTA: Este procedimiento no borra la cuenta de usuario de Windows. Solo elimina la cuenta de Security Manager. Para eliminar el usuario por completo, es necesario eliminarlo de Security Manager y de Windows.

1. Haga clic en **Inicio**, luego en **Todos los programas** y, a continuación, en **Consola administrativa de HP ProtectTools**.
2. En el panel izquierdo de Consola administrativa, haga clic en **Usuario**.
3. Haga clic en el nombre del usuario para la cuenta que desea eliminar y, a continuación, haga clic en **Eliminar**.
4. En el cuadro de diálogo de confirmación, haga clic en el botón **Sí**.

Comprobación de estado de un usuario

La sección usuario de Consola administrativa muestra el estado actual de cada usuario:

- **Marca de verificación verde** - Indica que el usuario ha configurado el(los) método(s) de seguridad de inicio de sesión requerido.
- **X rojo** - Indica que el usuario no ha configurado un método de seguridad de inicio de sesión requerido y será bloqueado del equipo cuando intente iniciar sesión. El usuario debe ejecutar el asistente de configuración para definir el(los) método(s) de inicio de sesión requerido.
- **Vacío** - Indica que no requiere un método de seguridad de inicio de sesión.

Configuración de parámetros de las aplicaciones

La ventana configuración incluye herramientas para configurar el comportamiento de Security Manager y sus aplicaciones. Para modificar la configuración:

1. Haga clic en **Inicio**, luego en **Todos los programas** y, a continuación, en **Consola administrativa de HP ProtectTools**.
2. En el panel izquierdo de Consola administrativa, haga clic en **Configuración**.
3. En la ficha **General**, elija la configuración general para HP ProtectTools Security Manager, a continuación haga clic en el botón **Aplicar**.
4. En la ficha **Aplicaciones**, seleccione las aplicaciones que desee activar o desactivar y, a continuación, haga clic en el botón **Aplicar**.

NOTA: La activación o desactivación de una aplicación puede que no tenga efecto si se reinicia el equipo.

Encriptado de unidades

Drive Encryption for HP ProtectTools le permite encriptar las unidades de disco duro del equipo, haciéndolas ilegibles e inaccesibles a cualquier persona que no esté autorizada que intente accederla incluso si la unidad se ha extraído del equipo o se ha enviado a un servicio de recuperación de datos.

Para activar o desactivar Drive Encryption, haga clic en el asistente de configuración de la consola administrativa.

△ **PRECAUCIÓN:** Es importante que haga una copia de seguridad de las claves de encriptación en una unidad flash USB y guarde el dispositivo en un lugar seguro. Si olvida su contraseña, este dispositivo le brinda el único acceso a la unidad de disco duro.

Para obtener más información sobre el uso de Drive Encryption for HP ProtectTools, consulte Drive Encryption for HP ProtectTools en la página 36.

Administración de Device Access

Device Access Manager for HP ProtectTools proporciona opciones avanzadas de seguridad para rechazar selectivamente varios tipos de dispositivos que pueden comprometer la seguridad de su PC. Para obtener más información acerca del uso de Device Access Manager for HP ProtectTools, consulte Device Access Manager for HP ProtectTools en la página 52.

5 HP ProtectTools Security Manager

HP ProtectTools Security Manager le permite aumentar significativamente la seguridad de su equipo. Mediante el uso de las aplicaciones de Security Manager, puede:

- Administrar el inicio de inicio de sesión y sus contraseñas
- Cambiar fácilmente la contraseña de Windows
- Configurar credenciales de autenticación, incluyendo smart card
- Triturar o purificar la unidad de disco duro
- Ver el estado de encriptaciones de unidades
- Visualizar la configuración de Device Access
- Hacer copia de seguridad y restaurar los datos de Security Manager

Administración de contraseñas

Credential Manager for HP ProtectTools crea y administra inicios de sesión, que le permite ejecutar y hacer inicio de sesión en sitios web y programas mediante la autenticación de sus credenciales autenticadas.

Para obtener más información sobre la administración de contraseñas, consulte Credential Manager for HP ProtectTools en la página 40.

Configuración de credenciales

Puede utilizar las credenciales de Security Manager para verificar su identidad. El administrador de este equipo puede configurar cuales credenciales pueden utilizarse para probar su identidad cuando inicie sesión en su cuenta de Windows, sitios web o programas.

Las credenciales disponibles pueden variar en función del dispositivo de seguridad integrado o conectado al equipo. Cada credencial admitida tendrá una entrada en el grupo de credenciales.

Cambio de la contraseña de Windows

Security Manager hace el cambio de la contraseña de Windows más simple y más rápido que si lo hace mediante el panel de control de Windows.

Para cambiar su contraseña de Windows:

1. En HP ProtectTools Security Manager, haga clic en la opción **Credenciales** del panel izquierdo.
2. Haga clic en **Contraseña de Windows**.
3. Escriba la contraseña actual en el cuadro **Contraseña actual de Windows**.
4. Escriba la nueva contraseña en los cuadros **Contraseña de Windows nueva** y **Confirmar nueva contraseña**.
5. Haga clic en **Cambiar**.

Trituración o purificación de archivos

File Sanitizer for HP ProtectTools elimina archivos al sobrescribirlos con datos insignificantes. Este proceso, denominado como “trituración”, mejora en gran medida la seguridad de la información, tornando los archivos eliminados difíciles de recuperar. File Sanitizer mejora la seguridad de la información al sobrescribir el espacio utilizado anteriormente en la unidad de disco duro mediante un proceso conocido como “purificación”. Los archivos eliminados mediante File Sanitizer no se pueden recuperar mediante el sistema operativo u otro software de recuperación de archivos que esté comúnmente disponible.

Para obtener más información acerca del uso de File Sanitizer for HP ProtectTools, consulte File Sanitizer for HP ProtectTools en la página 45.

Visualización de estado de encriptación de unidad

El administrador de Windows configura Drive Encryption en la Consola administrativa. Los usuarios pueden visualizar el estado de la encriptaciones en Security Manager.

Para ver el estado de encriptación de la unidad:

1. Haga clic en **Inicio**, luego en **Todos los programas** y, a continuación, en **HP ProtectTools Security Manager**.
2. En el panel izquierdo de Security Manager, haga clic en **Estado encriptación**. La página estado de encriptación muestra si la encriptación de la unidad está activa o inactiva y cuáles unidades están encriptadas y cuáles no.

Visualización de device access

El administrador de Windows configura Device Access en Consola administrativa. Los usuarios pueden visualizar la configuración de device access en Security Manager.

Para ver la configuración de device access:

1. Haga clic en **Inicio**, luego en **Todos los programas** y, a continuación, en **HP ProtectTools Security Manager**.
2. En el panel izquierdo de Security Manager, amplíe **Device Access Manager**.
3. Para ver qué dispositivos tienen el acceso denegado, haga clic en **Configuración sencilla**. Los dispositivos con una marca de verificación al lado tienen el acceso denegado.

4. Para ver qué usuarios o grupos tienen el acceso denegado, haga clic en **Configuración de clases de dispositivo**.

5. Haga clic en un dispositivo para ver qué usuarios o grupos tienen el acceso denegado o permitido a un dispositivo.

Adición de aplicaciones

Pueden estar disponibles aplicaciones adicionales para agregar nuevos recursos a este programa.

1. Haga clic en **Inicio**, luego en **Todos los programas** y, a continuación, en **HP ProtectTools Security Manager**.

2. En el panel izquierdo de Security Manager, haga clic en la opción **Descubrir más**.

NOTA: Si no existe ningún enlace **Descubrir más**, es porque el administrador del equipo lo desactivó.

3. En la ficha **Agregar aplicaciones**, navegue para buscar aplicaciones adicionales.

4. En la ficha **Actualizaciones y mensajes**, puede mantenerse informado sobre las nuevas aplicaciones y actualizaciones haciendo clic en la casilla de verificación **Mantenerme informado sobre nuevas aplicaciones y actualizaciones** y estableciendo un número de días para comprobar si existen actualizaciones, o también puede hacer clic en el botón **Comprobar ahora** para comprobar inmediatamente si existen actualizaciones.

Configuración de preferencias

La página preferencias le permite seleccionar la casilla de verificación **Mostrar icono en la barra de tareas** para visualizar el icono de Security Manager en el área de notificaciones de la barra de tareas (bandeja del sistema).

Para acceder a la página preferencias:

1. Haga clic en **Inicio**, luego en **Todos los programas** y, a continuación, en **HP ProtectTools Security Manager**.

2. En el panel izquierdo de Security Manager, haga clic en **Opciones avanzadas** y, a continuación, en **Preferencias**.

3. Marque o desmarque la casilla de verificación **Mostrar icono en la barra de tareas** y haga clic en **Aplicar**.

Copia de seguridad y restauración

Es una buena costumbre realizar una copia de seguridad de los datos de Security Manager de forma regular. La frecuencia con la que realice la copia de seguridad depende de la frecuencia con la que modifique los datos. Por ejemplo, si normalmente agrega nuevos inicios de sesión todos los días, probablemente debería realizar la copia de seguridad de sus datos a diario.

Las copias de seguridad también pueden utilizarse para migrar de un equipo a otro, este proceso también se conoce como importación y exportación. No obstante, recuerde que con este recurso sólo se realiza la copia de seguridad de los datos.

Su restaura el archivo de copia de seguridad para otro equipo, o al mismo equipo después de reinstalar el sistema operativo, HP ProtectTools Security Manager debe instalarse en el sistema antes de restaurar los datos desde el archivo de copia de seguridad.

Copias de seguridad de sus datos

Cuando realiza la copia de seguridad de sus datos, está guardando los inicios de sesión y la información de credenciales en un archivo codificado, protegido por la contraseña que introduzca.

Para realizar la copia de seguridad de sus datos:

1. Haga clic en **Inicio**, luego en **Todos los programas** y, a continuación, en **HP ProtectTools Security Manager**.
2. En el panel izquierdo de Security Manager, haga clic en **Opciones avanzadas** y, a continuación, en **Copia de seguridad y restauración**.
3. Haga clic en **Copia de seguridad de datos**.
4. Seleccione los módulos que desea incluir en la copia de seguridad. En la mayor parte de los casos, deseará seleccionar todos. Haga clic en **Siguiente**.
5. Introduzca la contraseña para verificar su identidad y, a continuación, haga clic en el botón de flecha.
6. Introduzca una ruta y nombre para el archivo de almacenamiento. De forma predeterminada, el archivo se guarda en la carpeta documentos. Haga clic en **Examinar** para especificar una ubicación diferente. Haga clic en **Siguiente**.
7. Ingrese y confirme una contraseña para proteger el archivo.
8. Haga clic en **Finalizar**.

Restauración de sus datos

Puede restaurar los datos a partir de un archivo codificado protegido con contraseña que se haya creado previamente con el recurso de copia de seguridad y restauración de Security Manager.

Para restaurar sus datos:

1. Haga clic en **Inicio**, luego en **Todos los programas** y, a continuación, en **HP ProtectTools Security Manager**.
2. En el panel izquierdo de Security Manager, haga clic en **Opciones avanzadas** y, a continuación, en **Copia de seguridad y restauración**.
3. Haga clic en **Restaurar datos**.
4. Ingrese una ruta y nombre para el archivo de almacenamiento o haga clic en **Examinar** y seleccione el archivo.
5. Ingrese la contraseña utilizada para proteger el archivo y haga clic en **Siguiente**.
6. Seleccione los módulos cuyos datos desea restaurar. En la mayor parte de los casos, serán todos los módulos de la lista. Haga clic en **Siguiente**.
7. Haga clic en **Finalizar**.

Cambio de la imagen y del nombre de usuario de Windows

En la esquina superior izquierda de Security Manager, aparece la imagen y el nombre de usuario de Windows.

Para cambiar la imagen y/o el nombre de usuario:

1. Haga clic en la sección superior izquierda de Security Manager que contiene el nombre de usuario y la imagen.
2. Para cambiar el nombre de usuario, escriba un nombre en el cuadro **Nombre de usuario de Windows**.
3. Para cambiar la imagen, haga clic en el botón **Elegir imagen** y examine para seleccionar una imagen.
4. Haga clic en el botón **Guardar** para guardar los cambios.

6 Drive Encryption for HP ProtectTools

NOTA: Drive Encryption for HP ProtectTools está disponible sólo en algunos modelos.

En el mundo actual, pueden robar un equipo suyo o de alguno de sus empleados y puede quedar expuesta información vital sobre su empresa, que puede comprometerlo seriamente. La encriptación de toda la unidad de disco duro del equipo torna la unidad ilegible e inaccesible a cualquier persona no autorizada que intente accederla, aún cuando la unidad se extrae de su equipo o se envíe a un servicio de recuperación de datos.

El software Drive Encryption for HP ProtectTools brinda protección completa de datos al encriptar la unidad de disco duro. Cuando Drive Encryption está activado, debe iniciar sesión en la pantalla de inicio de sesión de Drive Encryption, que se muestra antes de que se inicie Windows.

Drive Encryption no evita acceso no autorizado durante la misma sesión de Windows. Una vez que se inicializa la PC y usted ingresa su nombre de usuario y la contraseña, los datos en la unidad de disco duro están aún encriptados, pero están disponibles para cualquier usuario en el sistema. Asegúrese de proteger con contraseña su sesión de Windows cuando esté alejado de su equipo.

NOTA: Drive Encryption for HP ProtectTools sólo se puede activar en el asistente de configuración de la consola administrativa de HP ProtectTools.

NOTA: Drive Encryption no se admite en sistemas operativos de 64 bits cuando esté configurado con RAID en sistemas que utilicen un procesador AMD.

NOTA: Drive Encryption no admite la prevención de Dictionary Attack.

Drive Encryption:

- Permite encriptar todo en las unidades de disco duro internas.
- Proporciona acceso por contraseña y autenticación de preinicialización fáciles.
- Es compatible con Microsoft Windows XP, Windows Vista y Windows 7.

En Drive Encryption for HP ProtectTools se pueden llevar a cabo varias tareas:

- Administración de Drive Encryption
  - Encriptación o desencriptación de unidades individuales
- Copia de seguridad y restauración
  - Creación de claves de copia de seguridad
  - Realización de una restauración

△ **PRECAUCIÓN:** Es importante que haga una copia de seguridad de las claves de encriptación en una unidad flash USB y la guarde en un lugar seguro. Si olvida su contraseña, este dispositivo le brinda el único acceso a la unidad de disco duro.

PRECAUCIÓN: Si decide desinstalar el módulo Drive Encryption o si utiliza una solución de copia de seguridad y restauración, debe primero desencriptar todas las unidades encriptadas. Si no lo hace, no podrá acceder los datos en las unidades encriptadas. La reinstalación del módulo Drive Encryption no le permitirá acceder las unidades encriptadas.

Procedimientos de configuración

Apertura de Drive Encryption

1. Haga clic en **Inicio**, luego haga clic en **Todos los programas** y, a continuación, haga clic en **Consola administrativa de HP ProtectTools**.
2. Haga clic en **Drive Encryption**.

Tareas generales

Activación de Drive Encryption

Use el asistente de configuración de la consola administrativa de HP ProtectTools para activar Drive Encryption.

Desactivación de Drive Encryption

Use el asistente de configuración de la consola administrativa de HP ProtectTools para desactivar Drive Encryption.

Inicio de sesión después de activar Drive Encryption

Cuando inicializa el equipo después de activar Drive Encryption y realiza el registro de su cuenta, debe iniciar sesión en la pantalla de inicio de sesión de Drive Encryption:

NOTA: Si el administrador de Windows ha activado el recurso de seguridad de preinicialización en la consola administrativa de HP ProtectTools, podrá iniciar sesión en el equipo inmediatamente después de encender el equipo; es decir, no desde la pantalla de inicio de sesión de Drive Encryption.

NOTA: Si utiliza una clave de restauración en la pantalla de inicio de sesión de Drive Encryption, se le solicitará que seleccione su nombre de usuario en Windows y que escriba su contraseña en la pantalla de inicio de sesión de Windows.

Tareas avanzadas

Administración de Drive Encryption (tarea de administrador)

La ventana de Drive Encryption permite que los administradores de Windows vean y cambien el estado de Drive Encryption (activo o inactivo) y vean el estado de encriptación de todos las unidades de disco duro del equipo.

Encriptado o desencriptado de unidades individuales

1. En el panel izquierdo de la consola administrativa, amplíe **Drive Encryption**, y haga clic en **Administración de encriptado**.
2. Haga clic en el botón **Cambiar encriptación**.
3. En la casilla de diálogo Cambiar encriptación, seleccione o desmarque la casilla de verificación junto a cada unidad de disco duro que desea encriptar o desencriptar, y, a continuación, haga clic en **Aceptar**.

NOTA: Cuando se está realizando la encriptación o desencriptación de una unidad, la barra de progreso muestra el tiempo restante para completar el proceso durante la sesión actual. Si se apaga o se inicia la suspensión o hibernación del equipo durante el proceso de encriptación y luego se reinicia, la pantalla de tiempo restante restablece en el comienzo, pero la encriptación actual reanuda donde se interrumpió. La pantalla de tiempo restante y progreso cambiará más rápidamente para reflejar el progreso anterior.

Copia de seguridad y restauración (tarea de administrador)

Drive Encryption: La ventana Copia de seguridad y restauración permite que los administradores de Windows hagan copias de seguridad y recuperen las claves de encriptación.

Creación de claves de copia de seguridad

PRECAUCIÓN: Asegúrese de mantener el dispositivo de almacenamiento que contenga la clave de copia de seguridad en un lugar seguro, porque si olvida su contraseña, este dispositivo le brindará el único acceso a la unidad de disco duro.

1. En el panel izquierdo de la consola administrativa, amplíe **Drive Encryption**, y haga clic en **Copia de seguridad y restauración**.
2. Haga clic en el botón **Copia de seguridad de las claves**.
3. En la página “Seleccionar disco de copia de seguridad”, haga clic en el nombre donde desea hacer copia de seguridad de la clave de encriptación, y, a continuación, haga clic en **Siguiente**.
4. Lea la información que aparece en la página siguiente, y luego haga clic en **Siguiente**.

   La clave de encriptación se guarda en el dispositivo de almacenamiento que seleccionó.
5. Haga clic en **Aceptar** cuando abra la casilla de diálogo de confirmación.

NOTA: Consulte el archivo de ayuda de Drive Encryption for HP ProtectTools para obtener más información sobre la administración y ejecución de una restauración.

7 Credential Manager for HP ProtectTools

Inicio de sesión en Windows, sitios web y programas es más fácil y más seguro mediante el uso de Administrador de contraseñas.

Administrador de contraseñas le permite configurar las pantallas de inicio de sesión de sitios web y programas para obtener un acceso más rápido y seguro. Primero, Administrador de contraseñas aprende sobre sus inicios de sesión y los datos específicos a medida que escribe en las casillas de ingreso de cada pantalla de inicio de sesión. A continuación, cuando está en una pantalla de inicio de sesión, después de verificar su identidad, Administrador de contraseñas completa y envía los datos automáticamente.

Para obtener acceso aún más rápido, puede exhibir un menú de sus inicios de sesión simplemente utilizando una combinación configurable de tecla de acceso rápido (Ctrl+Windows+H es la predeterminada). En el menú, simplemente seleccione un inicio de sesión, y Administrador de contraseñas iniciará el sitio web o programa, navegará a la pantalla de inicio de sesión e iniciará sesión automáticamente.

Para verificar su identidad debe utilizar sus credenciales de HP ProtectTools for Small Business, como su contraseña de Windows. Esto significa que tendrá que utilizar las mismas credenciales para iniciar sesión en todas las pantallas de inicio de sesión que haya configurado. Por lo tanto, puede crear contraseñas más seguras que no tiene que anotar ni recordar y, de este modo, sus cuentas también estarán más seguras.

Administrador de contraseñas le permite ver rápidamente si alguna de sus contraseñas no es segura y puede generar automáticamente una contraseña compleja y segura para utilizar en nuevos sitios.

Con Administrador de contraseñas puede ver sus inicios de sesión y contraseñas, y editarlas a cualquier momento. También se puede acceder a muchos recursos de Administrador de contraseñas desde el icono de Administrador de contraseñas que aparece cuando se encuentra en la pantalla de inicio de sesión de un programa que se ha configurado o en la pantalla de inicio de sesión de cualquier sitio web. Si hace clic en el icono, se muestra un menú contextual en el que puede seleccionar entre las siguientes opciones.

Para las páginas web o programas donde no se ha creado un inicio de sesión:

Las siguientes opciones se muestran en el menú contextual:

- Agregar [algúndominio.com] a Administrador de contraseñas - Se utiliza para agregar un inicio de sesión para la pantalla de inicio de sesión actual.
- Abrir Administrador de contraseñas - Inicia Security Manager en la página de Administrador de contraseñas.

- Configuración del icono de Administrador de contraseñas - Le permite especificar las condiciones bajo las que se muestra el icono de Administrador de contraseñas.
- Ayuda - Muestra ayuda en línea para la aplicación de Administrador de contraseñas.

Para las páginas web o programas donde ya se ha creado un inicio de sesión:

Las siguientes opciones se muestran en el menú contextual:

- Completar datos de inicio de sesión - Coloca los datos de inicio de sesión en los campos de inicio de sesión y, a continuación, envía la página (si el envío se especificó cuando se creó o editó por última vez el inicio de sesión).
- Editar inicio de sesión - Le permite editar los datos de inicio de sesión para este sitio web.
- Agregar inicio de sesión - Se utiliza para agregar otro inicio de sesión para el mismo sitio web o programa.
- Abrir Administrador de contraseñas - Inicia el panel de Security Manager en la página de Administrador de contraseñas.
- Ayuda - Muestra ayuda en línea para la aplicación de Administrador de contraseñas.

Adición de inicios de sesión

Para agregar un inicio de sesión:

1. Abra la pantalla de inicio de sesión para un sitio web o programa.
2. Haga clic en la fecha del icono de Administrador de contraseñas y, a continuación, seleccione una de las opciones siguientes, en función de si la pantalla de inicio de sesión es de un sitio web o de un programa.
    - Para un sitio web - seleccione **Agregar [nombre de dominio] a Administrador de contraseñas**.
    - Para un programa - seleccione **Agregar esta pantalla de inicio de sesión a Administrador de contraseñas**.
3. Ingrese sus datos de inicio de sesión. Los campos de inicio de sesión en pantalla y sus campos correspondientes en el cuadro de diálogo se identifican con un borde anaranjado en negrita. Están disponibles otras opciones para mostrar este cuadro de diálogo, como la selección de la opción agregar inicio de sesión en la ficha **Administrar** de Administrador de contraseñas. Algunas opciones dependen de los dispositivos de seguridad conectados al equipo; por ejemplo, la utilización de la combinación de teclas de acceso directo Ctrl-H o la inserción de una smart card.
    - Haga clic en las flechas que están a la derecha del campo de inicio de sesión para completarlo con una de las varias opciones preformatadas.
    - También puede hacer clic en **Elegir otros campos** para agregar más campos de la pantalla al inicio de sesión.

- Desmarque la selección **Enviar datos de inicio de sesión** si desea que los campos de inicio de sesión se completen pero no desea enviarlos.
- Si desea ver la contraseña para este inicio de sesión, haga clic en **Mostrar contraseña**.

4. Haga clic en **Aceptar**. El símbolo más desaparece del icono de Administrador de contraseñas, lo que le indica que se ha creado el inicio de sesión.

Ahora, cada vez que vaya a ese sitio web o inicie ese programa, aparecerá el icono de Administrador de contraseñas, lo que le indica que puede utilizar la(s) credencial(es) registrada(s) para iniciar sesión.

Edición de inicios de sesión

Para editar un inicio de sesión:

1. Abra la pantalla de inicio de sesión para un sitio web o programa.
2. Haga clic en la flecha del icono Administrador de contraseñas y seleccione **Editar inicio de sesión** para mostrar un cuadro de diálogo en el que pueda editar la información de inicio de sesión. Los campos de inicio de sesión de la pantalla y los campos correspondientes del cuadro de diálogo se identifican con un borde anaranjado en negrita.
3. Edite la información de inicio de sesión.
   - Haga clic en las flechas que están a la derecha del campo de inicio de sesión para completarlo con una de las varias opciones preformatadas.
   - También puede hacer clic en **Elegir otros campos** para agregar más campos de la pantalla al inicio de sesión.
   - Desmarque la selección **Enviar datos de cuenta** si desea que los campos de inicio de sesión se completen pero no desea enviarlos.
   - Si desea ver la contraseña para este inicio de sesión, haga clic en Mostrar contraseña.
4. Haga clic en **Aceptar**.

Uso del menú inicios de sesión

Administrador de contraseñas ofrece un modo rápido y fácil de iniciar los sitios web y los programas para los que ha creado inicios de sesión. Sólo tiene que hacer doble clic en el inicio de sesión de un programa o sitio web del menú inicios de sesión o en la ficha **Administrar** de Administrador de contraseñas, y se abrirá la pantalla de inicio de sesión y se completarán los datos de inicio de sesión. De manera predeterminada, la información también se envía de forma inmediata al sitio web; sin embargo, puede elegir no hacerlo si desmarca la selección **Enviar datos de cuenta** cuando configura o edita el inicio de sesión por primera vez.

Cuando crea un inicio de sesión, éste se agrega automáticamente al menú inicios de sesión de Administrador de contraseñas.

Para mostrar el menú inicios de sesión, presione la combinación de teclas de acceso directo de Administrador de contraseñas. Ctrl-H es la predeterminada, pero puede cambiar la combinación de teclas de acceso directo desde **Administrador de contraseñas** > **Configuración**.

Organización de inicios de sesión en categorías

Utilice las categorías para guardar los inicios de sesión en orden. Es una tarea simple la creación de una o más categorías; y arrastrar y soltar los inicios de sesión a las categorías que desee.

Para agregar una categoría:

1. En el panel izquierdo de Security Manager, seleccione **Administrador de contraseñas**.
2. Seleccione la ficha **Administrar** y haga clic en **Agregar categoría**.
3. Ingrese un nombre para la categoría.
4. Haga clic en **Aceptar**.

Para agregar un inicio de sesión a una categoría:

1. Coloque el puntero del mouse sobre el inicio de sesión que desee.
2. Mantenga presionado el botón izquierdo del mouse.
3. Arrastre el inicio de sesión en la lista de categorías. Las categorías se resaltarán a medida que mueva el mouse sobre ellas.
4. Suelte el botón del mouse cuando desee seleccionar la categoría que está resaltada.

Sus inicios de sesión no se mueven a la categoría, sino que sólo se copian a la categoría seleccionada. Esto significa que puede agregar el mismo inicio de sesión a más de una categoría. Y siempre podrá ver toda la información sobre el inicio de sesión si hace clic en **Todo**.

Administración de inicios de sesión

Administrador de contraseñas hace que la administración de la información de inicio de sesión (nombres de usuario, contraseñas y varias cuentas de inicio de sesión) sea más sencilla e intuitiva, y se pueda realizar desde una ubicación central.

Sus inicios de sesión se muestran en la ficha **Administrar**. Cuando se han creado varios inicios de sesión para un mismo sitio web, cada inicio de sesión aparece debajo del nombre del sitio web y se incluye en la lista de inicio de sesión.

Para administrar los inicios de sesión:

En el panel izquierdo de Security Manager, seleccione **Administrador de contraseñas** y haga clic en la ficha **Administrar**.

- Adición de un inicio de sesión - Haga clic en **Agregar inicio de sesión** y siga las instrucciones que aparecen en pantalla.
- Edición de un inicio de sesión - Seleccione un inicio de sesión y haga clic en **Editar**. A continuación, cambie los datos de inicio de sesión según desee.
- Eliminación de un inicio de sesión - Seleccione un inicio de sesión y haga clic en **Eliminar**.

Para agregar otro inicio de sesión para un sitio web o programa:

1. Inicie la pantalla de inicio de sesión para un sitio web o programa.
2. Haga clic en el icono de Administrador de contraseñas para mostrar el menú de accesos directos.
3. Seleccione **Agregar inicio de sesión adicional** y siga las instrucciones que aparecen en pantalla.

Acceso a seguridad de la contraseña

El uso de contraseñas sólidas para iniciar sesión en sitios web y programas es un aspecto importante para proteger su identidad.

Administrador de contraseñas hace fácil monitorear y mejorar la seguridad mediante un análisis instantáneo y automático la seguridad de cada contraseña utilizada para iniciar sesión en sitios web y programas. Puede comprobar la seguridad de las contraseñas que utiliza para iniciar sesión en la ficha **Solidez de la contraseña** de Administrador de contraseñas.

Configuración del icono de Administrador de contraseñas

Administrador de contraseñas intenta identificar las pantallas de inicio de sesión para sitios web y programas. Cuando encuentra una pantalla de inicio de sesión para la que no se ha creado un inicio de sesión, Administrador de contraseñas le ofrecerá la opción de agregar un inicio de sesión para la pantalla mediante la visualización del icono de Administrador de contraseñas con un símbolo “+”.

Los siguientes parámetros son configurables:

- Preguntar siempre - Seleccione esta opción para que Administrador de contraseñas le pregunte si desea agregar un inicio de sesión siempre que se visualice una pantalla de inicio de sesión para la que no se haya configurado todavía un inicio de sesión.
- No preguntar para esta pantalla - Seleccione esta opción para que Administrador de contraseñas no le vuelva a preguntar si desea agregar un inicio de sesión para esta pantalla de inicio de sesión específica.
- No preguntar nunca - Seleccione esta opción para asegurarse de que Administrador de contraseñas nunca le haga esta pregunta para las pantallas de inicio de sesión que no se hayan configurado.

8 File Sanitizer for HP ProtectTools

File Sanitizer es una herramienta que permite eliminar archivos y carpetas críticos (información o archivos personales, datos de historiales o relacionados con la web y otros componentes de datos) del equipo de forma segura y que periódicamente realiza una purificación de la unidad de disco duro.

NOTA: File Sanitizer actualmente funciona sólo en la unidad de disco duro.

Acerca de trituración

La eliminación de archivos y/o carpetas en Windows, no elimina completamente el contenido de su unidad de disco duro. Windows sólo elimina la referencia. Los datos aún permanecen en la unidad de disco duro hasta que otro archivo sobrescribe esa misma área en la unidad de disco duro con nueva información.

Trituración es diferente que la eliminación estándar de Windows (también conocida como una eliminación simple en File Sanitizer) porque cuando tritura datos es virtualmente imposible recuperar esos datos.

Cuando seleccione un perfil de trituración (seguridad máxima, seguridad mediana, o seguridad baja), una lista de archivos y/o carpetas predefinidos y un método de borrado son automáticamente seleccionados para trituración. También puede personalizar un perfil de trituración, que le permite especificar el número de ciclos de trituración, cuales archivos incluir para trituración, cuales archivos confirmar antes de trituración, y cuales archivos excluir antes de trituración.

Puede definir una programación automática de trituración, y también puede triturar archivos y/o carpetas de forma manual cuando lo desee.

Acerca de purificación del espacio libre

La purificación de espacio libre le permite grabar con seguridad datos aleatorios sobre archivos eliminados, evitando que usuarios puedan visualizar el contenido original del archivo eliminado.

NOTA: Purificación de espacio libre es para aquellos archivos que usted eliminó utilizando la papelera de reciclaje de Windows o cuando eliminó un archivo de forma manual. Purificación de espacio libre no proporciona seguridad adicional a archivos triturados.

Puede definir una programación automática de purificación de espacio libre o puede activar de forma manual la purificación de espacio libre mediante el icono HP ProtectTools en el área de notificación, en el extremo derecho de la barra de tareas.

Procedimientos de configuración

Apertura de File Sanitizer

Para abrir File Sanitizer:

1. Haga clic en **Inicio**, luego en **Todos los programas** y, a continuación, en **HP ProtectTools Security Manager**.
2. En el panel izquierdo de Security Manager, haga clic en **File Sanitizer**.

   – o –

- Haga doble clic en el icono **File Sanitizer**.

  – o –

- Haga clic con el botón derecho del mouse en el icono HP ProtectTools del área de notificación situada en el extremo derecho de la barra de tareas, resalte **File Sanitizer** y, a continuación, haga clic en **Abrir File Sanitizer**.

Configuración de la programación de purificación del espacio libre

Para definir una programación de purificación del espacio libre:

1. En el panel izquierdo de Security Manager, amplíe **File Sanitizer** y haga clic en **Purificación de espacio libre**.
2. Seleccione la casilla de verificación **Activar programador**, ingrese su contraseña de Windows, y a continuación, ingrese el día y la hora para purificar la unidad de disco duro.
3. Haga clic en el icono **Guardar**.

NOTA: La operación de purificación de espacio libre puede llevar mucho tiempo. Aunque la operación de purificación de espacio libre se ejecuta en segundo plano, su equipo puede ejecutar despacio debido al aumento de uso del procesador.

Configuración de una programación de trituración

1. En el panel izquierdo de Security Manager, amplíe **File Sanitizer** y haga clic en **Triturar**.
2. Seleccione una opción de trituración:

   - **Apagado de Windows** — Elija esta opción para triturar todos los archivos seleccionados cuando se cierre Windows.

     NOTA: Cuando se selecciona esta opción, un cuadro de dialogo aparece en el cierre preguntando si desea continuar con la trituración de los archivos seleccionados o si desea omitir el procedimiento. Haga clic en Sí para omitir el procedimiento de trituración o en No para continuar la trituración. Debe seleccionar Sí o No rápidamente porque Windows cerrará el software para prepararse para el apagado y se producirá un error. Si selecciona No para continuar con la trituración, Windows puede mostrar una pantalla de error en la que se indique que File Sanitizer no está respondiendo. Permita que File Sanitizer complete la trituración y, a continuación, vuelva a iniciar el apagado.

   - **Abrir navegador web** — Elija esta opción para triturar todos los archivos relacionados a la web seleccionados, como historial de explorador URL, cuando abre un explorador web.

- **Salir navegador web** — Elija esta opción para triturar todos los archivos relacionados a la web seleccionados, como historial de explorador URL, cuando sale del explorador web.
- **Secuencia de clave** — Elija esta opción para iniciar la trituración mediante una secuencia de teclas.
- **Programador** — Seleccione la casilla de verificación activar programador, ingrese su contraseña de Windows, y a continuación, ingrese el día y la hora para triturar los archivos seleccionados.

3. Haga clic en el icono **Guardar**.

Selección o creación de un perfil de trituración

Puede especificar un método de borrado y seleccionar los archivos y/o carpetas para triturar seleccionando un perfil predefinido o creando su propio perfil.

Selección de un perfil de trituración predefinido

Cuando selecciona un perfil de trituración predefinido (seguridad máxima, seguridad mediana o seguridad baja), un método de borrado predefinido y una lista de archivos son automáticamente seleccionados. Puede hacer clic en el botón visualizar detalles para visualizar la lista de archivos predefinidos que están seleccionados para trituración.

Para seleccionar un perfil de trituración predefinido:

1. En el panel izquierdo de Security Manager, amplíe **File Sanitizer** y haga clic en **Configuración**.
2. Haga clic en un perfil de trituración predefinido.
3. Haga clic en **Visualizar detalles** para visualizar la lista de archivos que están seleccionados para trituración.
4. En **Triturar lo siguiente**, seleccione la casilla de verificación junto a cada archivo que desea confirmar antes de triturar.
5. Haga clic en **Aplicar**.

Personalización de un perfil de trituración de seguridad avanzada

Cuando crea un perfil de trituración, puede especificar el número de ciclos de trituración, cuales archivos incluir para trituración, cuales archivos confirmar antes de la trituración, y cuales archivos excluir antes de la trituración.

1. En el panel izquierdo de Security Manager, amplíe **File Sanitizer**, haga clic en **Configuración**, seleccione **Configuración Avanzada de seguridad** y, a continuación, haga clic en **Visualizar detalles**.
2. Especifique el número de ciclos de trituración.

NOTA: El número seleccionado de ciclos de trituración será ejecutado para cada archivo. Por ejemplo, si selecciona 3 ciclos de trituración, un algoritmo que borra los datos se ejecuta tres veces. Si elije ciclos de trituración con seguridad máxima, la trituración puede llevar un período significante de tiempo; sin embargo, mientras mayor el número de ciclos de trituración que especifique, mayor es la seguridad del equipo.

3. Seleccione los activos que desea triturar:

   a. En **Opciones de eliminación**, haga clic en un archivo, y a continuación haga clic en **Agregar**.

   b. Para agregar un archivo personalizado, haga clic en **Agregar opción personalizada**, ingrese o explore el nombre de un archivo o carpeta, y luego haga clic en **Aceptar**. Haga clic en el archivo personalizado, y en seguida haga clic en **Agregar**.

   NOTA: Para eliminar un archivo de las opciones de trituración disponibles, haga clic en el archivo y luego haga clic en **Eliminar**.

4. En **Triturar lo siguiente**, seleccione la casilla de verificación junto a cada archivo que desea confirmar antes de triturar.

NOTA: Para eliminar un archivo de la lista de trituración, haga clic en el archivo y luego haga clic en **Eliminar**.

5. En **No triture lo siguiente**, haga clic en **Agregar** para seleccionar los archivos específicos que desea excluir de la trituración.

6. Cuando termine de configurar el perfil de trituración, haga clic en **Aplicar**.

Personalización de un perfil de eliminación simple

El perfil de eliminación simple ejecuta una eliminación estándar de archivo sin trituración. Cuando personaliza un perfil de eliminación simple, usted especifica cuales archivos incluir para la eliminación simple, cuales archivos confirmar antes de ejecutar la eliminación simple y cuales archivos excluir de la eliminación simple:

NOTA: Se recomienda enfáticamente que ejecute la purificación de espacio libre si utiliza la opción de eliminación simple.

1. En el panel izquierdo de Security Manager, amplíe **File Sanitizer**, haga clic en **Configuración**, seleccione **Configuración de eliminación simple** y, a continuación, haga clic en **Visualizar detalles**.

2. Seleccione los archivos que desea eliminar:

   a. En **Opciones de eliminación disponibles**, haga clic en un archivo, y a continuación, haga clic en **Agregar**.

   b. Para agregar un archivo personalizado, haga clic en **Agregar opción personalizada**, ingrese o explore el nombre de un archivo o carpeta, y luego haga clic en **Aceptar**. Haga clic en el archivo personalizado, y en seguida haga clic en **Agregar**.

   NOTA: Para eliminar un archivo de las opciones de eliminación disponibles, haga clic en el archivo y luego haga clic en **Eliminar**.

3. En **Eliminar lo siguiente**, seleccione la casilla de verificación junto a cada archivo que desea confirmar antes de eliminar.

NOTA: Para eliminar un archivo de la lista de eliminación, haga clic en el archivo y luego haga clic en **Eliminar**.

4. En **No elimine lo siguiente**, haga clic en **Agregar** para seleccionar los archivos específicos que desea excluir de la trituración.

5. Cuando termine de configurar el perfil de eliminación simple, haga clic en **Aplicar**.

Tareas generales

Uso de una secuencia de teclas para iniciar trituración

Para especificar una secuencia de clave, siga los siguientes pasos:

1. En el panel izquierdo de Security Manager, amplíe **File Sanitizer** y haga clic en **Triturar**.

2. Seleccione la casilla de verificación **Secuencia de clave**.

3. Ingrese un carácter en la casilla disponible, y luego seleccione las teclas **CTRL**, **ALT**, o **MAYÚS**, o seleccione las tres.

   Por ejemplo, para iniciar trituración automática mediante la tecla S y Ctrl+Mayús, ingrese S en la casilla, y luego seleccione las opciones **CTRL** y **MAYÚS**.

NOTA: Asegúrese de seleccionar una secuencia de teclas que sea diferente de otras secuencias de teclas que ya configuró.

Para iniciar trituración a través de una secuencia de teclas:

1. Presione la tecla Ctrl, Alt, o Mayús (o la combinación que usted especificó) mientras presiona el carácter seleccionado.

2. Si aparece un cuadro de dialogo de confirmación, haga clic en **Sí**.

Uso del icono File Sanitizer

△ **PRECAUCIÓN:** Archivos triturados no pueden recuperarse. Considere cuidadosamente cuales elementos selecciona para trituración manual.

1. Navegue al documento o carpeta que desea triturar.

2. Arrastre el archivo para el icono File Sanitizer en el escritorio.

3. Cuando aparezca el cuadro de diálogo de confirmación, haga clic en **Sí**.

Trituración manual de un activo

△ **PRECAUCIÓN:** Archivos triturados no pueden recuperarse. Considere cuidadosamente cuales elementos selecciona para trituración manual.

1. Haga clic con el botón derecho del mouse en el icono **HP ProtectTools** del área de notificación situada en el extremo derecho de la barra de tareas, resalte **File Sanitizer** y, a continuación, haga clic en **Triturar uno**.

2. Cuando aparezca el cuadro de dialogo de explorar, navegue para el archivo que desea triturar, y haga clic en **Abrir**.

NOTA: El archivo seleccionado puede ser un único archivo o carpeta.

3. Cuando aparezca el cuadro de diálogo de confirmación, haga clic en **Sí**.

– o –

1. Haga clic con el botón derecho en el icono **File Sanitizer** en el escritorio, y luego haga clic en **Triturar uno**.
2. Cuando aparezca el cuadro de dialogo de explorar, navegue para el archivo que desea triturar, y haga clic en **Aceptar**.
3. Cuando aparezca el cuadro de diálogo de confirmación, haga clic en **Sí**.

– o –

1. En el panel izquierdo de Security Manager, amplíe **File Sanitizer** y haga clic en **Triturar**.
2. Haga clic en el botón **Explorar**.
3. Cuando aparezca el cuadro de dialogo de explorar, navegue para el archivo que desea triturar, y haga clic en **Abrir**.
4. Cuando aparezca el cuadro de diálogo de confirmación, haga clic en **Sí**.

Trituración manual de todos los elementos seleccionados

1. Haga clic con el botón derecho del mouse en el icono **HP ProtectTools** en el área de notificación situada en el extremo derecho de la barra de tareas, resalte **File Sanitizer** y, a continuación, haga clic en **Triturar ahora**.
2. Cuando aparezca el cuadro de diálogo de confirmación, haga clic en **Sí**.

– o –

1. Haga clic con el botón derecho en el icono **File Sanitizer** en el escritorio, y luego haga clic en **Triturar ahora**.
2. Cuando aparezca el cuadro de diálogo de confirmación, haga clic en **Sí**.

Activación manual de purificación de espacio libre

1. Haga clic con el botón derecho del mouse en el icono **HP ProtectTools** en el área de notificación situada en el extremo derecho de la barra de tareas, resalte **File Sanitizer** y, a continuación, haga clic en **Purificar ahora**.
2. Aparecerá una notificación en forma de burbuja que verifica que ha comenzado una operación de purificación.

– o –

1. En el panel izquierdo de Security Manager, amplíe **File Sanitizer** y haga clic en **Purificación**.
2. Haga clic en **Purificar ahora**.
3. Aparecerá una notificación en forma de burbuja que verifica que ha comenzado una operación de purificación.

Anulación de una operación de trituración o de purificación de espacio libre

Cuando una operación de purificación de espacio libre o trituración esté en curso, aparecerá un mensaje encima del icono de HP ProtectTools Security Manager, en el área de notificación. El mensaje aporta detalles sobre el proceso de purificación de espacio libre o trituración (porcentaje de progreso), y le provee la opción de cancelar la operación.

Para anular la operación:

▲ Haga clic en el mensaje, y luego haga clic en **Detener** para cancelar la operación.

Visualización de los archivos de registro

Cada vez que se ejecuta una operación de purificación de espacio libre o trituración, se generan archivos de registro de cualquier error o falla. Los archivos de registro son siempre actualizados según las últimas operaciones de trituración o de purificación de espacio libre.

NOTA: Los archivos que son triturados o purificados con éxito no aparecen en los archivos de registro.

Se crea un archivo de registro para operaciones de trituración y otro para las operaciones de purificación de espacio libre. Los dos archivos de registro están ubicados en la unidad de disco duro en:

- C:\Program Files\Hewlett-Packard\File Sanitizer\`[Username]`_ShredderLog.txt
- C:\Program Files\Hewlett-Packard\File Sanitizer\`[Username]`_DiskBleachLog.txt

9 Device Access Manager for HP ProtectTools

Esta herramienta de seguridad está disponible sólo para administradores. Device Access Manager for HP ProtectTools posee los siguientes recursos de seguridad que ofrecen protección contra al acceso no autorizado a dispositivos conectados al equipo:

- Perfiles de dispositivos son creados para cada usuario para definir acceso a dispositivos
- Acceso a dispositivos puede ser otorgado o negado con base a la membresía de grupo

NOTA: Device Access Manager utiliza Usuarios y grupos locales de Windows para administrar el acceso. Las versiones de Windows Home no son compatibles con Usuarios y grupos locales, por lo tanto, Device Access Manager no funcionará correctamente. Sin embargo, Device Access Manager funcionará en la versión de Vista Home de Microsoft Windows si utiliza los comandos DOS para la configuración de usuario. Consulte el archivo de ayuda de Device Access Manager para obtener instrucciones.

Inicio de servicio en segundo plano

Para que se apliquen los perfiles de dispositivo, es necesario que el servicio en segundo plano HP ProtectTools Device Locking/Auditing esté en ejecución. Cuando intente aplicar por primera vez un perfil de dispositivo, Consola administrativa de HP ProtectTools abrirá un cuadro de diálogo para preguntarle si desea iniciar el servicio en segundo plano. Haga clic en el botón **Sí** para iniciar el servicio en segundo plano y configurarlo para que se inicie automáticamente al iniciar el sistema.

Configuración sencilla

Device Access Manager crea un nuevo grupo de usuarios durante la inicialización denominado administradores del dispositivo para acceder y explorar los dispositivos como administrador. Coloque en este grupo a los usuarios que desee que tengan acceso de administrador a los dispositivos que controla a través de la Configuración sencilla de Device Access Manager.

Este recurso permite negar acceso a las siguientes clases de dispositivos:

- Dispositivos USB para todos los usuarios que no sean administradores de dispositivos
- Todos los medios extraíbles (disquetes, reproductores personales de música, pen drives, etc.) para todos los usuarios que no sean administradores de dispositivos

- Todas las unidades de DVD/CD-ROM para todos los usuarios que no sean administradores de dispositivos
- Todos los puertos en serie y paralelos para todos los usuarios que no sean administradores de dispositivos

Para denegar el acceso a una clase de dispositivo a todos los usuarios que no sean administradores de dispositivos:

1. Haga clic en **Inicio**, luego en **Todos los programas** y, a continuación, en **Consola administrativa de HP ProtectTools**.
2. En el panel izquierdo, haga clic en **Device Access Manager**, y luego haga clic en **Configuración sencilla**.
3. En el panel derecho, seleccione la casilla de verificación de un dispositivo para negar acceso.
4. Haga clic en el icono **Guardar**.

   NOTA: Si el servicio de segundo plano no está en ejecución, intenta iniciarlo ahora. Haga clic en **Sí** para permitirlo.

5. Haga clic en **Aceptar**.

Configuración de clases de dispositivos (avanzado)

Más selecciones están disponibles para permitir que a usuarios específicos o grupos de usuarios se les otorgue o niegue acceso a tipos de dispositivos.

Agregado de un usuario o grupo

1. Haga clic en **Inicio**, luego en **Todos los programas** y, a continuación, en **Consola administrativa de HP ProtectTools**.
2. En el panel izquierdo, amplíe **Device Access Manager** y, a continuación, haga clic en **Configuración de clases de dispositivos**.
3. En la lista de dispositivos, haga clic en la clase de dispositivos que desea configurar.
4. Haga clic en **Agregar**. Se abrirá el cuadro de diálogo **Seleccionar usuarios o grupos**.
5. Haga clic en **Opciones avanzadas** y, a continuación, en **Buscar ahora** para buscar los usuarios o grupos que desea agregar.
6. Haga clic en un usuario o un grupo para agregar a la lista de usuarios y grupos disponibles y, a continuación, haga clic en **Aceptar**.
7. Haga clic en **Aceptar**.

Eliminación de un usuario o grupo

1. Haga clic en **Inicio**, luego en **Todos los programas** y, a continuación, en **Consola administrativa de HP ProtectTools**.
2. En el panel izquierdo, amplíe **Device Access Manager** y, a continuación, haga clic en **Configuración de clases de dispositivos**.

3. En la lista de dispositivos, haga clic en la clase de dispositivos que desea configurar.
4. Haga clic en el usuario o grupo que desea quitar y, a continuación, haga clic en **Eliminar**.

Denegación o permiso de acceso a un usuario o grupo

1. Haga clic en **Inicio**, luego en **Todos los programas** y, a continuación, haga clic en **Consola administrativa de HP ProtectTools**.
2. En el panel izquierdo, amplíe **Device Access Manager** y, a continuación, haga clic en **Configuración de clases de dispositivos**.
3. En la lista de dispositivos, haga clic en la clase de dispositivos que desea configurar.
4. En **Usuario/Grupos**, agregue el usuario o grupo que desea negar acceso.
5. Haga clic en **Denegar**, en el usuario o grupo que desea negar acceso.
6. Haga clic en el icono **Guardar** y, a continuación, haga clic en **Aceptar**.

Configuraciones de acceso de usuario (avanzada)

Las configuraciones de acceso de usuario permite que los administradores especifiquen los usuarios y grupos que pueden utilizar las vistas Configuración sencilla y configuración de clases de dispositivos.

Un usuario o grupo debe tener acceso **Ver (sólo lectura) las opciones de configuración** para poder ver la información de Configuración sencilla y configuración de clases de dispositivos.

Un usuario o grupo debe tener acceso **Cambiar las opciones de configuración** para poder cambiar la información de Configuración sencilla y configuración de clases de dispositivos.

Un usuario o grupo debe tener acceso **Todos los derechos del usuario-administrador** para poder modificar la configuración en la vista Configuración sencilla y configuración de clases de dispositivos.

Adición de un usuario o grupo

1. Haga clic en **Inicio**, luego en **Todos los programas** y, a continuación, haga clic en **Consola administrativa de HP ProtectTools**.
2. En el panel izquierdo, amplíe **Device Access Manager** y, a continuación, haga clic en **Configuraciones de acceso de usuario**.
3. Haga clic en **Agregar**. Se abrirá el cuadro de diálogo **Seleccionar usuarios o grupos**.
4. Haga clic en **Opciones avanzadas** y, a continuación, haga clic en **Buscar ahora** para buscar los usuarios o grupos que desea agregar.
5. Haga clic en un usuario o un grupo que desea a agregar a la lista de usuarios y grupos disponibles y, a continuación, haga clic en **Aceptar**.
6. Haga clic en **Aceptar**.
7. Haga clic en el icono **Guardar**.

Eliminación de un usuario o grupo

1. Haga clic en **Inicio**, luego en **Todos los programas** y, a continuación, haga clic en **Consola administrativa de HP ProtectTools**.
2. En el panel izquierdo, amplíe **Device Access Manager** y, a continuación, haga clic en **Configuraciones de acceso de usuario**.
3. Haga clic en el usuario o grupo que desea quitar y, a continuación, haga clic en la opción **Quitar**.
4. Haga clic en el icono **Guardar**.

Permiso o denegación de permiso

1. Haga clic en **Inicio**, luego haga clic en **Todos los programas** y, a continuación, haga clic en **Consola administrativa de HP ProtectTools**.
2. En el panel izquierdo, amplíe **Device Access Manager** y, a continuación, haga clic en **Configuraciones de acceso de usuario**.
3. En el cuadro **Nombres de grupo o usuario**, seleccione un nombre de usuario o grupo.

4. En el cuadro **Permisos**, seleccione las casillas de verificación **Permitir** o **Denegar** para los permisos apropiados.
5. Haga clic en el icono **Guardar**.

Glosario

activo.
Un componente de datos que consiste de información o archivos personales, historiales y datos relacionados con la web, y así sucesivamente, que están ubicados en la unidad de disco duro.

administrador.
Consulte con el administrador de Windows.

administrador de Windows.
Un usuario con derechos completos para modificar permisos y administrar otros usuarios.

autenticación.
Proceso de verificación para determinar si un usuario está autorizado para realizar una tarea, por ejemplo, acceder a un equipo, modificar la configuración de un programa determinado o ver datos protegidos.

autenticación de inicio.
Recurso de seguridad que requiere alguna forma de autenticación, como una contraseña, al encender el equipo.

ciclo de trituración.
El número de veces que se ejecuta el algoritmo de trituración en cada activo. El número mayor de ciclos de trituración que seleccione, mayor es la seguridad del equipo.

credenciales.
Método que permite al usuario probar que está autorizado a realizar una tarea determinada en el proceso de autenticación, como un nombre de usuario y contraseña.

cuenta de red.
Cuenta de usuario o administrador de Windows, ya sea en un equipo local, un grupo de trabajo o un dominio.

cuenta de usuario de Windows.
Perfil para una persona autorizada a iniciar sesión en una red o un equipo individual.

dominio.
Grupo de equipos que integran una red y comparten una base de datos de directorios común. Los dominios poseen nombres exclusivos y cada uno tiene un conjunto de procedimientos y normas comunes.

eliminación simple.
Elimina con seguridad información sensible incluyendo archivos, historiales o contenido con base en la web u otros datos confidenciales.

Gerente de tecnología automática (ATM).
Permite que los administradores de la red administren sistemas de forma remota a nivel de BIOS.

Método de seguridad de inicio de sesión.
El método utilizado para iniciar sesión en el equipo.

perfil de trituración.
Un método de borrado específico y una lista de activos.

Purificación.
consulte **purificación de espacio libre**.

purificación de espacio libre.
La grabación segura de datos aleatorios sobre archivos eliminados en la unidad de disco duro para destorcer el contenido de los archivos eliminados, haciendo la recuperación de datos más difícil.

reinicio.
Proceso de reinicio del equipo.

Secuencia de clave.
Una combinación específica de teclas que, cuando presionadas, inician una trituración automática, por ejemplo, Ctrl+Alt+Mayús.

trituración automática.
Trituración programada que un usuario define en File Sanitizer for HP ProtectTools.

trituración manual.
Trituración inmediata de un activo o activos seleccionados, que ignoran la programación automática de trituración.

Triturar.
La ejecución de un algoritmo que oscurece los datos contenidos en un activo.

Índice

A

acceso
  control 52
  prevención no autorizada 21
acceso a HP ProtectTools Security 20
acceso no autorizado, prevención 21
asistente de configuración
  administradores 25

C

cambio de la contraseña de Windows 31
configuración del equipo
  contraseña de administrador 22
configuración de usuarios 25
configuración inicial 25
Consola administrativa de HP ProtectTools Security Console
  descripción general 1
  recursos 2
Consola administrativa de HP ProtectTools Security Manager
  administración de usuarios 27
  configuración del sistema 26
  configuración de parámetros de la aplicación 29
  encriptado de unidad 30
  rechazo de device access 30
contraseña
  administración 22
  HP ProtectTools 22
  pautas 22
  políticas, creación 21
  segura, creación 22
contraseña de administrador de BIOS 22
contraseña de configuración de seguridad 22
contraseña de configuración F10 22
contraseña de inicio
  definición 22
control de device access 52
copia de seguridad y restauración 33
Credential Manager for HP ProtectTools
  adición de inicios de sesión 41
  administración de inicios de sesión 43
  categorías de inicios de sesión 43
  configuración de icono 44
  configuración fácil 8
  contraseña de inicio de sesión 22
  edición de inicios de sesión 42
  recursos 2
  seguridad de contraseña 44
  uso del menú inicios de sesión 42
  visualización y administración de autenticaciones guardadas 10

D

datos, restricción de acceso a 20
desencriptación de una unidad 36
Device Access Manager for HP ProtectTools
  configuración de clase de dispositivos 53
  configuración fácil 16
  configuración sencilla 52
  denegación de acceso, usuario o grupo 54
  ejemplos de uso común 5
  recursos 3
  servicio en segundo plano 52
  usuario o grupo, agregado 53
  usuario o grupo, eliminación 53
Drive Encryption for HP ProtectTools
  activación 38
  administración de Drive Encryption 39
  apertura 37
  configuración fácil 18
  copia de seguridad y restauración 39
  creación de claves de copia de seguridad 39
  desactivación 38
  ejemplos de uso común 4
  encriptación de unidades individuales 39
  inicio de sesión después de activar Drive Encryption 38

E

ejemplos de uso común 3
encriptación de una unidad 36

F

File Sanitizer 49

File Sanitizer for HP ProtectTools
activación manual de purificación de espacio libre 50
anulación de una operación de trituración o de purificación de espacio libre 51
apertura 46
configuración de una programación de purificación 46
configuración de una programación de trituración 46
configuración fácil 13
ejemplos de uso común 4
perfil de eliminación simple 48
perfil de trituración 47
perfil de trituración, selección o creación 47
perfil de trituración predeterminado 47
procedimientos de configuración 46
purificación 45
recursos 3
trituración 45
trituración manual de todos los elementos seleccionados 50
trituración manual de un activo 49
uso del icono File Sanitizer 49
uso de una secuencia de clave para iniciar trituración 49
visualización de archivos de registro 51

G
Guía de configuración fácil 6

H
HP ProtectTools Security, acceso 20
HP ProtectTools Security Manager
adición de aplicaciones 33
administración de contraseñas 31
cambio del nombre de usuario de Windows 35
cambio de su imagen 35
configuración de credenciales 31
copia de seguridad y restauración 33
descripción general 1
device access 32
estado de encriptación de unidad 32
preferencias 33
recursos 2
trituración o purificación de archivos 32

I
inicio de sesión en Windows
contraseña 22

O
objectivos, seguridad 20
objetivos principales de seguridad 20

P
Pasos iniciales 6
Password Manager for HP ProtectTools
ejemplos de uso común 3
perfil de eliminación simple
personalización 48
perfil de trituración
personalización 47
predefinido 47
selección o creación 47

R
recursos, HP ProtectTools 2
recursos de HP ProtectTools 2
restricción
acceso a datos sensibles 20
device access 52

S
seguridad
asistente de configuración 25
funciones 21
métodos de inicio de sesión 25
niveles 25
objetivos principales 20
servicio en segundo plano, Device Access Manager 52

T
tareas avanzadas
Device Access Manager 53