HP ProtectTools
Guía del usuario

Bluetooth es una marca comercial de su propietario utilizada por Hewlett-Packard Company bajo licencia. Java es una marca registrada de Sun Microsystems, Inc. en EE.UU. Microsoft y Windows son marcas comerciales registradas en EE. UU. de Microsoft Corporation.

La información contenida en el presente documento está sujeta a cambios sin previo aviso. Las únicas garantías para los productos y servicios de HP están estipuladas en las declaraciones expresas de garantía que acompañan a dichos productos y servicios. La información contenida en este documento no debe interpretarse como una garantía adicional. HP no se responsabilizará por errores técnicos o de edición ni por omisiones contenidas en el presente documento.

Primera edición: noviembre de 2009

Número de referencia del documento: 593308-E51

Tabla de contenido

1 Introducción a la seguridad

Recursos de HP ProtectTools 2
Cómo lograr los objetivos clave de seguridad 4
Protección contra robos específicos 4
Restricción del acceso a los datos sensibles 4
Prevención de acceso no autorizado desde ubicaciones internas o externas 4
Creación de políticas de contraseñas sólidas 5
Elementos de seguridad adicionales 6
Asignación de las funciones de seguridad 6
Administración de contraseñas de HP ProtectTools 6
Creación de una contraseña segura 8
Copia de seguridad y restauración de las credenciales de HP ProtectTools 8

2 Pasos iniciales con el Asistente de configuración

3 Consola administrativa de HP ProtectTools Security Manager

Abrir la consola administrativa 12
Uso de la consola administrativa 13

4 Configuración de su sistema

Configuración de autenticación para su equipo 15
Política de inicio de sesión 15
Política de sesión 15
Configuración 16
Administración de usuarios 17
Especificación de la configuración del dispositivo 18
Huellas digitales 18
Smart Card 18
Rostro 18
Configuración avanzada 19

5 Configuración de sus aplicaciones

Ficha General 21

Ficha Aplicaciones 22

6 Herramientas de administración

Actualizaciones y mensajes 24

7 HP ProtectTools Security Manager

Abrir HP ProtectTools Security Manager 26
Uso del panel de control de Security Manager 27
Procedimientos de configuración 28
Registro de credenciales 28
Registro de sus huellas digitales 28
Registro de escenas 28
Configuración de usuario avanzado 30
Cambio de su contraseña de Windows 30
Configuración de una smart card 31
Tareas generales 32
Administrador de contraseñas 32
Para páginas web o programas donde no se haya creado aún el inicio de sesión 32
Para páginas web o programas donde ya se haya creado el inicio de sesión 33
Adición de inicios de sesión 33
Edición de inicios de sesión 34
Uso del menú de Inicios de sesión 35
Organización de inicios de sesión en categorías 35
Administración de sus inicios de sesión 35
Evaluación de la seguridad de su contraseña 36
Configuración del icono del Administrador de contraseñas 36
Configuración 37
Credenciales 37
Su tarjeta de identificación personal 38
Configuración de sus preferencias 38
General 38
Huella digital 39
Realización de copias de seguridad y restauración de sus datos 39
Descubrir más 40
Actualizaciones y mensajes 40
Estado de las aplicaciones de seguridad 40

8 Drive Encryption for HP ProtectTools (sólo en algunos modelos)

Procedimientos de configuración 42
Apertura de Drive Encryption 42
Tareas generales 43

Activación de Drive Encryption 43
Desactivación de Drive Encryption 43
Inicio de sesión después de la activación de Drive Encryption 43
Protección de sus datos mediante la encriptación de su unidad de disco duro 44
Mostrar el estado de la encriptación 44
Tareas avanzadas 46
Administración de Drive Encryption (tarea de administrador) 46
Encriptación o desencriptación de unidades individuales 46
Copias de seguridad y recuperación (tarea de administrador) 46
Creación de claves de la copia de seguridad 46
Realización de una recuperación 47

9 Privacy Manager for HP ProtectTools (sólo en algunos modelos)

Procedimientos de configuración 49
Apertura de Privacy Manager 49
Administración de certificados de Privacy Manager 49
Solicitación e instalación de un certificado de Privacy Manager 49
Solicitud de un certificado de Privacy Manager 50
Obtención de un certificado corporativo preasignado de Privacy Manager 50
Instalación de un certificado de Privacy Manager 50
Visualización de los detalles del certificado de Privacy Manager 51
Renovación de un certificado de Privacy Manager 51
Configuración de un certificado de Privacy Manager predeterminado 51
Eliminación de un certificado de Privacy Manager 52
Restauración de un certificado de Privacy Manager 52
Revocación de su certificado de Privacy Manager 52
Administración de contactos confiables 53
Agregado de contactos confiables 53
Adición de un contacto confiable 53
Adición de Contactos Confiables usando sus contactos de Microsoft Outlook 54
Visualización de detalles de Contactos confiables 55
Eliminación de un contacto confiable 55
Verificación del estado de revocación de un contacto confiable 55
Tareas generales 56
Uso de Privacy Manager en Microsoft Outlook 56
Configuración de Privacy Manager para Microsoft Outlook 56
Firma y envío de un mensaje de correo electrónico 57
Sellado y envío de un mensaje de correo electrónico 57
Visualización de un mensaje de correo electrónico sellado 57
Uso de Privacy Manager en un documento de Microsoft Office 2007 57
Configuración de Privacy Manager para Microsoft Office 58
Firma de un documento de Microsoft Office 58

Adición de una línea de firma cuando firma un documento de Microsoft Word o Microsoft Excel ... 58
Adición de firmantes sugeridos a documentos de Microsoft Word o Microsoft Excel ... 59
Adición de una línea de firma para un firmante sugerido ... 59
Encriptación de un documento de Microsoft Office ... 60
Eliminación de la encriptación de un documento de Microsoft Office ... 60
Envío de un documento de Microsoft Office encriptado ... 60
Visualización de un documento de Microsoft Office firmado ... 61
Visualización de un documento de Microsoft Office encriptado ... 61
Uso de Privacy Manager en Windows Live Messenger ... 61
Inicio de una sesión de chat en Privacy Manager ... 62
Configuración de Privacy Manager para Windows Live Messenger ... 63
Realización de un chat en la ventana del chat de Privacy Manager ... 63
Visualización del historial del chat ... 64
Revelación de todas las sesiones ... 64
Revelar sesiones de una cuenta específica ... 64
Visualización de una identidad de sesión ... 65
Visualización de una sesión ... 65
Búsqueda de un texto específico en las sesiones ... 65
Eliminación de una sesión ... 65
Adición o eliminación de columnas ... 66
Filtrado de sesiones mostradas ... 66
Tareas avanzadas ... 68
Migración de certificados de Privacy Manager y de contactos confiables a otro equipo ... 68
Copia de respaldo de certificados de Privacy Manager y contactos confiables ... 68
Restauración de certificados de Privacy Manager y contactos confiables ... 68
Administración central de Privacy Manager ... 69

10 File Sanitizer for HP ProtectTools

Eliminación definitiva ... 71
Limpieza para liberar espacio ... 72
Procedimientos de configuración ... 73
Apertura de File Sanitizer ... 73
Programación de una eliminación definitiva ... 73
Programación de limpieza para liberar espacio ... 74
Selección o creación de un perfil de eliminación definitiva ... 74
Selección de un perfil de eliminación definitiva predefinido ... 74
Personalización de un perfil de eliminación definitiva ... 75
Personalización de un perfil de borrado simple ... 75
Tareas generales ... 77
Uso de una secuencia de teclas para iniciar la trituración ... 77

Uso del icono de File Sanitizer 78
Eliminación definitiva manual de un activo 78
Eliminación definitiva manual de todos los elementos seleccionados 79
Activación manual de la limpieza para liberar espacio 79
Interrupción de una operación de eliminación definitiva o de una limpieza para liberar espacio 79
Visualización de los archivos de registro 79

11 Device Access Manager for HP ProtectTools (sólo en algunos modelos)

Procedimientos de configuración 82
Apertura de Device Access Manager 82
Configuración del acceso a los dispositivos 82
Grupo de administradores de dispositivos 82
Configuración sencilla 83
Inicio del servicio en segundo plano 83
Configuración por clases de dispositivo 84
Negación del acceso a un usuario o grupo 86
Permitir el acceso de un usuario o grupo 86
Quitar el acceso de un usuario o grupo 87
Permitirle el acceso a una clase de dispositivos a un usuario de un grupo 87
Permitirle el acceso a un dispositivo específico a un usuario de un grupo 87
Restablecimiento de la configuración 88
Tareas avanzadas 89
Control del acceso a la configuración 89
Concesión de acceso a un grupo o usuario existente 89
Negación del acceso a un grupo o usuario existente 90
Agregar un nuevo grupo o usuario 90
Quitar el acceso de un grupo o usuario 90
Documentación relacionada 90

12 LoJack Pro for HP ProtectTools

13 Solución de problemas

HP ProtectTools Security Manager 93
Device Access Manager for HP ProtectTools 95
Varios 97

Glosario 98

Índice 103

1 Introducción a la seguridad

El software HP ProtectTools Security Manager proporciona recursos de seguridad que lo ayudan a protegerse contra el acceso no autorizado al equipo, a la red y a los datos críticos. La administración de HP ProtectTools Security Manager se realiza mediante el recurso de la consola administrativa.

Usando la Consola administrativa de HP ProtectTools, el administrador local puede realizar las siguientes tareas:

- Activación o desactivación de los recursos de seguridad
- Registro de sus huellas digitales y las de otros usuarios de este equipo
- Registro de una o más escenas para la autenticación de rostros
- Configuración de una Smart Card para la autenticación
- Especificación de las credenciales necesarias para la autenticación
- Administración de usuarios del equipo
- Ajuste de los parámetros específicos del dispositivo
- Configuración de las aplicaciones de Security Manager instaladas
- Adición de otras aplicaciones de Security Manager

Usando el panel de control de Security Manager, los usuarios generales pueden realizar las siguientes tareas:

- Configurar opciones generales provistas por un administrador
- Permitir controles limitados de algunos módulos de HP ProtectTools

Los módulos de software disponibles para su equipo pueden variar según el modelo.

Los módulos del software HP ProtectTools pueden estar preinstalados, precargados o pueden descargarse del sitio Web de HP. Para obtener más información, visite http://www.hp.com.

NOTA: Las instrucciones de esta guía han sido redactadas bajo el supuesto de que ya han sido instalados los módulos correspondientes del software HP ProtectTools.

Recursos de HP ProtectTools

La siguiente tabla detalla los recursos claves de los módulos de HP ProtectTools.

Módulo	Recursos clave
Consola administrativa do HP ProtectTools Security Manager (para administradores)	• Instalar y configurar los niveles de seguridad y los métodos de inicio de sesión seguro usando el asistente de configuración de Security Manager. • Configurar opciones ocultas de usuarios básicos. • Configurar las configuraciones de Device Access Manager y el acceso de usuarios. • Agregar y quitar usuarios de HP ProtectTools y ver el estado usando las herramientas del administrador.
HP ProtectTools Security Manager (para usuarios generales)	• Organizar, instalar y cambiar los nombres y contraseñas de usuarios. • Configurar y cambiar credenciales de usuarios tales como la contraseña de Windows y Smart Card. • Configurar y cambiar las opciones de Trituración, Purificación y Configuraciones de File Sanitizer. • Ver las configuraciones de Device Access Manager. • Configurar opciones de preferencias y de copia de seguridad y restauración.
Credential Manager for HP ProtectTools (Administrador de contraseñas)	• Guardar, organizar y proteger sus nombres y contraseñas. • Configurar las pantallas de inicio de sesión en sitios Web y en programas para un acceso rápido y seguro. • Guardar los nombres de usuario y las contraseñas para sitios web introduciéndolos en el Administrador de contraseñas. La próxima vez que visite el sitio, el Administrador de contraseñas rellena y envía la información automáticamente. • Crear contraseñas más fuertes para tener más seguridad en la cuenta. El Administrador de contraseñas rellena y envía la información automáticamente.
Drive Encryption for HP ProtectTools (sólo en algunos modelos)	• Proporcionar una encriptación completa del volumen total de la unidad de disco duro. • Exigir autenticación de preinicio para desencriptar y acceder a los datos.
Privacy Manager for HP ProtectTools (sólo en algunos modelos)	• Utilizar técnicas de inicio de sesión avanzadas para verificar la fuente, la integridad y la seguridad del correo electrónico, de los documentos de Microsoft® Office o de la comunicación por mensajería instantánea (IM).

Módulo	Recursos clave
File Sanitizer for HP ProtectTools	• Eliminar definitivamente activos digitales (información sensible que incluye archivos de aplicación, contenido histórico o relacionado con la web u otros datos confidenciales) de su equipo y limpiar periódicamente la unidad de disco duro.
Device Access Manager for HP ProtectTools (sólo en algunos modelos)	• Permitir a los administradores de TI controlar el acceso a dispositivos con base en perfiles de usuario. • Impedir que usuarios no autorizados eliminen datos usando medios externos de almacenamiento y que introduzcan virus en el sistema a partir de medios externos. • Permitir a los administradores desactivar el acceso de individuos o grupos de usuarios a dispositivos de grabación.

Cómo lograr los objetivos clave de seguridad

Los módulos de HP ProtectTools pueden funcionar juntos para ofrecer soluciones a una diversidad de problemas de seguridad, incluidos los siguientes objetivos clave de seguridad:

- Protección contra robo dirigido
- Restricción de acceso a datos sensibles
- Prevención de acceso no autorizado desde ubicaciones internas o externas
- Creación de políticas de contraseñas fuertes

Protección contra robos específicos

Un ejemplo de robo específico es el robo de un equipo que contenga datos confidenciales e información del cliente en el puesto de control de seguridad de un aeropuerto. Los siguientes recursos lo ayudan a protegerse contra este tipo de robos:

- El recurso de autenticación de preinicio, si está activado, ayuda a evitar el acceso al sistema operativo. Vea los siguientes procedimientos:
  - Security Manager
  - Drive Encryption

Restricción del acceso a los datos sensibles

Supongamos que el auditor de un contrato está trabajando en su empresa y se le ha dado acceso por computadora para revisar datos financieros delicados. Usted no desea que el auditor pueda imprimir o guardar estos archivos en un dispositivo grabable como un CD. El siguiente recurso ayuda a restringir el acceso a los datos:

- Device Access Manager for HP ProtectTools les permite a los gerentes de TI restringir el acceso a dispositivos grabables de forma que la información delicada no se pueda imprimir o copiar desde el disco duro a un medio extraíble.

Prevención de acceso no autorizado desde ubicaciones internas o externas

El acceso no autorizado a un PC empresarial presenta un riesgo muy tangible para los recursos de red corporativos, como información de servicios financieros, de un ejecutivo o de un equipo de investigación y desarrollo, y para la información privada, como registros de pacientes o de finanzas personales. Los siguientes recursos ayudan a evitar el acceso no autorizado:

- El recurso de autenticación de preinicio, si está activado, ayuda a evitar el acceso al sistema operativo. Vea los siguientes procedimientos:
  - Administrador de contraseñas
  - Drive Encryption
- El Administrador de contraseñas ayuda a asegurar que un usuario no autorizado no pueda obtener las contraseñas o acceder a aplicaciones protegidas por contraseña.

- Device Access Manager for HP ProtectTools les permite a los gerentes de TI restringir el acceso a dispositivos grabables de forma que la información delicada no se pueda copiar desde el disco duro.
- File Sanitizer permite efectuar el borrado seguro de los datos mediante la eliminación segura de archivos críticos y carpetas o mediante la limpieza del disco duro (grabando sobre datos que han sido borrados pero que todavía son recuperables).
- DriveLock ayuda a asegurar que no se pueda acceder a sus datos, incluso si la unidad de disco duro se retira e instala en un sistema inseguro.

Creación de políticas de contraseñas sólidas

Si se hace valer una regla que exija el uso de una política de contraseñas sólidas para una gran cantidad de aplicaciones y bases de datos basadas en la Web, Security Manager ofrece un repositorio protegido para las contraseñas y la practicidad de Single Sign On.

Elementos de seguridad adicionales

Asignación de las funciones de seguridad

En la administración de la seguridad de equipos (particularmente en grandes organizaciones), una importante práctica consiste en dividir responsabilidades y derechos entre varios tipos de administradores y usuarios.

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

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

- Oficial de seguridad—Define el nivel de seguridad para la empresa o red y determina los recursos de seguridad a implementar, como Java™ Card, lectores biométricos o token USB.

  NOTA: Muchos de los recursos de HP ProtectTools pueden ser personalizados por el responsable de la seguridad en cooperación con HP. Para obtener más información, visite el sitio web de HP en http://www.hp.com.

- Administrador: aplica y administra los recursos de seguridad definidos por el funcionario de seguridad. También puede activar o desactivar algunos recursos. Por ejemplo, si el funcionario de seguridad ha decidido implementar Java Cards, el administrador de TI puede activar el modo de seguridad de Java Cards en el BIOS.

- Usuario—Utiliza los recursos de seguridad. Por ejemplo, si el oficial de seguridad y el administrador de TI han activado Java Card para el sistema, el usuario puede definir el PIN de la Java Card y utilizar la tarjeta para su autenticación.

PRECAUCIÓN: Se estimula a los administradores a seguir las “mejores prácticas” en la restricción de los privilegios de los usuarios finales y en la restricción del acceso de los usuarios.

A los usuarios no autorizados no se les debe conceder privilegios administrativos.

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 ésta.

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

Contraseña de HP ProtectTools	Definir el módulo siguiente	Función
Contraseña de inicio de sesión de Windows	Panel de control de Windows® o HP ProtectTools Security Manager	Puede utilizarse para el inicio de sesión manual y para la autenticación con el fin de acceder a distintos recursos de Security Manager.
Contraseña de copia de seguridad y recuperación de Security Manager	Security Manager, por usuario individual	Protege el acceso al archivo de copia de seguridad y recuperación de Security Manager.
PIN de Java™ Card	Java Card Security	Protege contra el acceso al contenido de la Java Card y autentica a los usuarios de la

Contraseña de HP ProtectTools	Definir el módulo siguiente	Función
		Java Card. Cuando se utiliza para realizar autenticación de inicio, el PIN de Java Card también protege contra el acceso a la utilidad de configuración y al contenido del equipo. Autentica los usuarios de Drive Encryption, si se selecciona el token de la Java Card.

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 ninguna 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.
- 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 y restauración de las credenciales de HP ProtectTools

Puede usar la función de copia de seguridad y recuperación de HP ProtectTools para seleccionar y realizar copias de seguridad de los datos y configuraciones de las credenciales de HP ProtectTools.

2 Pasos iniciales con el Asistente de configuración

El asistente de configuración de HP ProtectTools lo guía en el proceso de configuración de los recursos de Security Manager usados con más frecuencia. Sin embargo, existe una gama de funcionalidades adicionales disponibles a través de la consola administrativa de HP ProtectTools. Las mismas configuraciones encontradas en el asistente, así como recursos de seguridad adicionales, se pueden configurar mediante la consola, a la cual se accede desde el menú de Inicio de Windows®. Estas configuraciones se aplican al equipo y a todos los usuarios que lo compartan.

1. Una semana después de la configuración inicial del equipo, o cuando un usuario con derechos administrativos deslice un dedo por el lector de huellas digitales por primera vez, el asistente de configuración de Security Manager se iniciará automáticamente para guiarlo en los pasos básicos de configuración del programa. Se inicia automáticamente un tutorial en vídeo sobre cómo configurar el equipo.

   – ó –

   Abra HP ProtectTools Security Manager en el icono de **Dispositivo** en la barra lateral de Windows o en el icono de la barra de tareas en el área de notificación, en el extremo derecho de la barra de tareas.

   

   El color de la barra superior del icono de Dispositivo indica una de las siguientes condiciones:

   - Rojo: no se ha configurado HP ProtectTools, o existe una condición de error con uno de los módulos de ProtectTools.
   - Amarillo: verifique la página de Estado de la aplicación en Security Manager para los cambios de configuración que se deban realizar.
   - Azul: HP ProtectTools se ha configurado y está funcionando correctamente.

   NOTA: El icono de Dispositivo no está disponible en Windows XP.

   – ó –

Haga clic en **Inicio**, **Todos los programas**, y luego haga clic en **Consola administrativa de HP ProtectTools**.

2. Lea la pantalla "Bienvenido" y luego haga clic en **Siguiente**.

NOTA: En la pantalla Bienvenido, puede desactivar la exhibición del asistente seleccionando una de las opciones.

3. El asistente de configuración le pide que verifique su identidad.

   Escriba la contraseña de Windows o escanee su huella digital con el lector de huellas digitales, y luego haga clic en **Siguiente**.

   Si no cuenta con un lector de huellas digitales ni una Smart Card, se le pide que introduzca su contraseña de Windows. Debe utilizar esta contraseña en el futuro cada vez que se requiera la autenticación.

   Si aún no ha creado una contraseña de Windows, se le pide que cree una. Se requiere una contraseña de Windows a fin de proteger su cuenta de Windows del acceso por parte de personas no autorizadas y a fin de utilizar los recursos de HP ProtectTools Security Manager.

4. El asistente de configuración lo guía por el proceso de configurar los recursos de seguridad que se aplican a todos los usuarios del equipo:

   - Windows Logon Security protege sus cuentas de Windows al exigir el uso de credenciales específicas para el acceso.
   - Drive Encryption protege sus datos mediante la encriptación de las unidades de disco, haciendo ilegible la información para quienes carecen de la autorización apropiada.
   - Pre-Boot Security protege su equipo al prohibir el acceso por parte de personas no autorizadas antes del inicio de Windows.

   NOTA: Pre-Boot Security no está disponible si el BIOS de su equipo no lo admite.

   Para activar un recurso de seguridad, seleccione su casilla de verificación. Mientras más recursos seleccione, más seguro es su equipo.

5. En la página final del asistente, haga clic en **Finalizar**.

   Aparece el panel de control de Security Manager.

NOTA: Si no completa el asistente, éste se inicia automáticamente dos veces más. Después de eso, puede acceder al asistente desde el globo de notificación que aparece en el área de notificación, en el extremo derecho de la barra de tareas (a menos que lo haya desactivado) hasta que se haya completado la configuración.

3 Consola administrativa de HP ProtectTools Security Manager

La administración de HP ProtectTools Security Manager se realiza mediante la consola administrativa.

NOTA: La administración de HP ProtectTools requiere privilegios de administrador.

La consola cuenta con los siguientes recursos:

- Activación o desactivación de los recursos de seguridad
- Administración de usuarios del equipo
- Ajuste de los parámetros específicos del dispositivo
- Configuración de las aplicaciones de Security Manager
- Adición de otras aplicaciones de Security Manager

▲ Para usar las aplicaciones de HP ProtectTools Security Manager, inicie HP ProtectTools Security Manager en el menú Inicio o haga clic con el botón derecho en el icono de Security Manager en el área de notificación, ubicado en el extremo derecho de la barra de tareas.

La Consola administrativa de HP ProtectTools y sus aplicaciones están disponibles para todos los usuarios que comparten este equipo.

Abrir la consola administrativa

Para tareas administrativas como definir las políticas del sistema o configurar el software, abra la consola como sigue:

- Haga clic en **Inicio**, **Todos los programas**, **HP** y luego en **Consola administrativa de HP ProtectTools**.

  – ó –

  En el panel izquierdo del panel de control de Security Manager, haga clic en **Administración**.

Para realizar tareas del usuario, como el registro de huellas digitales o el uso de Security Manager, abra la consola como se describe a continuación:

- Haga clic en **Inicio**, **Todos los programas**, **HP** y en **HP ProtectTools Security Manager**.

  – ó –

  Haga doble clic en el icono de **HP ProtectTools Security Manager** en el área de notificación, en el extremo derecho de la barra de tareas.

Uso de la consola administrativa

La consola administrativa de Security Manager es la ubicación central destinada a la administración de HP ProtectTools Security Manager.

La consola está compuesta por los siguientes componentes:

- **Herramientas**: muestra las siguientes categoría para configurar la seguridad en su equipo:
  - **Inicio**: le permite seleccionar las tareas de seguridad que se van a realizar.
  - **Sistema**: le permite configurar los recursos de seguridad y la autenticación para usuarios y dispositivos.
  - **Aplicaciones**: muestra las configuraciones generales para HP ProtectTools Security Manager y para las aplicaciones de Security Manager.
  - **Datos**: ofrece un menú que se expande con enlaces a aplicaciones de Security Manager que protegen sus datos.
- **Herramientas de administración**: provee información sobre herramientas adicionales. El panel muestra las siguientes opciones:
  - **Asistente de configuración de HP ProtectTools Security Manager**: lo guía por la configuración de HP ProtectTools Security Manager.
  - **Ayuda**: muestra este archivo de Ayuda, que brinda información sobre Security Manager y sus aplicaciones preinstaladas. La ayuda para las aplicaciones que usted puede agregar se brinda dentro de las mismas aplicaciones.
  - **Acerca de**: muestra información acerca de HP ProtectTools Security Manager, como el número de versión y el aviso de copyright.
- **Área principal**: muestra pantallas específicas para aplicaciones.

4 Configuración de su sistema

Al grupo del Sistema se accede desde el panel del menú Herramientas a la izquierda de la pantalla de la Consola administrativa de HP ProtectTools. Puede utilizar las aplicaciones de este grupo para administrar las políticas y configuraciones del equipo, sus usuarios y sus dispositivos.

Las siguientes aplicaciones se incluyen en el grupo del Sistema:

- **Seguridad**: administre los recursos, la autenticación y la configuración que rigen cómo los usuarios interactúan con este equipo.
- **Usuarios**: configure, administre y registre los usuarios de este equipo.
- **Dispositivos**: administre la configuración de los dispositivos de seguridad incorporados o conectados al equipo.

Configuración de autenticación para su equipo

En la aplicación Autenticación, puede seleccionar qué recursos de seguridad deben implementarse en este equipo, establecer las políticas que rigen el acceso al equipo y configurar parámetros avanzados adicionales. Puede especificar las credenciales necesarias para autenticar cada clase de usuario cuando inicia sesión en Windows o en sitios Web y programas durante una sesión del usuario.

Para configurar la autenticación en su equipo:

1. En el menú del panel de Seguridad, haga clic en **Autenticación**.
2. Para configurar la autenticación de inicio de sesión, haga clic en la ficha **Política de inicio de sesión**, efectúe los cambios y haga clic en **Aplicar**.
3. Para configurar la autenticación de la sesión, haga clic en la ficha **Política de sesión**, efectúe los cambios y haga clic en **Aplicar**.

Política de inicio de sesión

Para definir las políticas que rigen las credenciales necesarias para autenticar a un usuario cuando inicia sesión en Windows:

1. En el menú Herramientas, haga clic en **Seguridad**, y luego en **Autenticación**.
2. En la ficha **Política de inicio de sesión**, haga clic en una categoría de usuario.
3. Especifique la(s) credencial(es) de autenticación necesaria(s) para la categoría seleccionada de usuario. Debe especificar por lo menos una credencial.
4. Elija si se requiere CUALQUIERA (sólo una) de las credenciales especificadas o si se requieren TODAS las credenciales especificadas para autenticar a un usuario. También puede evitar que cualquier usuario use el equipo.
5. Haga clic en **Aplicar**.

Política de sesión

Para definir las políticas que rigen las credenciales necesarias para acceder a las aplicaciones de HP ProtectTools durante una sesión en Windows:

1. En el menú Herramientas, haga clic en **Seguridad**, y luego en **Autenticación**.
2. En la ficha **Política de sesión**, haga clic en una categoría de usuario.
3. Especifique la(s) credencial(es) de autenticación necesaria(s) para la categoría seleccionada de usuario.
4. Elija si se requiere UNA de las credenciales especificadas o si se requieren TODAS las credenciales especificadas para autenticar a un usuario. También puede exigir que no se use autenticación para acceder al software HP ProtectTools.
5. Haga clic en **Aplicar**.

Configuración

Puede permitir una o más de las siguientes configuraciones de seguridad:

- **Permitir One Step logon**: permite que los usuarios de este equipo omitan el inicio de sesión en Windows si se realizó la autenticación a nivel del BIOS o del disco encriptado.
- **Permitir la autenticación de HP SpareKey para inicio de sesión de Windows**: permite que los usuarios de este equipo utilicen el recurso HP SpareKey para iniciar una sesión en Windows a pesar de cualquier otra política de autenticación requerida por Security Manager.

Para editar la configuración:

1. Haga clic para activar o desactivar una configuración específica.
2. Haga clic en **Aplicar** para guardar los cambios realizados.

Administración de usuarios

Dentro de la aplicación Usuarios, puede supervisar y administrar a los usuarios de HP ProtectTools en este equipo.

Todos los usuarios de HP ProtectTools se enumeran y verifican con relación a las políticas fijadas a través de Security Manager. Además, se verifica si registraron o no las credenciales adecuadas que les permitan cumplir con dichas políticas.

Para administrar usuarios, seleccione las siguientes configuraciones:

- Para agregar usuarios, haga clic en **Agregar**.
- Para eliminar un usuario, haga clic en el usuario y a continuación haga clic en **Eliminar**.
- Para registrar huellas digitales o configurar credenciales adicionales para el usuario, haga clic en el usuario y luego en **Registrar**.
- Para ver las políticas referentes a un usuario específico, seleccione el usuario y visualice las políticas en la ventana inferior.

Especificación de la configuración del dispositivo

Dentro de la aplicación Dispositivos, puede especificar la configuración disponible para cualquier dispositivo incorporado o conectado reconocido por HP ProtectTools Security Manager.

Huellas digitales

La página Huellas digitales tiene tres fichas: Registro, Sensibilidad y Avanzadas.

Registro

Puede elegir la cantidad mínima y máxima de huellas digitales que se le permite registrar a un usuario.

También puede borrar todos los datos del lector de huellas digitales.

△ **PRECAUCIÓN:** La eliminación de todos los datos del lector de huellas digitales borra todos los datos de las huellas digitales de todos los usuarios, incluyendo a los administradores. Si la política de inicio de sesión requiere sólo huellas digitales, puede evitar que todos los usuarios inicien sesión en el equipo.

Sensibilidad

Para ajustar la sensibilidad utilizada por el lector de huellas digitales cuando escanea sus huellas digitales, mueva el control deslizante.

Si su huella digital no se reconoce uniformemente, puede ser necesaria una configuración de menor sensibilidad. Una configuración mayor aumenta la sensibilidad a las variaciones en los escaneos de las huellas digitales y, por lo tanto, disminuye la posibilidad de una aceptación falsa. La configuración Media-Alta brinda una buena combinación de seguridad y comodidad.

Avanzadas

Puede configurar el lector de huellas digitales para ahorrar energía cuando el equipo está funcionando con batería.

Smart Card

Puede configurar el equipo para que se bloquee automáticamente cuando se retire una Smart Card. Sin embargo, el equipo se bloqueará sólo si se utilizó la Smart Card como credencial de autenticación cuando se inicia la sesión de Windows. La extracción de una Smart Card que no se utilizó para iniciar la sesión de Windows no bloqueará el equipo.

▲ Seleccione la casilla de verificación para activar o desactivar el bloqueo cuando se retire una Smart Card.

Rostro

Es posible definir el nivel de seguridad de Face Recognition para equilibrar la facilidad de uso y la dificultad para violar la seguridad del equipo.

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

3. Para obtener mayor practicidad, haga clic en el control deslizante para moverlo hacia la izquierda, o para obtener mayor precisión, haga clic en el control deslizante para moverlo hacia la derecha.

   - **Practicidad**: para facilitar que los usuarios registrados logren acceder en situaciones marginales, haga clic en la barra deslizante para mover el control deslizante a la posición **Practicidad**.
   - **Equilibrio**: para brindar un buena simetría entre seguridad y capacidad de uso, o si tiene información delicada o su equipo se encuentra en un área donde pueden producirse intentos de iniciar sesión sin autorización, haga clic en la barra deslizante para mover el control deslizante a la posición **Equilibrio**.
   - **Precisión**: para dificultar que un usuario logre acceder si las escenas de registro o las condiciones de iluminación actuales son inferiores a las normales y es menos probable que se produzca una falsa aceptación, haga clic en la barra deslizante para mover el control deslizante a la posición **Precisión**.

NOTA: El nivel de Seguridad se aplica a todos los usuarios

4. Haga clic en **Aplicar**.

Configuración avanzada

1. Haga clic en **Inicio**, **Todos los programas**, **HP** y luego en **Consola administrativa de HP ProtectTools**.
2. Haga clic en **Dispositivos** y a continuación haga clic en **Rostro**.
3. Haga clic en **Avanzadas**.
   - **No se requiere nombre de usuario para iniciar sesión en Windows.**
     - Seleccione la casilla de verificación para permitir que los usuarios inicien sesión en Windows sin un nombre de usuario.
     - Desmarque la casilla de verificación para requerir un nombre de usuario para iniciar sesión.
   - **Haga obligatorio el uso de un PIN para iniciar sesión mediante el reconocimiento de rostros**: seleccione la casilla de verificación para requerir que cada usuario configure y utilice un PIN (número de identificación personal) para iniciar sesión.
     - **Extensión mínima permitida para el PIN**: haga clic en la flecha hacia arriba para aumentar o la flecha hacia abajo para disminuir la cantidad mínima de caracteres requeridos para el PIN.
     - **Extensión máxima permitida para el PIN**: haga clic en la flecha hacia arriba para aumentar o la flecha hacia abajo para disminuir la cantidad máxima de caracteres permitidos para el PIN.
     - **Número máximo de intentos permitidos para el PIN**: haga clic en la flecha hacia arriba para aumentar o la flecha hacia abajo para disminuir la cantidad máxima de veces que puede reingresarse el PIN.
4. Haga clic en **Aceptar**.

5 Configuración de sus aplicaciones

Al grupo de Aplicaciones se accede desde el panel del menú Aplicaciones de seguridad a la izquierda de la Consola administrativa de HP ProtectTools. Puede utilizar Configuración para personalizar el comportamiento de las aplicaciones de HP ProtectTools Security instaladas actualmente.

Para editar la configuración de su aplicación:

1. En el menú Herramientas, en el grupo **Aplicaciones**, haga clic en **Configuración**.
2. Haga clic para activar o desactivar una configuración específica.
3. Haga clic en **Aplicar** para guardar los cambios realizados.

Ficha General

Las siguientes configuraciones están disponibles en la ficha General:

- **No iniciar automáticamente el asistente de configuración para administradores**: seleccione esta opción para evitar que el asistente se abra automáticamente al realizar el inicio de sesión.
- **No iniciar automáticamente el asistente de Pasos iniciales para usuarios**: seleccione esta opción para evitar que la configuración de usuario se abra automáticamente al realizar el inicio de sesión.

Ficha Aplicaciones

La configuración que se muestra aquí puede cambiar cuando se agregan nuevas aplicaciones a Security Manager. La configuración mínima que se muestra en forma predeterminada es la siguiente:

- **Estado de las aplicaciones**: permite visualizar el estado de todas las aplicaciones.
- **Administrador de contraseñas**: activa la aplicación Administrador de contraseñas para todos los usuarios del equipo.
- **Privacy Manager**: activa la aplicación Privacy Manager para todos los usuarios de este equipo.
- **Activar el botón Descubrir más**: permite que todos los usuarios de este equipo agreguen aplicaciones a HP ProtectTools Security Manager haciendo clic en el botón **[+] Descubrir más**.

Para volver todas las aplicaciones a la configuración predeterminada de fábrica, haga clic en el botón **Restaurar valores predeterminados**.

6 Herramientas de administración

Puede que haya disponibles aplicaciones adicionales para agregar nuevas herramientas de administración a Security Manager. El administrador de este equipo puede desactivar este recurso a través de la aplicación de Configuración.

Para agregar herramientas de administración adicionales, haga clic en **[+] Herramientas de administración**.

Actualizaciones y mensajes

Si se dispone de una conexión a Internet, puede acceder al sitio Web de DigitalPersona http://www.digitalpersona.com/ para consultar sobre nuevas aplicaciones o configurar un programa de actualizaciones automáticas.

1. Para solicitar información sobre nuevas aplicaciones y actualizaciones, seleccione la casilla de verificación de **Manténgame informado sobre las nuevas aplicaciones y actualizaciones.**
2. Para definir un calendario para actualizaciones automáticas, seleccione el número de días.
3. Para verificar si hay actualizaciones, haga clic en **Verificar ahora**.

7 HP ProtectTools Security Manager

HP ProtectTools Security Manager le permite aumentar de forma considerable la seguridad de su equipo.

Puede utilizar las aplicaciones de Security Manager precargadas, así como también las aplicaciones adicionales disponibles para descarga inmediata de la Web:

- Administre su inicio de sesión y contraseñas
- Cambie fácilmente su contraseña del sistema operativo Windows®
- Configure preferencias de programas
- Utilice huellas digitales para mayor seguridad y comodidad
- Registre una o más escenas para autenticación
- Configure una Smart Card para autenticación
- Realice copias de seguridad y restaure los datos de sus programas
- Agregue más aplicaciones

Abrir HP ProtectTools Security Manager

Puede abrir HP ProtectTools Security Manager de cualquiera de las formas siguientes:

- Haga clic en **Inicio**, **Todos los programas**, **HP** y en **HP ProtectTools Security Manager**.
- Haga doble clic en el icono de **HP ProtectTools** en el área de notificación, en el extremo derecho de la barra de tareas.
- Haga clic con el botón derecho en el icono **HP ProtectTools**, y haga clic en **Abrir HP ProtectTools Security Manager**.
- Haga clic en el dispositivo **Tarjeta de identificación de Security Manager** en la barra lateral de Windows.
- Presione la combinación de teclas de acceso rápido ctrl+Windows+h para abrir el menú Enlaces rápidos de Security Manager.

Uso del panel de control de Security Manager

El panel de control de Security Manager es la ubicación central para el acceso fácil a los recursos, las aplicaciones y configuraciones de Security Manager.

▲ Para abrir el panel de Security Manager, haga clic en **Inicio**, **Todos los programas**, **HP** y en **HP ProtectTools Security Manager**.

El panel de control está compuesto por los siguientes componentes:

- **Tarjeta de identificación**: muestra el nombre de usuario de Windows y una foto seleccionada que identifica la cuenta de usuario con sesión iniciada.
- **Aplicaciones de seguridad**: muestra un menú que se expande con enlaces para configurar las siguientes categorías de seguridad:
  - **Credential Manager**
  - **Mis datos**
- **Descubrir más**: abre una página en la que puede encontrar aplicaciones adicionales para mejorar la seguridad de su identidad, sus datos y sus comunicaciones.
- **Área principal**: muestra pantallas específicas para aplicaciones.
- **Administración**: abre la Consola administrativa de HP ProtectTools.
- **Botón de Ayuda**: muestra información acerca de la pantalla actual.
- **Avanzadas**: le permite acceder a las siguientes opciones:
  - **Preferencia**: le permite personalizar las configuraciones de Security Manager.
  - **Copia de seguridad y restauración**: le permite efectuar copias de seguridad o restaurar datos.
  - **Acerca de**: muestra la información de la versión acerca de Security Manager.

Procedimientos de configuración

Registro de credenciales

Se puede utilizar la página Mi identidad para registrar sus diversos métodos de autenticación o sus credenciales. Después de haberse registrado, puede utilizar estos métodos para iniciar la sesión en Security Manager.

Registro de sus huellas digitales

Si su equipo tiene incorporado o conectado un lector de huellas digitales, el asistente de configuración de HP ProtectTools Security Manager lo guiará por el proceso de configurar o de “registrar” sus huellas digitales.

1. Se muestra un diagrama de dos manos. Los dedos que ya están registrados aparecen resaltados en verde. Haga clic en un dedo del diagrama.

   NOTA: Para eliminar una huella digital registrada anteriormente, haga clic en el dedo correspondiente.

2. Una vez que haya seleccionado un dedo para registrar, se le pide que escanee el dedo hasta que su huella digital se registre satisfactoriamente. Se resalta un dedo registrado con el contorno verde.

3. Debe registrar por lo menos dos dedos, se prefieren los dedos índice o medio. Repita los pasos 1 a 3 para otro dedo.

4. Haga clic en **Siguiente** y siga las instrucciones que aparecen en la pantalla.

NOTA: Cuando registre huellas digitales a través del proceso de Pasos iniciales, la información de la huella digital no se guarda hasta que haga clic en **Siguiente**. Si deja el equipo inactivo por un momento, o cierra el programa, los cambios que efectuó **no** se guardan.

Registro de escenas

Debe registrar una o más escenas con el fin de usar el inicio de sesión mediante reconocimiento de rostros.

Para registrar una nueva escena desde el asistente de configuración de HP ProtectTools Security Manager:

1. Haga clic en el icono de **HP ProtectTools Security Manager** en la barra lateral a la derecha de la pantalla.

2. Escriba su contraseña de Windows® y haga clic en **Siguiente**.

3. En **Active los recursos de seguridad**, seleccione la casilla de verificación **Seguridad de inicio de sesión en Windows** y luego haga clic en **Siguiente**.

4. En **Elija sus credenciales**, seleccione la casilla de verificación **Rostro** y luego haga clic en **Siguiente**.

5. Haga clic en **Registrar una nueva escena**.

Una vez que se haya registrado de forma satisfactoria, también puede registrar una nueva escena en caso de que haya tenido dificultad durante el inicio de sesión debido a que ocurrió una o más de las siguientes situaciones:

- Su rostro ha cambiado de forma significativa desde su último registro.
- La iluminación es muy diferente a la de cualquiera de sus registros anteriores.
- Llevaba puestos anteojos (o no) durante su último registro.

NOTA: Si tiene dificultades para registrar escenas, pruebe a acercarse a la cámara web. Al igual que en cualquier tipo de fotografía o vídeo, la iluminación y el contraste son extremadamente importantes. Asegúrese de que en su sesión la iluminación sea principalmente de primer plano, no de fondo. Si Face Recognition no lo autentica fácilmente, usted puede volver a registrar su escena en mejores condiciones de iluminación.

Para registrar una nueva escena desde HP ProtectTools Security Manager:

1. Haga clic en **Inicio**, **Todos los programas**, **HP** y en **HP ProtectTools Security Manager**.
2. Haga clic en **Credenciales** y a continuación haga clic en **Rostro**.
3. Haga clic en **Registrar una nueva escena**.

Configuración de usuario avanzado

1. Haga clic en **Inicio**, **Todos los programas** y entonces en **HP ProtectTools Security Manager**.
2. Haga clic en **Configurar sus credenciales de autenticación** y a continuación haga clic en **Rostro**.
3. Haga clic en el botón **Avanzado**, y seleccione a partir de las siguientes opciones.

   a. Para requerir el uso de un PIN para el inicio de sesión mediante reconocimiento de rostros, haga clic en **Crear PIN**, ingrese su contraseña de Windows, escriba el nuevo PIN y luego confirme el nuevo PIN reingresándolo.

   b. Seleccione una configuración adicional, si lo desea. Esta configuración se aplica sólo al usuario actual:

   - **Reproducir sonido en los eventos de reconocimiento de rostros**
     - Seleccione la casilla de verificación para reproducir un sonido cuando el reconocimiento de rostros se realiza con éxito o falla.
     - Desmarque la casilla de verificación para desactivar esta opción.
   - **Solicitar actualizar las escenas cuando falla el inicio de sesión**
     - Seleccione la casilla de verificación para permitir que un usuario actualice escenas si el reconocimiento de rostros falla. Si la verificación llega al umbral de "quizás", se solicita al usuario que decida si inserta las imágenes en vivo en el inicio de sesión "fallido" para la escena actual con el fin de aumentar la posibilidad de un inicio de sesión con éxito la próxima vez.
     - Desmarque la casilla de verificación para desactivar esta opción.
   - **Solicitar registrar una escena nueva cuando falla el inicio de sesión**
     - Seleccione la casilla de verificación para mostrar una solicitud para que el usuario registre una nueva escena si el inicio de sesión mediante reconocimiento de rostros falla y la verificación no llega al umbral de “quizás”. Esto puede aumentar la posibilidad de un inicio de sesión con éxito la próxima vez.
     - Desmarque la casilla de verificación para desactivar esta opción.

   c. Para registrar una nueva escena, haga clic en **Registrar una nueva escena** y luego siga las instrucciones que aparecerán en la pantalla.

Cambio de su contraseña de Windows

Con Security Manager es más fácil y más rápido cambiar su contraseña de Windows que hacerlo a través del Panel de control de Windows.

Para cambiar su contraseña de Windows, siga estos pasos:

1. En el panel de control de Security Manager, haga clic en **Credenciales** y luego haga clic en **Contraseña**.
2. Escriba su contraseña actual en el cuadro de texto **Contraseña de Windows actual**.

3. Escriba una nueva contraseña en el cuadro de texto **Contraseña de Windows nueva** y luego vuelva a escribirla en el cuadro de texto **Confirmar nueva contraseña**.

4. Haga clic en **Cambiar** para cambiar inmediatamente su contraseña actual por la nueva que introdujo.

Configuración de una smart card

Si elige el inicio de sesión con Smart Card y hay un lector de Smart Card incorporado o conectado a su equipo, el asistente de configuración de Security Manager le pide que configure un PIN (número de identificación personal) de Smart Card.

Para configurar un PIN de Smart Card:

1. En **Configurar Smart Card**, introduzca y confirme un PIN.

   También puede cambiar su PIN. Escriba su PIN actual y luego introduzca uno nuevo.

2. Para continuar, haga clic en **Siguiente** y siga las instrucciones que aparecen en la pantalla.

– o –

▲ En el panel de control de Security Manager, haga clic en **Credenciales** y luego haga clic en **Smart Card**.

- Para configurar un PIN de Smart Card: en **Configurar Smart Card**, escriba y confirme un PIN.
- Para cambiar su PIN: primero escriba su PIN actual y luego introduzca y confirme uno nuevo.

Tareas generales

Las aplicaciones incluidas en este grupo lo ayudan a administrar distintos aspectos de su identidad digital.

- **Security Manager**: crea y administra Enlaces rápidos, que le permite iniciar y hacer inicio de sesión en sitios Web y en programas autenticándose con su contraseña de Windows, su huella digital o con una smart card.
- **Credenciales**: brinda un medio para cambiar fácilmente su contraseña de Windows, registrar sus huellas digitales o configurar una smart card.

Para agregar más aplicaciones, haga clic en el botón **Descubrir más** [+] en el ángulo inferior izquierdo del panel de control. Este botón puede desactivarlo el administrador.

Administrador de contraseñas

Iniciar sesión en Windows, sitios Web y aplicaciones es más fácil y más seguro cuando utiliza su Administrador de contraseñas. Puede utilizarlo para crear contraseñas más fuertes que no tiene que anotar o recordar y luego iniciar sesión fácil y rápidamente con una huella digital, Smart Card o su contraseña de Windows.

El Administrador de contraseñas ofrece las siguientes opciones:

- Agregue, edite o elimine inicios de sesión desde la ficha Administrar.
- Utilice los Enlaces rápidos para abrir su navegador predeterminado e iniciar sesión en un sitio Web o programa, una vez que se haya configurado.
- Arrastre y suelte para organizar sus Enlaces rápidos en categorías.
- Consulte de un vistazo si alguna de sus contraseñas representa un riesgo de seguridad y genere automáticamente una contraseña fuerte compleja para utilizar en sitios nuevos.

Muchos recursos del Administrador de contraseñas también están disponibles en el icono del Administrador de contraseñas que se muestra cuando una página web o una pantalla de inicio de sesión de un programa tiene el foco. Haga clic en el icono para mostrar un menú de contexto en el que pueda elegir entre las siguientes opciones.

Para páginas web o programas donde no se haya creado aún el inicio de sesión

Las siguientes opciones se muestran en el menú de contexto:

- **Agregar [algúndominio.com] al Administrador de contraseñas**: le permite agregar un inicio de sesión para la pantalla de inicio de sesión actual.
- **Abrir Administrador de contraseñas**: abre el Administrador de contraseñas.
- **Configuraciones del icono**: le permite especificar las condiciones en las que aparece el icono del Administrador de contraseñas.
- **Ayuda**: muestra la Ayuda del software Administrador de contraseñas.

Para páginas web o programas donde ya se haya creado el inicio de sesión

Las siguientes opciones se muestran en el menú de contexto:

- **Completar datos de inicio de sesión**: coloca sus datos de inicio de sesión en los campos de inicio de sesión y luego envía la página (si se especificó el envío cuando se creó o editó por última vez el inicio de sesión).
- **Editar inicio de sesión**: le permite editar sus datos de inicio de sesión para este sitio Web.
- **Agregar una cuenta nueva**: le permite agregar una cuenta a un inicio de sesión.
- **Abrir Administrador de contraseñas**: abre la aplicación Administrador de contraseñas.
- **Ayuda**: muestra la Ayuda del software Administrador de contraseñas.

NOTA: El administrador de este equipo puede haber configurado Security Manager para requerir más de una credencial cuando verifica su identidad.

Adición de inicios de sesión

Puede agregar con facilidad un inicio de sesión a un sitio web o a un programa ingresando la información de inicio de sesión. Desde que se inicia sesión, el Administrador de contraseñas ingresa automáticamente la información. Puede usar estos inicios de sesión después de navegar por un sitio Web o de usar un programa, o de hacer clic en un inicio de sesión en el menú **Inicios de sesión** para que el Administrador de contraseñas abra el sitio web o el programa y realice el inicio 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 flecha en el icono del **Administrador de contraseñas** y luego haga clic en una de las siguientes opciones, dependiendo de que la pantalla de inicio de sesión sea para un sitio Web o para un programa:
   - Para un sitio Web, haga clic en **Agregar [nombre de dominio] al Administrador de contraseñas**.
   - Para un programa, haga clic en **Agregar esta pantalla de inicio de sesión al Administrador de contraseñas**.
3. Escriba sus datos de inicio de sesión. Los campos de inicio de sesión en la pantalla y sus campos correspondientes en el cuadro de diálogo se identifican con un borde naranja en negrita. También puede mostrar este cuadro de diálogo haciendo clic en **Agregar inicio de sesión** en la ficha **Administrador de contraseñas**. Algunas opciones dependen de los dispositivos de seguridad conectados al equipo; por ejemplo, la utilización de las teclas de acceso rápido ctrl+Windows+h, el escaneo de su huella digital o la inserción de una Smart Card.
   a. Para completar un campo de inicio de sesión con una de las opciones formateadas previamente, haga clic en las flechas a la derecha del campo.
   b. Para ver la contraseña para este inicio de sesión, haga clic en **Mostrar contraseña**.
   c. Para tener los campos de inicio de sesión completados, pero no enviados, desmarque la casilla de verificación **Enviar de forma automática los datos para el inicio de sesión**.
   d. Haga clic en **Aceptar**, en el método de autenticación que desee utilizar: **Huellas digitales**, **Contraseña** o **Rostro** y luego inicie sesión con el método de autenticación deseado.

El signo más (+) se elimina del icono del Administrador de contraseñas para notificarle que se creó el inicio de sesión.

e. Si el Administrador de contraseñas no detecta los campos de inicio de sesión, haga clic en **Más campos**.

   i. Seleccione la casilla de verificación para cada campo que se necesita para el inicio de sesión o desmarque la casilla de verificación de los campos que no se requieren para el inicio de sesión.

   ii. Si el Administrador de contraseñas no puede detectar todos los campos de inicio de sesión aparece un mensaje que le pregunta si desea continuar. Haga clic en **Sí**.

   iii. Aparece un diálogo con sus campos de inicio de sesión completados. Haga clic en el icono para cada campo y arrástrelo hasta el campo de inicio de sesión correspondiente y luego haga clic en el botón para ingresar en el sitio Web.

   NOTA: Una vez que utilice el modo manual para ingresar los datos del inicio de sesión para un sitio, debe continuar utilizando este método para iniciar sesión en el mismo sitio Web en el futuro.

   NOTA: El modo manual de ingresar datos de inicio de sesión está disponible sólo con Internet Explorer 8.

   iv. Haga clic en **Cerrar**.

Cada vez que acceda a ese sitio Web o abra ese programa, aparecerá el icono del administrador de contraseñas, lo que indica que puede utilizar sus credenciales registradas para iniciar sesión.

Edición de inicios de sesión

Para editar un inicio de sesión, siga estos pasos:

1. Abra la pantalla de inicio de sesión para un sitio Web o programa.
2. Para mostrar un cuadro de diálogo donde puede editar su información de inicio de sesión, haga clic en la flecha en el icono del **Administrador de contraseñas** y luego haga clic en **Editar inicio de sesión**. Los campos de inicio de sesión en la pantalla y sus campos correspondientes en el cuadro de diálogo se identifican con un borde naranja en negrita.

   También puede mostrar este cuadro de diálogo haciendo clic en **Editar para el inicio de sesión deseado** en la ficha **Administrador de contraseñas**.
3. Edite su información de inicio de sesión.
   - Para completar un campo de inicio de sesión con una de las opciones formateadas previamente, haga clic en las flechas a la derecha del campo.
   - Para agregar campos adicionales de la pantalla a su inicio de sesión, haga clic en **Más campos**.
   - Para tener los campos de inicio de sesión completados, pero no enviados, desmarque la casilla de verificación **Enviar datos de inicio de sesión**.
   - Para ver la contraseña para este inicio de sesión, haga clic en **Mostrar contraseña**.
4. Haga clic en **Aceptar**.

Uso del menú de Inicios de sesión

El Administrador de contraseñas ofrece una forma rápida y fácil de abrir los sitios Web y los programas para los que creó inicios de sesión. Haga doble clic en el inicio de sesión de un programa o sitio Web en el menú **Inicios de sesión**, o la ficha **Administrar** en **Administrador de contraseñas**, para abrir la pantalla de inicio de sesión y luego complete sus datos de inicio de sesión.

Cuando crea un inicio de sesión, se agrega automáticamente a su menú del Administrador de contraseñas.

Para mostrar el menú Inicios de sesión:

1. Presione la combinación de teclas de acceso rápido del **Administrador de contraseñas**. ctrl +Windows+h es la configuración de fábrica. Para cambiar la combinación de las teclas de acceso rápido, haga clic en **Administrador de contraseñas** y luego en **Configuración**.
2. Escanee su huella digital (en equipos con un lector de huellas digitales incorporado o conectado).

Organización de inicios de sesión en categorías

Utilice categorías para mantener sus inicios de sesión en orden creando una o más categorías. Luego arrastre y suelte sus inicios de sesión en las categorías deseadas.

Para agregar una categoría:

1. En el panel de control de Security Manager, haga clic en **Administrador de contraseñas**.
2. Haga clic en la ficha **Administrar** y luego haga clic en **Agregar categoría**.
3. Introduzca 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 deseado.
2. Mantenga presionado el botón izquierdo del mouse.
3. Arrastre el inicio de sesión a la lista de categorías. Las categorías se resaltarán cuando mueva el cursor sobre ellas.
4. Libere el botón del mouse cuando se resalte la categoría deseada.

Sus inicios de sesión no se mueven a la categoría, sino que sólo se copian a la categoría seleccionada. Puede agregar el mismo inicio de sesión a más de una categoría y puede mostrar todos los inicios de sesión haciendo clic en **Todos**.

Administración de sus inicios de sesión

El Administrador de contraseñas hace que sea fácil administrar nuestra información de inicio de sesión de acuerdo con nombres de usuario, contraseñas y múltiples cuentas de inicio de sesión, desde una ubicación central.

Sus inicios de sesión se listan en la ficha Administrar. Si se han creado varios inicios de sesión para el mismo sitio web, cada inicio de sesión se lista bajo el nombre del sitio web y se alinean en la lista de inicio de sesión.

Para administrar sus inicios de sesión:

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

- **Agregar inicio de sesión**: haga clic en **Agregar inicio de sesión** y siga las instrucciones que aparecen en la pantalla.
- **Editar inicio de sesión**: haga clic en un inicio de sesión, en **Editar** y luego cambie los datos de inicio de sesión.
- **Eliminar inicio de sesión**: haga clic en un inicio de sesión, y luego en **Eliminar**.

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

1. Abra la pantalla de inicio de sesión para el sitio Web o programa.
2. Haga clic en el icono del **Administrador de contraseñas** para mostrar su menú de acceso directo.
3. Haga clic en **Agregar inicio de sesión adicional** y siga las instrucciones en la pantalla.

Evaluación de la seguridad de su contraseña

La utilización de contraseñas sólidas para sus sitios Web y programas es un aspecto importante de la protección de su identidad.

El Administrador de contraseñas facilita la supervisión y la mejoría de su seguridad con un análisis instantáneo y automatizado de la solidez de cada una de las contraseñas utilizadas para iniciar sesión en sus sitios Web y programas.

Configuración del icono del Administrador de contraseñas

El Administrador de contraseñas intenta identificar las pantallas de inicio de sesión para los sitios Web y programas. Cuando detecta una pantalla de inicio de sesión para la que no creó un inicio de sesión, el Administrador de contraseñas le pide que agregue un inicio de sesión para la pantalla mostrando el icono del Administrador de contraseñas con un signo "+".

Haga clic en la flecha del icono, y luego en **Configuraciones del icono** para personalizar la forma en que el **Administrador de contraseñas** maneja los sitios de inicio de sesión posibles.

- **Solicitud para agregar inicios de sesión para las pantallas de inicio de sesión**: haga clic en esta opción para que el Administrador de contraseñas le pida agregar un inicio de sesión cuando una pantalla de inicio de sesión muestra que todavía no tiene una configuración de inicio.
- **Excluir esta pantalla**: seleccione la casilla de verificación de modo que el Administrador de contraseñas no le solicite de nuevo que añada un inicio de sesión para esta pantalla de inicio de sesión.

Para acceder a las configuraciones adicionales del Administrador de contraseñas, haga clic en **Administrador de contraseñas** y entonces en **Configuración** en el panel de control de Security Manager.

Configuración

Puede especificar configuraciones para personalizar HP ProtectTools Security Manager:

1. **Solicitud para agregar inicios de sesión para las pantallas de inicio de sesión**: el icono del Administrador de contraseñas con un signo más aparece cada vez que se detecta una pantalla de inicio de sesión de un sitio Web o programa, lo que indica que puede agregar un inicio de sesión para esta pantalla a la bóveda de contraseñas. Para desactivar este recurso, en el cuadro de diálogo **Configuraciones del icono**, desmarque la casilla de verificación que está al lado de **Solicitud para agregar inicios de sesión para las pantallas de inicio de sesión**.
2. **Abra el Administrador de contraseñas con ctrl+Windows+h**: las teclas de acceso rápido predeterminadas que abren el menú Enlaces rápidos del Administrador de contraseñas son ctrl +Windows+h. Para cambiar las teclas de accedo rápido, haga clic en esta opción e introduzca una nueva combinación de teclas. Las combinaciones pueden incluir una o más de las siguientes teclas: ctrl, alt o mayús, y cualquier tecla del alfabeto o numérica.
3. Haga clic en **Aplicar** para guardar los cambios.

Credenciales

Utiliza sus credenciales de Security Manager para verificar que realmente es usted. El administrador local de este equipo puede configurar cuáles credenciales pueden utilizarse para probar su identidad cuando inicia sesión en su cuenta de Windows, sitios Web o programas.

Las credenciales disponibles pueden variar según los dispositivos de seguridad incorporados o conectados al equipo. Cada credencial admitida tendrá una entrada en el grupo **Mi identidad, Credenciales**.

Se enumeran las credenciales disponibles, los requisitos y el estado actual y puede incluir lo siguiente:

- Huellas digitales
- Contraseña
- Smart Card
- Rostro

Para registrar o cambiar una credencial, haga clic en el enlace y siga las instrucciones que aparecerán en la pantalla.

Su tarjeta de identificación personal

Su tarjeta de identificación lo identifica de forma única como el propietario de esta cuenta de Windows, muestra su nombre y una imagen de su elección. Se muestra visiblemente en el ángulo superior izquierdo de las páginas de Security Manager, y como un dispositivo de barra lateral de Windows.

Hacer clic en su tarjeta de identificación en la barra lateral de Windows es una de las muchas formas de obtener acceso rápido a Security Manager.

Puede cambiar la imagen y la forma en la que aparece su nombre. De forma predeterminada, se muestran su nombre de usuario de Windows completo y la imagen que seleccionó durante la configuración de Windows.

Para cambiar el nombre que se muestra:

1. En el panel de control de Security Manager, haga clic en el icono **Tarjeta de identificación** en el ángulo superior izquierdo.
2. Haga clic en la casilla de verificación que muestra el nombre que usted ingresó en su cuenta en Windows. El sistema mostrará su nombre de usuario en Windows para esta cuenta.
3. Para cambiar este nombre, escriba el nombre nuevo y luego haga clic en el botón **Guardar**.

Para cambiar la imagen que se muestra:

1. En el panel de control de Security Manager, haga clic en la **Tarjeta de identificación** en el ángulo superior izquierdo.
2. Haga clic en el botón **Elegir imagen**, haga clic en una imagen y a continuación haga clic en el botón **Guardar**.

Configuración de sus preferencias

Puede personalizar las configuraciones para HP ProtectTools Security Manager. En el panel de control de Security Manager, haga clic en **Avanzado** y luego haga clic en **Preferencias**. Las configuraciones disponibles se muestran en dos fichas: General y Huella digital.

General

Las siguientes configuraciones están disponibles en la ficha General:

Apariencia: **muestra el icono en la barra de tarea**

- Para activar la visualización del icono en la barra de tareas, seleccione la casilla de verificación.
- Para desactivar la visualización del icono en la barra de tareas, desmarque la casilla de verificación.

Huella digital

Las siguientes configuraciones están disponibles en la ficha Huella digital:

- **Quick Actions (Acciones rápidas)**: utilice Quick Actions para seleccionar la tarea de Security Manager que realizará cuando mantenga presionada una tecla designada mientras escanea su huella digital.

  Para asignar una Quick Action a una de las teclas indicadas, haga clic en una opción **(Tecla) +Huella digital** y luego seleccione una de las tareas disponibles en el menú.

- **Fingerprint Scan Feedback (Respuesta de escaneo de huella digital)**: aparece sólo cuando se dispone de un lector de huellas digitales. Utilice esta configuración para ajustar la respuesta que se produce cuando escanea su huella digital.

  - **Activar respuesta de sonido**: Security Manager le da una respuesta de audio cuando se escanea una huella digital, reproduciendo diferentes sonidos para eventos específicos del programa. Puede asignar nuevos sonidos a estos eventos a través de la ficha Sonido en el Panel de control de Windows o desactivar la respuesta de sonido desmarcando esta opción.

  - **Mostrar respuesta sobre la calidad del escaneo**

    Para mostrar todos los escaneos, independientemente de la calidad, seleccione la casilla de verificación.

    Para mostrar sólo los escaneos de buena calidad, seleccione la casilla de verificación.

Realización de copias de seguridad y restauración de sus datos

Se recomienda efectuar copias de seguridad de sus datos de Security Manager de forma periódica. La frecuencia con la que realice copias de seguridad depende de la frecuencia con la que cambian los datos. Por ejemplo, si agrega nuevos inicios de sesión todos los días, probablemente deba realizar copias de seguridad de sus datos diariamente.

Las copias de seguridad también pueden utilizarse para migrar de un equipo a otro, también denominado importación y exportación.

NOTA: Sólo se pueden realizar copias de seguridad de los datos con este recurso.

HP ProtectTools Security Manager debe estar instalado en cualquier equipo que deba recibir copias de seguridad de datos antes de que los datos puedan restaurarse desde el archivo de copia de seguridad.

Para realizar una copia de seguridad de sus datos:

1. En el panel izquierdo haga clic en **Avanzadas**, y luego en **Copias de seguridad y restauración**.
2. Haga clic en **Copia de seguridad de datos**.
3. Seleccione los módulos que desea incluir en la copia de seguridad. En la mayoría de los casos, deseará seleccionar todos.
4. Introduzca un nombre para el archivo de almacenamiento. De forma predeterminada, el archivo se guardará en su carpeta de Documentos. Haga clic en **Examinar** para especificar una ubicación diferente.
5. Introduzca una contraseña para proteger el archivo.

6. Verifique su identidad.
7. Haga clic en **Finalizar**.

Para restaurar sus datos:

1. En el panel izquierdo haga clic en **Avanzadas**, y luego en **Copias de seguridad y restauración**.
2. Haga clic en **Restaurar datos**.
3. Seleccione el archivo de almacenamiento creado anteriormente. Puede escribir la ruta en el campo provisto, o hacer clic en **Explorar**.
4. Introduzca la contraseña utilizada para proteger el archivo.
5. Seleccione los módulos cuyos datos desea restaurar. En la mayoría de los casos, serán todos los módulos enumerados.
6. Haga clic en **Finalizar**.

Descubrir más

Puede que haya disponibles aplicaciones adicionales que brindan nuevos recursos para este programa.

en el panel de control de Security Manager, haga clic en **[+] Descubrir más** para buscar más aplicaciones.

NOTA: Si no hay un enlace a **[+] Descubrir más** en la sección inferior izquierda del panel de control, este ha sido desactivado por el administrador del equipo.

Actualizaciones y mensajes

1. Para solicitar información sobre nuevas aplicaciones y actualizaciones, seleccione la casilla de verificación de **Manténgame informado sobre las nuevas aplicaciones y actualizaciones.**
2. Para definir un calendario para actualizaciones automáticas, seleccione el número de días.
3. Para verificar si hay actualizaciones, haga clic en **Verificar ahora**.

Estado de las aplicaciones de seguridad

La página de estado de las aplicaciones de Security Manager muestra el estado general de sus aplicaciones de seguridad instaladas. La página muestra las aplicaciones que están configuradas y el estado de configuración de cada una. El resumen aparece automáticamente cuando abre el panel de control de Security Manager y hace clic en **Verifique el estado de las aplicaciones de seguridad**, al hacer clic en **Aplicaciones de seguridad** o al hacer clic en **Verificar ahora** en el icono **Dispositivo**, en la barra lateral de Windows en el extremo derecho de la pantalla.

8 Drive Encryption for HP ProtectTools (sólo en algunos modelos)

△ **PRECAUCIÓN:** Si decide desinstalar el módulo Drive Encryption, primero debe desencriptar todas las unidades encriptadas. Si no lo hace, no podrá acceder a los datos de las unidades encriptadas a menos que se haya registrado en el Servicio de recuperación de Drive Encryption. La reinstalación del módulo Drive Encryption no le permitirá acceder a las unidades encriptadas.

Drive Encryption for HP ProtectTools brinda completa protección de datos al encriptar la unidad de disco duro de su equipo. 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 el sistema operativo Windows®.

El asistente de configuración de HP ProtectTools les permite a los administradores de Windows activar Drive Encryption, hacer una copia de seguridad de la clave de encriptación, agregar y eliminar usuarios y desactivar Drive Encryption. Para obtener más información, consulte la ayuda del software HP Protect Tools Security Manager.

Es posible realizar las siguientes tareas con Drive Encryption:

- Administración de encriptación

  Encriptación o desencriptación de unidades individuales

  NOTA: Solamente se pueden encriptar las unidades de disco duro internas.

- Recuperación
  - Creación de claves de la copia de seguridad
  - Realización de una recuperación

Procedimientos de configuración

Apertura de Drive Encryption

1. Haga clic en **Inicio**, **Todos los programas**, **HP** y luego en **Consola administrativa de HP ProtectTools**.
2. En el panel izquierdo, haga clic en **Drive Encryption**.

Tareas generales

Activación de Drive Encryption

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

NOTA: Este asistente también se utiliza para agregar y eliminar usuarios.

- o -

1. Haga clic en **Inicio**, **Todos los programas**, **HP** y luego en **Consola administrativa de HP ProtectTools**.
2. En el panel izquierdo, haga clic en **Seguridad**, y luego haga clic en **Recursos**.
3. Seleccione la casilla de verificación **Drive Encryption** y entonces haga clic en **Siguiente**.
4. En **Unidades que se encriptarán**, seleccione la casilla de verificación de la unidad de disco duro que desea encriptar.
5. Inserte el dispositivo de almacenamiento en la ranura adecuada.

   NOTA: Para guardar la clave de encriptación, debe usar un dispositivo de almacenamiento USB con formato FAT32.

6. En **Dispositivo de almacenamiento externo para guardar la clave de encriptación**, seleccione la casilla de verificación del dispositivo de almacenamiento donde se guardará la clave de encriptación.
7. Haga clic en **Aplicar**.

   Comienza la encriptación de la unidad.

Para obtener más información, consulte la ayuda del software HP Protect Tools Security Manager.

Desactivación de Drive Encryption

Use el asistente de configuración de HP ProtectTools para desactivar Drive Encryption. Para obtener más información, consulte la ayuda del software HP Protect Tools Security Manager.

- o -

1. Haga clic en **Inicio**, **Todos los programas**, **HP** y luego en **Consola administrativa de HP ProtectTools**.
2. En el panel izquierdo, haga clic en **Seguridad**, y luego haga clic en **Recursos**.
3. Desmarque la casilla de verificación **Drive Encryption** y luego haga clic en **Aplicar**.

   Comienza la desencriptación de la unidad.

Inicio de sesión después de la activación de Drive Encryption

Cuando encienda el equipo después de que se active Drive Encryption y su cuenta de usuario esté inscrita, debe iniciar sesión en la pantalla de inicio de sesión de Drive Encryption:

NOTA: Si el administrador de Windows activó la seguridad de inicio previo en HP ProtectTools Security Manager, iniciará la sesión en el equipo inmediatamente después del encendido, en lugar de hacerlo en la pantalla de inicio de sesión de Drive Encryption.

1. Haga clic en su nombre de usuario y escriba su contraseña de Windows o el PIN de la Java™ Card, o deslice un dedo cuya huella digital esté registrada.
2. Haga clic en **Aceptar**.

NOTA: Si utiliza una clave de recuperación para iniciar la sesión en la pantalla de inicio de sesión de Drive Encryption, también se le pedirá que seleccione su nombre de usuario y que escriba su contraseña de Windows en la pantalla de inicio de sesión de Windows.

Protección de sus datos mediante la encriptación de su unidad de disco duro

Use el asistente de configuración de HP ProtectTools para proteger sus datos mediante la encriptación de su unidad de disco:

1. En Security Manager, haga clic en **Pasos iniciales** y luego en el icono **Configuración de Security Manager**. Se inicia una demostración que describe los recursos de Security Manager. (También podrá iniciar Security Manager en la página de Drive Encryption.)
2. En el panel izquierdo, haga clic en **Drive Encryption**, y entonces haga clic en **Administración de encriptación**.
3. Haga clic en **Cambiar encriptación**.
4. Seleccione una o más unidades para encriptar.

NOTA: Se recomienda enfáticamente encriptar la unidad de disco duro.

Mostrar el estado de la encriptación

Los usuarios pueden visualizar el estado de encriptación en HP ProtectTools Security Manager.

NOTA: Los cambios en el estado de la encriptación de la unidad deben efectuarse utilizando la Consola administrativa de HP ProtectTools.

1. Abra **HP ProtectTools Security Manager**.
2. En **Mis datos**, haga clic en **Estado de la encriptación**.

   Si Drive Encryption está activo, el estado de la unidad muestra uno de los siguientes códigos de estado:

   - Activo
   - Inactivo
   - No encriptado
   - Encriptado
   - Encriptando
   - Desencriptando

Si la unidad de disco duro está en proceso de ser encriptada o desencriptada, una barra de progreso muestra el porcentaje completado y el tiempo restante para concluir la encriptación o desencriptación.

Tareas avanzadas

Administración de Drive Encryption (tarea de administrador)

La página Administración de encriptación permite que los administradores vean y cambien el estado de Drive Encryption (activo o inactivo) y que vean el estado de encriptación de todas las unidades de disco duro en el equipo.

- Si el estado es inactivo, el administrador aún no ha activado Drive Encryption en HP ProtectTools Security Manager y no está protegiendo la unidad de disco duro. Use el asistente de configuración de HP ProtectTools Security Manager para activar Drive Encryption.
- Si el estado es activo, se ha activado y configurado Drive Encryption. La unidad está en uno de los siguientes estados:
  - No encriptado
  - Encriptado
  - Encriptando
  - Desencriptando

Encriptación o desencriptación de unidades individuales

Para encriptar una o más unidades de disco duro en el equipo o desencriptar una unidad que ya se ha encriptado, use la función Cambiar encriptación:

1. Abra la **Consola administrativa de HP ProtectTools**, haga clic en **Drive Encryption** y entonces haga clic en **Administración de encriptación**.
2. Haga clic en **Cambiar encriptación**.
3. En el cuadro de diálogo Cambiar encriptación, seleccione o desmarque la casilla de verificación junto a cada unidad de disco duro que desea encriptar o desencriptar y luego haga clic en **Aceptar**.

NOTA: Cuando la unidad se está encriptando o desencriptando, la barra de progreso muestra el tiempo restante para concluir el proceso durante la sesión actual. Si el equipo se apaga o inicia la suspensión, modo de espera o hibernación durante el proceso de encriptación y después se reinicia, la pantalla de tiempo restante se reinicia al comienzo, pero la encriptación real se reanuda desde donde se detuvo por última vez. La pantalla de tiempo restante y de progreso cambiará más rápidamente para reflejar el progreso anterior.

Copias de seguridad y recuperación (tarea de administrador)

La página Recuperación permite que los administradores hagan copias de seguridad y recuperen claves de encriptación.

Copia de seguridad de clave de Drive Encryption local: le permite hacer copias de seguridad de claves de encriptación en medios extraíbles cuando Drive Encryption está activado.

Creación de claves de la copia de seguridad

Puede hacer una copia de seguridad de la clave de encriptación de una unidad encriptada en un dispositivo de almacenamiento extraíble:

△ **PRECAUCIÓN:** Asegúrese de guardar el dispositivo de almacenamiento que contiene la copia de seguridad de la clave en un lugar seguro ya que si olvida su contraseña o pierde su Java Card, este dispositivo será el único modo de acceder a su unidad de disco duro.

1. Abra la **Consola administrativa de HP ProtectTools**, haga clic en **Drive Encryption** y entonces haga clic en **Recuperación**.
2. Presione **Crear copia de seguridad de las claves**.
3. En la página Elegir disco para copia de seguridad, seleccione el dispositivo donde desea hacer la copia de seguridad de su clave de encriptación y entonces haga clic en **Siguiente**.
4. Lea la información en la siguiente página que aparece y luego haga clic en **Siguiente**. La clave de encriptación se guarda en el dispositivo de almacenamiento que usted seleccionó.
5. Cuando se abra el cuadro de diálogo de confirmación, haga clic en **Finalizar**.

Realización de una recuperación

Para realizar una recuperación si olvida su contraseña, siga estos pasos:

1. Encienda el equipo.
2. Inserte el dispositivo de almacenamiento extraíble que contiene la copia de seguridad de su clave.
3. Cuando se abra el cuadro de diálogo de inicio de sesión de Drive Encryption for HP ProtectTools, haga clic en **Cancelar**.
4. Haga clic en **Opciones** en la esquina inferior izquierda de la pantalla, y luego haga clic en **Recuperación**.
5. Seleccione el archivo que contiene la copia de seguridad de su clave o haga clic en **Examinar** para buscarlo, y a continuación haga clic en **Siguiente**.
6. Cuando se abra el cuadro de diálogo de confirmación, haga clic en **Aceptar**.

   Se inicia el equipo.

NOTA: Se recomienda enfáticamente que reinicie su contraseña después de realizar una recuperación.

9 Privacy Manager for HP ProtectTools (sólo en algunos modelos)

Privacy Manager for HP ProtectTools le permite usar métodos de inicio de sesión (autenticación) seguros avanzados para verificar el origen, la integridad y la seguridad de las comunicaciones cuando use correo electrónico, documentos de Microsoft® Office o mensajería instantánea (MI).

Privacy Manager utiliza la infraestructura de seguridad suministrada por HP ProtectTools Security Manager, que incluye los siguientes métodos de inicio de sesión seguros:

- Autenticación por huella digital
- Contraseña de Windows®
- Tarjeta Java™ de HP ProtectTools

Puede usar cualquiera de los métodos de inicio de sesión seguros de Privacy Manager.

Privacy Manager requiere lo siguiente:

- HP ProtectTools Security Manager 5.00 o superior
- Sistema operativo Windows® 7, Windows Vista® o Windows XP
- Microsoft Outlook 2007 o Microsoft Outlook 2003
- Cuenta de correo electrónico válida

NOTA: Se debe requerir e instalar un certificado de Privacy Manager (un certificado digital) desde Privacy Manager antes de que pueda acceder a los recursos de seguridad. Para obtener información sobre cómo requerir un certificado de Privacy Manager, consulte Solicitación e instalación de un certificado de Privacy Manager en la página 49.

Procedimientos de configuración

Apertura de Privacy Manager

Para abrir Privacy Manager:

1. Haga clic en **Inicio**, **Todos los programas**, **HP** y en **HP ProtectTools Security Manager**.
2. Haga clic en **Privacy Manager**.

– o –

Haga clic con el botón derecho del mouse en el icono de **HP ProtectTools** en el área de notificación, en el extremo derecho de la barra de tareas, y a continuación haga clic en **Privacy Manager** y en **Configuración**.

– o –

En la barra de herramientas de un mensaje de correo electrónico de Microsoft Outlook, haga clic en **Enviar de Forma Segura** y luego haga clic en **Administrador de Certificado** o en **Contactos confiables**.

– o –

En la barra de herramientas de un documento de Microsoft Office, haga clic en **Firmar y encriptar** y luego haga clic en **Administrador de Certificado** o en **Contactos confiables**.

Administración de certificados de Privacy Manager

Los certificados de Privacy Manager protegen los datos y mensajes utilizando una tecnología criptográfica denominada infraestructura de clave pública (PKI). La PKI requiere que los usuarios obtengan claves criptográficas y un certificado de Privacy Manager emitido por una autoridad de certificación (CA). A diferencia de la mayoría del software de codificación y autenticación, que sólo requiere que se autentique periódicamente, Privacy Manager requiere autenticación cada vez que firma un mensaje de correo electrónico o un documento de Microsoft Office utilizando una clave criptográfica. Privacy Manager hace que el proceso de guardado y envío de su información importante sea seguro.

Puede realizar las siguientes tareas:

- Solicitar e instalar un certificado de Privacy Manager
- Ver los detalles del certificado de Privacy Manager
- Renovar certificados de Privacy Manager
- Cuando se dispone de múltiples certificados, definir un certificado de Privacy Manager predeterminado que utilizará Privacy Manager
- Eliminar y revocar un certificado de Privacy Manager (avanzado)

Solicitación e instalación de un certificado de Privacy Manager

Antes de poder utilizar los recursos de Privacy Manager, debe solicitar e instalar un certificado de Privacy Manager (desde dentro de Privacy Manager) con una dirección de correo electrónico válida. La dirección de correo electrónico debe configurarse como una cuenta dentro de Microsoft Outlook en el mismo equipo desde el que solicita el certificado de Privacy Manager.

Solicitud de un certificado de Privacy Manager

1. Abra Privacy Manager y haga clic en **Administrador de Certificado**.
2. Haga clic en **Solicite un certificado Privacy Manager**.
3. Lea el texto de bienvenida y entonces haga clic en **Siguiente**.
4. En la página Acuerdo de licencia, lea el acuerdo de licencia.
5. Asegúrese de que la casilla de verificación al lado de **Marque aquí para aceptar los términos del contrato de licencia** esté seleccionada y luego haga clic en **Siguiente**.
6. En la página Sus detalles de certificado, introduzca la información requerida y haga clic en **Siguiente**.
7. En la página Solicitación de Certificado Aceptada, haga clic en **Finalizar**.
8. Haga clic en **Aceptar** para cerrar el certificado.

Recibirá un mensaje de correo electrónico en Microsoft Outlook con su certificado de Privacy Manager en archivo adjunto.

Obtención de un certificado corporativo preasignado de Privacy Manager

1. En Outlook, abra el correo electrónico que recibió que indica que se le preasignó un Certificado corporativo.
2. Haga clic en **Obtener**.
3. Recibirá un mensaje de correo electrónico en Microsoft Outlook con su certificado de Privacy Manager en archivo adjunto.
4. Para instalar el certificado, consulte Instalación de un certificado de Privacy Manager en la página 50

Instalación de un certificado de Privacy Manager

1. Cuando reciba el mensaje de correo electrónico con su certificado de Privacy Manager adjunto, abra el mensaje y haga clic en el botón **Configuración**, en el extremo inferior derecho del mensaje en Outlook 2007, o en el extremo superior izquierdo en Outlook 2003.
2. Autentíquese usando su método de inicio de sesión seguro elegido.
3. En la página Certificado instalado, haga clic en **Siguiente**.
4. En la página Copia de seguridad de certificado, ingrese un lugar y un nombre para el archivo de copia de seguridad o haga clic en **Explorar** para buscar una ubicación.

   △ **PRECAUCIÓN:** Asegúrese de guardar el archivo en una ubicación que no sea su unidad de disco duro y colóquelo en un lugar seguro. Este archivo debe ser únicamente para su uso y será necesario en caso de que necesite restaurar su certificado de Privacy Manager y las claves asociadas.

5. Escriba y confirme una contraseña y haga clic en **Siguiente**.

6. Autentíquese usando su método de inicio de sesión seguro elegido.

7. Si ha elegido comenzar con el proceso de invitación de un contacto confiable, siga las instrucciones en la pantalla comenzando por el paso 2 de este tópico Adición de Contactos Confiables usando sus contactos de Microsoft Outlook en la página 54.

   – o –

   Si hace clic en **Cancelar**, consulte Adición de un contacto confiable en la página 53 para obtener información sobre cómo añadir un contacto confiable en una ocasión posterior.

Visualización de los detalles del certificado de Privacy Manager

1. Abra Privacy Manager y haga clic en **Administrador de Certificado**.

2. Haga clic en un certificado de Privacy Manager.

3. Haga clic en **Detalles de su Certificado**.

4. Cuando haya finalizado la visualización de los detalles, haga clic en **Aceptar**.

Renovación de un certificado de Privacy Manager

Cuando su certificado de Privacy Manager se aproxime al vencimiento, se le notificará que necesita renovarlo:

1. Abra Privacy Manager y haga clic en **Administrador de Certificado**.

2. Haga clic en **Renovar certificado**.

3. Siga las instrucciones que aparecen en la pantalla para comprar un nuevo certificado de Privacy Manager.

NOTA: El proceso de renovación de certificados de Privacy Manager no sustituye su antiguo certificado de Privacy Manager. Será necesario que compre un certificado Privacy Manager y que lo instale usando los mismos procedimientos que en Solicitación e instalación de un certificado de Privacy Manager en la página 49.

Configuración de un certificado de Privacy Manager predeterminado

Sólo los certificados de Privacy Manager pueden verse desde adentro de Privacy Manager, incluso si hay instalados en su equipo certificados adicionales de otras autoridades de certificación.

Si tiene más de un certificado de Privacy Manager en su equipo que se instaló desde dentro de Privacy Manager, puede especificar uno de ellos como certificado predeterminado:

1. Abra Privacy Manager y haga clic en **Administrador de Certificado**.

2. Seleccione el Certificado de Privacy Manager que desea utilizar como predeterminado, y luego haga clic en **Fijar predeterminado**.

3. Haga clic en **Aceptar**.

NOTA: No está obligado a utilizar su certificado de Privacy Manager predeterminado. Desde dentro de las distintas funciones de Privacy Manager, puede seleccionar cualquiera de los certificados de Privacy Manager que desee utilizar.

Eliminación de un certificado de Privacy Manager

Si elimina un certificado de Privacy Manager, no podrá abrir archivos ni ver ningún dato que haya encriptado con ese certificado. Si ha borrado accidentalmente un certificado de Privacy Manager, puede restaurarlo usando el archivo de copia de seguridad que creó cuando instaló el certificado. Consulte Restauración de un certificado de Privacy Manager en la página 52 para obtener más información.

Para eliminar un certificado de Privacy Manager:

1. Abra Privacy Manager y haga clic en **Administrador de Certificado**.
2. Seleccione el Certificado de Privacy Manager que desea eliminar, y luego haga clic en **Avanzado**.
3. Haga clic en **Eliminar**.
4. Cuando se abra el cuadro de diálogo de confirmación, haga clic en **Sí**.
5. Haga clic en **Cerrar** y, a continuación, haga clic en **Aplicar**.

Restauración de un certificado de Privacy Manager

Durante la instalación de su certificado de Privacy Manager, se le solicita que cree una copia de seguridad del certificado. También puede crear una copia de seguridad de la página de Migración. Esta copia de seguridad se puede usar cuando migre a otro equipo o cuando desee restaurar un certificado en el mismo equipo.

1. Abra Privacy Manager y haga clic en **Migración**.
2. Haga clic en **Restaurar**.
3. En la página de Archivo de migración, haga clic en **Explorar** para buscar el archivo .dppsm que usted creó en el proceso de copia de seguridad, y luego haga clic en **Siguiente**.
4. Introduzca la contraseña que utilizó cuando creó la copia de seguridad y luego haga clic en **Siguiente**.
5. Haga clic en **Finalizar**.
6. Haga clic en **Aceptar**.

Consulte Instalación de un certificado de Privacy Manager en la página 50 o Copia de respaldo de certificados de Privacy Manager y contactos confiables en la página 68 para obtener más información.

Revocación de su certificado de Privacy Manager

Si considera que la seguridad de su certificado de Privacy Manager ha estado en peligro, puede revocar su propio certificado:

NOTA: Un certificado de Privacy Manager revocado no se elimina. El certificado aún puede utilizarse para visualizar los archivos encriptados.

1. Abra Privacy Manager y haga clic en **Administrador de Certificado**.
2. Haga clic en **Avanzado**.
3. Seleccione el Certificado de Privacy Manager que desea revocar, y luego haga clic en **Revocar**.
4. Cuando se abra el cuadro de diálogo de confirmación, haga clic en **Sí**.

5. Autentíquese usando su método de inicio de sesión seguro elegido.

6. Siga las instrucciones que aparecen en la pantalla.

Administración de contactos confiables

Los contactos confiables son usuarios con quien intercambió certificados de Privacy Manager, lo que les permite comunicarse entre sí con seguridad.

El Administrador de Contactos Confiables le permite realizar las siguientes tareas:

- Visualizar detalles de los contactos confiables
- Eliminar contactos confiables
- Verificar el estado de revocación de los contactos confiables (avanzado)

Agregado de contactos confiables

El agregado de contactos confiables es un proceso que consta de tres pasos:

1. Usted envía una invitación de correo electrónico a un destinatario que es un contacto confiable.
2. El destinatario contacto confiable responde al mensaje de correo electrónico.
3. Usted recibe la respuesta de correo electrónico del destinatario del Contacto confiable y haga clic en **Aceptar**.

Puede enviar invitaciones de correo electrónico de contacto confiable a destinatarios individuales o puede enviar la invitación a todos los contactos de su libreta de direcciones de Microsoft Outlook.

Consulte las siguientes secciones para agregar contactos confiables.

NOTA: Para responder a su invitación de convertirse en un contacto confiable, los destinatarios del contacto confiable deben tener Privacy Manager instalado en sus equipos o tener un cliente alternativo instalado. Para obtener más información sobre la instalación del cliente alternativo, acceda al sitio web de DigitalPersonal en http://DigitalPersona.com/PrivacyManager.

Adición de un contacto confiable

1. Abra Privacy Manager, haga clic en **Administrador de Contactos Confiables** y luego haga clic en **Invite contactos**.

   – o –

   En Microsoft Outlook, haga clic en la flecha hacia abajo al lado de **Enviar de Forma Segura** en la barra de herramientas y luego haga clic en **Invite contactos**.

2. Si se abre el cuadro de diálogo de selección de certificado, haga clic en el certificado de Privacy Manager que desea utilizar y luego haga clic en **Aceptar**.

3. Cuando se abra el cuadro de diálogo de invitación de contacto confiable, lea el texto y luego haga clic en **Aceptar**.

   Se genera automáticamente un correo electrónico.

4. Escriba una o más direcciones de correo electrónico de los destinatarios que desee agregar como contactos confiables.

5. Edite el texto y firme su nombre (opcional).

6. Haga clic en **Enviar**.

NOTA: Si no ha obtenido un certificado de Privacy Manager, un mensaje le informa que debe tener un certificado de Privacy Manager para enviar una solicitación de contacto confiable. Haga clic en **Aceptar** para iniciar el asistente de solicitud de certificado. Consulte Solicitación e instalación de un certificado de Privacy Manager en la página 49 para obtener más información.

7. Autentíquese usando su método de inicio de sesión seguro elegido.

NOTA: Cuando el destinatario del contacto confiable recibe el correo electrónico, el destinatario debe abrir el mensaje y hacer clic en **Aceptar** en el extremo inferior derecho del correo electrónico y luego hacer clic en **OK** cuando se abra el cuadro de diálogo de confirmación.

8. Cuando usted reciba un correo electrónico de un destinatario que acepte la invitación para convertirse en un contacto confiable, haga clic en **Aceptar** en el extremo inferior derecho del correo electrónico.

   Se abre un cuadro de diálogo, que confirma que el destinatario se agregó con éxito a su lista de contactos confiables.

9. Haga clic en **Aceptar**.

Adición de Contactos Confiables usando sus contactos de Microsoft Outlook

1. Abra Privacy Manager, haga clic en **Administrador de Contactos Confiables** y luego haga clic en **Invite contactos**.

   – o –

   En Microsoft Outlook, haga clic en la flecha hacia abajo al lado de **Enviar de Forma Segura** en la barra de herramientas y luego haga clic en **Invitar a todos mis contactos de Outlook**.

2. Cuando se abra la página de Invitación de contacto confiable, seleccione las direcciones de correo electrónico de los destinatarios a quienes desea agregar a sus contactos confiables y entonces haga clic en **Siguiente**.

3. Cuando se abra la página Enviando una invitación, haga clic en **Finalizar**.

   Se genera automáticamente un mensaje de correo electrónico que enumera las direcciones de correo electrónico de Microsoft Outlook.

4. Edite el texto y firme su nombre (opcional).

5. Haga clic en **Enviar**.

NOTA: Si no ha obtenido un certificado de Privacy Manager, un mensaje le informa que debe tener un certificado de Privacy Manager para enviar una solicitación de contacto confiable. Haga clic en **Aceptar** para iniciar el asistente de solicitud de certificado. Consulte Solicitación e instalación de un certificado de Privacy Manager en la página 49 para obtener más información.

6. Autentíquese usando su método de inicio de sesión seguro elegido.

NOTA: Cuando el destinatario del Contacto Confiable recibe el mensaje de correo electrónico, el destinatario debe abrir el mensaje y hacer clic en **Aceptar** en el extremo inferior derecho del correo electrónico y luego hacer clic en **OK** cuando se abra el cuadro del diálogo de confirmación.

7. Cuando usted reciba un mensaje de correo electrónico de un destinatario aceptando la invitación para convertirse en un Contacto Confiable, haga clic en **Aceptar** en el extremo inferior derecho del correo electrónico.

   Se abre un cuadro de diálogo, que confirma que el destinatario se agregó con éxito a su lista de Contactos Confiables.

8. Haga clic en **Aceptar**.

Visualización de detalles de Contactos confiables

1. Abra Privacy Manager y haga clic en **Administrador de Contactos Confiables**.
2. Haga clic en contacto confiable.
3. Haga clic en **Detalles de contacto**.
4. Cuando haya finalizado la visualización de los detalles, haga clic en **Aceptar**.

Eliminación de un contacto confiable

1. Abra Privacy Manager y haga clic en **Contactos Confiables**.
2. Haga clic en el contacto confiable que desea eliminar.
3. Haga clic en **Elimine contacto**.
4. Cuando se abra el cuadro de diálogo de confirmación, haga clic en **Sí**.

Verificación del estado de revocación de un contacto confiable

Para ver si un contacto confiable revocó el certificado de Privacy Manager:

1. Abra Privacy Manager y haga clic en **Contactos Confiables**.
2. Haga clic en contacto confiable.
3. Haga clic en el botón **Avanzado**.

   Se abre el cuadro de diálogo de administración avanzada de contactos confiables.

4. Haga clic en **Verificar Anulación**.
5. Haga clic en **Cierre**.

Tareas generales

Puede usar Privacy Manager con los siguientes productos de Microsoft:

- Microsoft Outlook
- Microsoft Office
- Windows Live Messenger

Uso de Privacy Manager en Microsoft Outlook

Cuando se instala Privacy Manager, un botón de Privacidad se mostrará en la barra de herramientas de Microsoft Outlook y un botón Enviar de Forma Segura se mostrará en la barra de herramientas de cada mensaje de correo electrónico de Microsoft Outlook. Cuando hace clic en la flecha hacia abajo cerca de **Privacidad** o de **Enviar de Forma Segura**, puede elegir una de las siguientes opciones:

- Firmar y Enviar (solamente el botón Enviar de Forma Segura): esta opción agrega una firma digital al mensaje de correo electrónico y lo envía después de que usted se autentica usando el método de inicio de sesión de seguridad elegido.
- Selle para Contactos Confiables y Envíe (solamente el botón Enviar de Forma Segura): esta opción agrega una firma digital, encripta el mensaje de correo electrónico y lo envía después de que usted se autentica usando el método de inicio de sesión de seguridad elegido.
- Invitar contactos: esta opción le permite enviar una invitación de contacto confiable. Consulte Adición de un contacto confiable en la página 53 para obtener más información.
- Invitar contactos de Outlook: esta opción le permite enviar una invitación de contacto confiable a todos los contactos de su libreta de direcciones de Microsoft Outlook. Consulte Adición de Contactos Confiables usando sus contactos de Microsoft Outlook en la página 54 para obtener más información.
- Abrir el software Privacy Manager: las opciones de Certificados, Contactos confiables y Configuración le permiten abrir el software Privacy Manager para agregar, ver o cambiar sus configuraciones actuales. Consulte Configuración de Privacy Manager para Microsoft Outlook en la página 56 para obtener más información.

Configuración de Privacy Manager para Microsoft Outlook

1. Abra Privacy Manager, haga clic en **Configuración** y luego en la ficha **Correo electrónico**.

   – o –

   En la barra de herramientas de Microsoft Outlook, haga clic en la flecha hacia abajo al lado de **Enviar de Forma Segura** (**Privacy** en Outlook 2003), y después haga clic en **Configuración**.

   – o –

   En la barra de herramientas de un mensaje de correo electrónico de Microsoft, haga clic en la flecha abajo al lado de **Enviar de Forma Segura** y entonces haga clic en **Configuración**.

2. Seleccione las acciones que desea realizar cuando envíe un mensaje de correo electrónico seguro y entonces haga clic en **Aceptar**.

Firma y envío de un mensaje de correo electrónico

1. En Microsoft Outlook, haga clic en **Nuevo** o en **Responder**.
2. Redacte su mensaje de correo electrónico.
3. Haga clic en la flecha hacia abajo al lado de **Enviar de Forma Segura** (**Privacy** en Outlook 2003), y después haga clic en **Firme y envíe mensaje**.
4. Autentíquese usando su método de inicio de sesión seguro elegido.

Sellado y envío de un mensaje de correo electrónico

Los mensajes de correo electrónico que estén firmados y sellados (encriptados) digitalmente sólo podrán ser vistos por personas que usted elija de su lista de contactos confiables.

Para sellar y enviar un mensaje de correo electrónico a un contacto confiable:

1. En Microsoft Outlook, haga clic en **Nuevo** o en **Responder**.
2. Redacte su mensaje de correo electrónico.
3. Haga clic en la flecha hacia abajo al lado de **Enviar de Forma Segura** (**Privacy** en Outlook 2003), y después haga clic en **Selle para contactos confiables y envíe mensaje**.
4. Autentíquese usando su método de inicio de sesión seguro elegido.

Visualización de un mensaje de correo electrónico sellado

Al abrir un mensaje de correo electrónico sellado, la etiqueta de seguridad se muestra en el encabezamiento del documento. La etiqueta de seguridad suministra la siguiente información:

- Las credenciales que se utilizaron para verificar la identidad de la persona que firma el mensaje de correo electrónico
- El producto que se utilizó para verificar las credenciales de la persona que firmó el mensaje de correo electrónico

Uso de Privacy Manager en un documento de Microsoft Office 2007

NOTA: Privacy Manager solamente se puede usar con documentos de Microsoft Office 2007.

Después de instalar su certificado de Privacy Manager, aparecerá un botón Firme y Codifique en el lado derecho de la barra de herramientas de todos los documentos de Microsoft Word, Microsoft Excel y Microsoft PowerPoint. Cuando haga clic en la flecha hacia abajo cerca de **Firme y Codifique**, podrá elegir una de las siguientes opciones:

- Firme documento: esta opción le agrega su firma digital al documento.
- Agregar línea de firma antes de firmar (solamente en Microsoft Word y Microsoft Excel): de forma predeterminada, se añade una línea de firma cuando se firma o se encripta un documento de Microsoft Word o Microsoft Excel. Para desactivar esta opción, haga clic en **Agregar línea de firma** para desmarcar la casilla de verificación.
- Codifique Documento: esta opción le agrega su firma digital al documento y lo encripta.

- Eliminar Codificación: esta opción le quita la encriptación al documento.
- Abrir el software Privacy Manager: las opciones de Certificados, Contactos confiables y Configuración le permiten abrir el software Privacy Manager para agregar, ver o cambiar sus configuraciones actuales. Consulte Administración de certificados de Privacy Manager en la página 49, Administración de contactos confiables en la página 53, o Configuración de Privacy Manager para Microsoft Office en la página 58 para obtener más información.

Configuración de Privacy Manager para Microsoft Office

1. Abra Privacy Manager, haga clic en **Configuración** y luego en la ficha **Documentos**.

   – o –

   En la barra de herramientas de un documento de Microsoft Office, haga clic en la flecha abajo al lado de **Firme y Codifique** y entonces haga clic en **Configuración**.

2. Seleccione las acciones que desee configurar y haga clic en **Aceptar**.

Firma de un documento de Microsoft Office

1. En Microsoft Word, Microsoft Excel o Microsoft PowerPoint, cree y guarde un documento.
2. Haga clic en la flecha abajo al lado de **Firme y Codifique** y entonces haga clic en **Firme documento**.
3. Autentíquese usando su método de inicio de sesión seguro elegido.
4. Cuando se abre el cuadro de diálogo de confirmación, lea el texto y haga clic en **Aceptar**.

Si más adelante decide editar el documento, siga estos pasos:

1. Haga clic en el botón **Office**, en la esquina superior izquierda de la pantalla.
2. Haga clic en **Preparar** y luego en **Marcar como final**.
3. Cuando se abra el cuadro del diálogo de confirmación, haga clic en **Sí** y continúe trabajando.
4. Una vez que haya terminado de editar, firme nuevamente el documento.

Adición de una línea de firma cuando firma un documento de Microsoft Word o Microsoft Excel

Privacy Manager le permite agregar una línea de firma cuando usa un documento de Microsoft Word o Microsoft Excel:

1. En Microsoft Word o Microsoft Excel, cree y guarde un documento.
2. Haga clic en el menú **Inicio**.
3. Haga clic en la flecha abajo al lado de **Firme y Codifique** y entonces haga clic en **Agregar línea de firma antes de firmar**.

NOTA: Aparecerá una marca de verificación al lado de Agregar línea de firma antes de firmar cuando esta opción esté seleccionada. Esta opción está activada de forma predeterminada.

4. Haga clic en la flecha abajo al lado de **Firme y Codifique** y entonces haga clic en **Firme documento**.

5. Autentíquese usando su método de inicio de sesión seguro elegido.

Adición de firmantes sugeridos a documentos de Microsoft Word o Microsoft Excel

Usted puede agregar más de una línea de firma a su documento designando firmantes sugeridos. Un firmante sugerido es un usuario que ha sido designado por el propietario de un documento de Microsoft Word o Microsoft Excel para agregar una línea de firma al documento. Los firmantes sugeridos pueden ser usted u otra persona que usted desee que firme su documento. Por ejemplo, si usted prepara un documento que debe ser firmado por todos los miembros de su departamento, puede incluir líneas de firma para esos usuarios al final de la última página del documento con instrucciones para que sea firmado hasta una fecha específica.

Para agregar un firmante sugerido a un documento de Microsoft Word o Microsoft Excel:

1. En Microsoft Word o Microsoft Excel, cree y guarde un documento.

2. Haga clic en el menú **Insertar**.

3. En el grupo **Texto**, en la barra de herramientas, haga clic en la flecha al lado de **Línea de firma** y entonces haga clic en **Proveedor de Firma de Privacy Manager**.

   Se abre el cuadro de diálogo de Configuración de firma.

4. En el cuadro de texto debajo de **Signatario sugerido**, introduzca el nombre del signatario sugerido.

5. En el cuadro de texto debajo de **Instrucciones para el signatario**, escriba un mensaje para este signatario sugerido.

NOTA: Este mensaje aparecerá en el lugar de un cargo y se borra o sustituye por el cargo del usuario cuando se firma el documento.

6. Seleccione la casilla de verificación **Exhiba la fecha de firma en la línea de firma** para mostrar la fecha.

7. Seleccione la casilla de verificación **Exhiba cargo del signatario en la línea de firma** para mostrar el cargo.

NOTA: Como el propietario de un documento designa los firmantes sugeridos para su documento, si las casillas de verificación **Exhiba la fecha de firma en la línea de firma** y/o **Exhiba cargo del signatario en la línea de firma** no están seleccionadas, el firmante sugerido no podrá mostrar la fecha y/o el cargo en la línea de firma, incluso si las configuraciones del documento del firmante sugerido están definidas para eso.

8. Haga clic en **Aceptar**.

Adición de una línea de firma para un firmante sugerido

Cuando los firmantes sugeridos abren el documento, verán su nombre entre paréntesis, indicando que se requiere su firma.

Para firmar el documento:

1. Haga doble clic en la línea de firma adecuada.

2. Autentíquese usando su método de inicio de sesión seguro elegido.

Se mostrará la línea de firma de acuerdo con la configuración especificada por el propietario del documento.

Encriptación de un documento de Microsoft Office

Puede encriptar un documento de Microsoft Office para usted y sus contactos confiables. Cuando encripta un documento y lo cierra, usted y el(los) contacto(s) confiable(s) seleccionado(s) de la lista deberá(n) autenticarse antes de abrirlo.

Para encriptar un documento de Microsoft Office:

1. En Microsoft Word, Microsoft Excel o Microsoft PowerPoint, cree y guarde un documento.
2. Haga clic en el menú **Inicio**.
3. Haga clic en la flecha hacia abajo al lado de **Firme y Codifique** y luego haga clic en **Codifique Documento**.

   Se abre el cuadro de diálogo Seleccione Contactos Confiables.
4. Haga clic en el nombre de un contacto confiable que podrá abrir el documento y ver su contenido.

NOTA: Para seleccionar varios nombres de contactos confiables, mantenga presionada la tecla ctrl y haga clic en los nombres individuales.

5. Haga clic en **Aceptar**.

Si más adelante decide editar el documento, siga los pasos indicados en Eliminación de la encriptación de un documento de Microsoft Office en la página 60. Cuando elimine la encriptación, podrá editar el documento. Siga los pasos de esta sección para encriptar el documento de nuevo.

Eliminación de la encriptación de un documento de Microsoft Office

Cuando elimina la encriptación de un documento de Microsoft Office, usted y sus contactos confiables ya no precisarán autenticarse para abrir y ver el contenido del documento.

Para eliminar la encriptación de un documento de Microsoft Office:

1. Abra un documento encriptado de Microsoft Word, Microsoft Excel o Microsoft PowerPoint.
2. Autentíquese usando su método de inicio de sesión seguro elegido.
3. Haga clic en el menú **Inicio**.
4. Haga clic en la flecha hacia abajo al lado de **Firme y Codifique** y luego haga clic en **Eliminar Codificación**.

Envío de un documento de Microsoft Office encriptado

Puede adjuntar un documento encriptado de Microsoft Office a un mensaje de correo electrónico sin firmar ni encriptar el propio mensaje. Para hacer esto, cree y envíe un mensaje de correo electrónico con un documento firmado o encriptado como lo haría normalmente con cualquier mensaje con un archivo adjunto.

Sin embargo, para optimizar la seguridad, se recomienda que encripte el mensaje de correo electrónico cuando le adjunta un documento de Microsoft Office firmado o encriptado.

Para enviar un mensaje de correo electrónico sellado con un documento de Microsoft Office firmado y/o encriptado, siga estos pasos:

1. En Microsoft Outlook, haga clic en **Nuevo** o en **Responder**.
2. Redacte su mensaje de correo electrónico.
3. Adjunte el documento de Microsoft Office.
4. Consulte Sellado y envío de un mensaje de correo electrónico en la página 57 para obtener más instrucciones.

Visualización de un documento de Microsoft Office firmado

NOTA: No es necesario tener un certificado de Privacy Manager para ver o firmar un documento de Microsoft Office.

Cuando se abre un documento de Microsoft Office firmado, se muestra un icono de Firma digital en la barra de estado en la parte inferior de la ventana del documento.

1. Haga clic en el icono de **Firmas digitales** para alternar la exhibición del cuadro de diálogo de Firmas, que muestra el nombre de todos los usuarios que firmaron el documento y la fecha en que cada usuario lo firmó.
2. Para ver detalles adicionales sobre cada firma, haga clic con el botón derecho sobre un nombre en el cuadro de diálogo de Firmas y seleccione Detalles de firmas.

Visualización de un documento de Microsoft Office encriptado

Para ver un documento de Microsoft Office encriptado en otro equipo, Privacy Manager debe estar instalado en ese equipo. Además, debe restaurar el certificado de Privacy Manager que se utilizó para encriptar el archivo.

Un contacto confiable que desea ver un documento de Microsoft Office encriptado debe tener un certificado de Privacy Manager y Privacy Manager debe estar instalado en su equipo. Además, el contacto confiable debe haber sido elegido por el usuario del documento de Microsoft Office encriptado.

Uso de Privacy Manager en Windows Live Messenger

Privacy Manager agrega los siguientes recursos de comunicaciones seguras a Windows Live Messenger:

- **Chat seguro**: los mensajes se transmiten usando SSL/TLS (Secure Sockets Layer/Transport Layer Security) sobre el protocolo XML, la misma tecnología que garantiza la seguridad de las transacciones de comercio electrónico.
- **Identificación del destinatario**: es posible verificar la presencia y la identidad de una persona antes de mandarle un mensaje.
- **Mensajes firmados**: puede firmar electrónicamente sus mensajes. Entonces, si alguien interfiere en el mensaje, estará marcado como inválido cuando el destinatario lo reciba.
- **Recurso ocultar/mostrar**: puede ocultar cualquiera o todos los mensajes en la ventana de chat de Privacy Manager. También puede enviar un mensaje en el que el contenido esté oculto. Se requiere la autenticación antes de que se muestre el mensaje.

- **Historial de chat seguro**: los registros de sus sesiones de chat se encriptan antes de guardarse y requieren autenticación para poder verlos.
- **Bloqueo/desbloqueo automático**: puede bloquear y desbloquear la ventana de chat de Privacy Manager o configurarla para que se bloquee después de un período de inactividad especificado.

Inicio de una sesión de chat en Privacy Manager

NOTA: Para usar Privacy Manager Chat, ambas partes deben tener Privacy Manager y un certificado de Privacy Manager instalados. Para obtener más detalles sobre la instalación de un certificado de Privacy Manager, consulte Solicitación e instalación de un certificado de Privacy Manager en la página 49.

1. Para iniciar el chat de Privacy Manager en Windows Live Messenger, realice uno de estos procedimientos:

   a. Haga clic con el botón derecho en un contacto de Live Messenger que esté en línea y seleccione **Iniciar una actividad**.

   b. Haga clic en **Iniciar chat**.

   – o –

   a. Haga doble clic en un contacto de Live Messenger que esté en línea y luego seleccione el menú **Ver una lista de actividades**.

   b. Haga clic en **Acción** y luego en **Iniciar chat**.

   – o –

   a. Haga clic en el icono de **ProtectTools** en el área de notificación, haga clic en **Privacy Manager for HP ProtectTools**, y después seleccione **Iniciar chat**.

   b. En Live Messenger, haga clic en **Acciones: iniciar una actividad** y luego seleccione **Chat de Privacy Manager**.

   NOTA: Cada usuario debe estar en línea en Live Messenger y se deben mostrar mutuamente en las ventanas en línea respectivas de Live Messenger. Haga clic para seleccionar un usuario en línea.

   Privacy Manager envía una invitación al contacto para iniciar el chat de Privacy Manager. Cuando los contactos invitados aceptan, se abre la ventana Chat de Privacy Manager. Si el contacto invitado no tiene Privacy Manager, se le solicitará que lo descargue.

2. Haga clic en **Iniciar** para comenzar un chat seguro.

Configuración de Privacy Manager para Windows Live Messenger

1. En el chat de Privacy Manager, haga clic en el botón **Configuración**.

   – o –

   En Privacy Manager, haga clic en **Configuración** y luego en la ficha **Conversación**.

   – o –

   En el Visualizador del historial de Live Messenger en Privacy Manager, haga clic en el botón **Configuración**.

2. Para especificar el tiempo que el chat de Privacy Manager espera antes de bloquear su sesión, seleccione un número en la lista de **Bloquee sesión después de _ minutos de inactividad**.

3. Para especificar una carpeta de historial para sus sesiones de chat, haga clic en **Navegar** para buscar una carpeta y entonces haga clic en **Aceptar**.

4. Para encriptar y guardar automáticamente sus sesiones cuando las cierra, seleccione la casilla de verificación **Guarde automáticamente el historial de conversación con seguridad**.

5. Haga clic en **Aceptar**.

Realización de un chat en la ventana del chat de Privacy Manager

Después de iniciar el chat de Privacy Manager, se abre una ventana específica en Windows Live Messenger El uso del chat de Privacy Manager es similar al uso básico de Windows Live Messenger, excepto que los siguientes recursos adicionales se encuentran disponibles en la ventana del chat de Privacy Manager:

- **Guardar**: haga clic en este botón para guardar su sesión de chat en la carpeta especificada en su configuración. También puede configurar el chat de Privacy Manager para que guarde automáticamente cada sesión cuando se cierra.
- **Ocultar todo** y **Mostrar todo**: haga clic en el botón apropiado para expandir o cerrar los mensajes que se muestran en la ventana Comunicaciones seguras. Usted también puede ocultar o mostrar mensajes individuales haciendo clic en el encabezamiento del mensaje.
- **¿Estás ahí?**: haga clic en este botón para solicitar la autenticación de su contacto.
- **Bloquear**: haga clic en este botón para cerrar la ventana de chat de Privacy Manager y volver a la ventana de entrada de chat. Para mostrar nuevamente la ventana de Comunicaciones seguras, haga clic en **Reanudar la sesión** y entonces autentíquese usando su método de inicio de sesión seguro.
- **Enviar**: haga clic en este botón para enviar un mensaje encriptado a su contacto.
- **Enviar firmado**: seleccione esta casilla de verificación para firmar y encriptar electrónicamente sus mensajes. Entonces, si alguien interfiere en el mensaje, estará marcado como inválido cuando el destinatario lo reciba. Debe autenticarse cada vez que envíe un mensaje firmado.
- **Enviar oculto**: seleccione esta casilla de verificación para encriptar y enviar un mensaje mostrando sólo el encabezamiento del mensaje. Su contacto deberá autenticarse para leer el contenido del mensaje.

Visualización del historial del chat

Chat de Privacy Manager: el Visualizador del historial de Live Messenger muestra los archivos encriptados de las sesiones de chat de Privacy Manager. Las sesiones pueden guardarse haciendo clic en **Guardar** en la ventana del chat de Privacy Manager o configurando el guardado automático en la ficha Chat de Privacy Manager. En el visualizador, cada sesión muestra el nombre de pantalla del contacto (encriptado) y la fecha y hora de inicio y finalización de la sesión. De forma predeterminada, se muestran las sesiones de todas las cuentas de correo electrónico que haya configurado. Puede usar el menú **Exhibir historial de** para seleccionar sólo algunas cuentas específicas para su visualización.

El visualizador le permite realizar las siguientes tareas:

- Revelación de todas las sesiones en la página 64
- Revelar sesiones de una cuenta específica en la página 64
- Visualización de una identidad de sesión en la página 65
- Visualización de una sesión en la página 65
- Búsqueda de un texto específico en las sesiones en la página 65
- Eliminación de una sesión en la página 65
- Adición o eliminación de columnas en la página 66
- Filtrado de sesiones mostradas en la página 66

Para iniciar el Visualizador del historial de Live Messenger:

▲ En el área de notificación, en el extremo derecho de la barra de tareas, haga clic con el botón derecho en el icono de **HP ProtectTools**, luego en **Privacy Manager: for HP ProtectTools** y después en **Visualizador del historial de Live Messenger**.

– o –

▲ En una sesión de chat, haga clic en **Visualizador del historial** o **Historial**.

Revelación de todas las sesiones

La revelación de todas las sesiones muestra el nombre de pantalla del contacto desencriptado de las sesiones actuales seleccionadas y de todas las sesiones de la misma cuenta.

Para revelar todas sus sesiones con historiales de chat guardados:

1. En el visualizador del historial de chat de Live Messenger, haga clic con el botón derecho en cualquier sesión y luego seleccione **Revelar todas las sesiones**.
2. Autentíquese usando su método de inicio de sesión seguro elegido.

   Los nombres de pantalla de contacto se desencriptan.
3. Haga doble clic en cualquier sesión para ver su contenido.

Revelar sesiones de una cuenta específica

La revelación de una sesión muestra el nombre de pantalla del contacto desencriptado de la sesión actual seleccionada.

Para revelar una sesión específica de historial del chat:

1. En el visualizador del historial del chat de Live Messenger, haga clic con el botón derecho en cualquier sesión y luego seleccione **Revelar sesión**.
2. Autentíquese usando su método de inicio de sesión seguro elegido.

   El nombre de pantalla del contacto se desencripta.
3. Haga doble clic en cualquier sesión revelada para ver su contenido.

NOTA: Otras sesiones encriptadas con el mismo certificado se mostrarán con un icono de desbloqueo, lo que indica que puede verlas haciendo doble clic en cualquiera de ellas sin autenticación adicional. Las sesiones encriptadas con otro certificado mostrarán un icono de bloqueo, lo que indica que se requiere autenticación para dichas sesiones antes de ver los nombres de pantalla del contacto o el contenido.

Visualización de una identidad de sesión

Para ver una identidad de sesión:

- En el Visualizador del historial del chat de Live Messenger, haga clic con el botón derecho en cualquier sesión revelada y luego seleccione **Ver identidad de sesión**.

Visualización de una sesión

La visualización de una sesión abre el archivo para su visualización. Si la sesión no ha sido revelada (mostrando el nombre de pantalla del contacto desencriptado) previamente, se revelará en el mismo momento.

Para ver una sesión en el historial de Live Messenger:

1. En el Visualizador del historial de Live Messenger, haga clic con el botón derecho en cualquier sesión y luego seleccione **Visualizar**.
2. Si se le solicita, autentíquese usando su método de inicio de sesión seguro elegido.

   El contenido de la sesión se desencripta.

Búsqueda de un texto específico en las sesiones

Sólo puede buscar un texto en las sesiones reveladas (desencriptadas) que se muestran en la pantalla del visualizador. Estas son las sesiones en las que el nombre de pantalla del contacto se muestra como texto común.

Para buscar un texto en las sesiones de los historiales del chat:

1. En el visualizador del historial del chat de Live Messenger, haga clic en el botón **Buscar**.
2. Escriba el texto que desea buscar, configure cualquier parámetro deseado y luego haga clic en **Aceptar**.

   Las sesiones que contienen el texto aparecen resaltadas en la ventana del visualizador.

Eliminación de una sesión

1. Seleccione una sesión del historial del chat.
2. Haga clic en **Eliminar**.

Adición o eliminación de columnas

De forma predeterminada, se muestran las tres columnas más utilizadas en el Visualizador del historial de Live Messenger. Puede agregar columnas adicionales para mostrar o puede eliminar columnas de la pantalla.

Para agregar columnas:

1. Haga clic con el botón derecho en cualquier encabezamiento de columna y luego seleccione **Agregar/Quitar columnas**.
2. Seleccione un encabezamiento de columna en el panel izquierdo y entonces haga clic en **Agregar** para moverlo hacia el panel de la derecha.

Para quitar columnas de la pantalla:

1. Haga clic con el botón derecho en cualquier encabezamiento de columna y luego seleccione **Agregar/Quitar columnas**.
2. Seleccione un encabezamiento de columna en el panel derecho y entonces haga clic en **Quitar** para moverlo hacia el panel izquierdo.

Filtrado de sesiones mostradas

Se muestra una lista de sesiones de todas sus cuentas en el Visualizador del historial del chat de Live Messenger. También puede filtrar las sesiones mostradas referentes a:

- Cuentas específicas. Para obtener detalles, consulte Exhibición de sesiones de una cuenta específica en la página 66.
- Intervalos de fechas. Para obtener detalles, consulte Exhibición de sesiones entre dos fechas determinadas en la página 66.
- Carpetas diferentes. Para obtener detalles, consulte Exhibición de sesiones guardadas en una carpeta diferente de la carpeta predeterminada en la página 66.

Exhibición de sesiones de una cuenta específica

▲ En el visualizador del historial del chat de Live Messenger, seleccione una cuenta del menú **Exhiba historial para**.

Exhibición de sesiones entre dos fechas determinadas

1. En el visualizador del historial de Live Messenger, haga clic en el icono **Filtro avanzado**.

   Se abre el cuadro de diálogo Filtro avanzado.

2. Seleccione la casilla de verificación **Sólo mostrar sesiones del período definido**.
3. En los cuadros de texto **Desde** y **Hasta**, escriba el día, mes y/o año o haga clic en la flecha al lado del calendario para seleccionar las fechas.
4. Haga clic en **Aceptar**.

Exhibición de sesiones guardadas en una carpeta diferente de la carpeta predeterminada

1. En el visualizador del historial de Live Messenger, haga clic en el icono **Filtro avanzado**.
2. Seleccione la casilla de verificación **Usar carpeta alternativa para arch. hist.**.

3. Introduzca la ubicación de la carpeta o haga clic en **Buscar** para buscar una carpeta.
4. Haga clic en **Aceptar**.

Tareas avanzadas

Migración de certificados de Privacy Manager y de contactos confiables a otro equipo

Puede migrar con seguridad sus certificados de Privacy Manager y Contactos Confiables a otro equipo, o realizar una copia de seguridad de sus datos para protegerlos. Para hacerlo, realice la copia de seguridad de los datos en un archivo protegido con contraseña en una ubicación de red o en cualquier dispositivo de almacenamiento extraíble y luego restaure el archivo en el nuevo equipo.

Copia de respaldo de certificados de Privacy Manager y contactos confiables

Para realizar una copia de seguridad de sus certificados de Privacy Manager y los Contactos Confiables en un archivo protegido con contraseña, siga estos pasos:

1. Abra Privacy Manager y haga clic en **Migración**.
2. Haga clic en **Crear copia de seguridad**.
3. En la página Seleccionar datos, elija las categorías de datos que se incluirán en el archivo de migración y entonces haga clic en **Siguiente**.
4. En la página Archivo de migración, ingrese un nombre de archivo o haga clic en **Explorar** para buscar una ubicación, y entonces haga clic en **Siguiente**.
5. Escriba y confirme una contraseña y haga clic en **Siguiente**.

NOTA: Guarde esta contraseña en un lugar seguro, porque la necesitará cuando restaure el archivo de migración.

6. Autentíquese usando su método de inicio de sesión seguro elegido.
7. En la página Archivo de migración guardado, haga clic en **Finalizar**.

Restauración de certificados de Privacy Manager y contactos confiables

Para restaurar sus certificados de Privacy Manager y los Contactos Confiables en un equipo diferente como parte del proceso de migración o en el mismo equipo, siga estos pasos:

1. Abra Privacy Manager y haga clic en **Migración**.
2. Haga clic en **Restaurar**.
3. En la página Archivo de migración, haga clic en **Explorar** para buscar el archivo, y entonces haga clic en **Siguiente**.
4. Introduzca la contraseña que utilizó cuando creó el archivo de la copia de seguridad y luego haga clic en **Siguiente**.
5. En la página Archivo de migración guardado, haga clic en **Finalizar**.

Administración central de Privacy Manager

Su instalación de Privacy Manager puede ser parte de una instalación centralizada, que haya sido personalizada por su administrador. Uno o más de los siguientes recursos puede estar activado o desactivado:

- **Política de uso del certificado**: usted puede estar restringido al uso de los certificados de Privacy Manager emitidos por Comodo, o se le puede permitir el uso de certificados digitales emitidos por otras autoridades de certificación.
- **Política de encriptación**: los recursos de encriptación pueden estar activados o desactivados de forma individual en Microsoft Office u Outlook y en Windows Live Messenger.

10 File Sanitizer for HP ProtectTools

File Sanitizer es una herramienta que le permite triturar (eliminar definitivamente) de forma segura activos de datos (información o archivos personales, datos históricos o relacionados con Internet u otros componentes de datos) de su equipo y “desinfectar” periódicamente su unidad de disco duro.

NOTA: Esta versión de File Sanitizer sólo admite la unidad de disco duro del sistema.

Eliminación definitiva

La trituración es distinta de la eliminación estándar de Windows® (también denominada eliminación simple en File Sanitizer) ya que cuando se tritura un activo usando File Sanitizer se utiliza un algoritmo que oculta los datos, lo que hace que sea prácticamente imposible recuperar el activo original. Una eliminación simple de Windows puede dejar el archivo (o activo) intacto en la unidad de disco duro o en un estado que podría permitir su recuperación mediante la utilización de métodos especiales.

Al optar por la trituración de un archivo (seguridad máxima, media o baja), se selecciona automáticamente una lista predefinida de activos y un método de eliminación para efectuar el procedimiento. También puede personalizar un perfil de trituración, lo que le permite especificar el número de ciclos de eliminación, qué activos se incluirán en la trituración, qué activos deben confirmarse antes de ejecutar el procedimiento y qué activos deben excluirse de la trituración. Para obtener más información, consulte Selección o creación de un perfil de eliminación definitiva en la página 74.

Puede configurar una programación de trituración automática y también puede realizar este procedimiento manualmente en cualquier momento. Para obtener más información, consulte Programación de una eliminación definitiva en la página 73, Eliminación definitiva manual de un activo en la página 78 o Eliminación definitiva manual de todos los elementos seleccionados en la página 79.

NOTA: Un archivo .dll es eliminado totalmente y se lo retira del sistema sólo si se lo ha transferido a la papelera de reciclaje.

Limpieza para liberar espacio

La eliminación de un activo en Windows no elimina por completo el contenido del activo de su unidad de disco duro. Windows sólo elimina la referencia al activo. El contenido del activo aún continúa en la unidad de disco duro hasta que otro activo sobrescriba la misma área en la unidad de disco duro con información nueva.

La purificación de espacio libre le permite grabar con seguridad datos aleatorios sobre los activos eliminados, lo que evita que los usuarios puedan visualizar el contenido original del activo eliminado.

NOTA: La purificación de espacio libre es para aquellos activos que usted elimina usando la Papelera de reciclaje de Windows o cuando elimina manualmente un activo. La purificación de espacio libre no brinda seguridad adicional para los activos triturados.

Puede configurar una purificación de espacio libre automática o también puede activar el procedimiento manualmente usando el ícono de **HP ProtectTools** en el área de notificación, en el extremo derecho de la barra de tareas. Para obtener más información, consulte Programación de limpieza para liberar espacio en la página 74 o Activación manual de la limpieza para liberar espacio en la página 79.

Procedimientos de configuración

Apertura de File Sanitizer

Para abrir el File Sanitizer:

1. Haga clic en **Inicio**, **Todos los programas**, **HP** y en **HP ProtectTools Security Manager**.
2. Haga clic en **File Sanitizer**.

– o –

▲ Haga doble clic en el icono **File Sanitizer** ubicado en su escritorio.

– o –

▲ Haga clic con el botón derecho en el icono **HP ProtectTools** en el área de notificación, en el extremo derecho de la barra de tareas, haga clic en **File Sanitizer**, y luego haga clic en **Abrir File Sanitizer**.

Programación de una eliminación definitiva

NOTA: Para obtener información sobre un perfil de trituración predefinido o sobre la creación de un perfil de trituración, consulte Selección o creación de un perfil de eliminación definitiva en la página 74.

NOTA: Para obtener más información sobre la eliminación definitiva manual de activos, consulte Eliminación definitiva manual de un activo en la página 78.

1. Abra el File Sanitizer y haga clic en **Triturar**.
2. Seleccione una opción de trituración:
   - **Apagado de Windows**: Elija esta opción para triturar todos los activos seleccionados cuando se cierra Windows.

     NOTA: Cuando se selecciona esta opción, se muestra un cuadro de diálogo en el momento del cierre preguntando si desea continuar con la trituración de los activos seleccionados o si desea saltear este procedimiento. Haga clic en **Sí** para saltear el procedimiento de trituración o haga clic en **No** para continuar con el procedimiento.
   - **Abrir navegador web**: Elija esta opción para triturar todos los archivos seleccionados relacionados con Internet, como el historial de sitios visitados, cuando abre un explorador web.
   - **Salir navegador web**: Elija esta opción para triturar todos los archivos seleccionados relacionados con Internet, como el historial de sitios visitados, cuando cierra un explorador web.
   - **Secuencia de clave**: Elija esta opción para iniciar la trituración con una secuencia de teclas.
   - **Programador**: Seleccione la casilla de verificación **Activar Programador**, ingrese su contraseña de Windows y, a continuación, introduzca un día y un horario para triturar los activos seleccionados.

NOTA: Un archivo .dll es eliminado totalmente y se lo retira del sistema sólo si se lo ha transferido a la papelera de reciclaje.

3. Haga clic en **Aplicar** y, a continuación, haga clic en **Aceptar**.

Programación de limpieza para liberar espacio

NOTA: La purificación de espacio libre es para aquellos activos que usted elimina usando la Papelera de reciclaje de Windows o para los activos eliminados manualmente. La purificación de espacio libre no brinda seguridad adicional para los activos triturados.

Para configurar una programación de purificación de espacio libre:

1. Abra el File Sanitizer y haga clic en **Purificación de Espacio Libre**.
2. Seleccione la casilla de verificación **Activar Programador**, escriba su contraseña de Windows y luego ingrese un día y hora para blanquear su unidad de disco duro.
3. Haga clic en **Aplicar** y, a continuación, haga clic en **Aceptar**.

NOTA: La operación de purificación de espacio libre puede demandar un tiempo prolongado. Si bien la purificación de espacio libre se efectúa en segundo plano, su equipo puede funcionar más lentamente debido a un mayor uso del procesador.

Selección o creación de un perfil de eliminación definitiva

Puede especificar un método de borrado y seleccionar los activos que triturará seleccionado un perfil predefinido o creando su propio perfil.

Selección de un perfil de eliminación definitiva predefinido

Cuando elige un perfil de trituración predefinido (Seguridad máxima, Seguridad media o Seguridad baja), se seleccionan automáticamente un método de borrado y una lista de activos predefinidos. Puede hacer clic en el botón **Visualizar detalles** para visualizar la lista de activos predefinidos que se seleccionan para la trituración.

Para seleccionar un perfil de trituración predefinido:

1. Abra el 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 activos seleccionados para la trituración.
4. En **Triture lo siguiente**, seleccione la casilla de verificación al lado de cada activo que desea confirmar antes de la trituración.
5. Haga clic en **Aplicar** y, a continuación, haga clic en **Aceptar**.

Personalización de un perfil de eliminación definitiva

Al crear un perfil de trituración, usted especifica el número de ciclos de trituración, qué activos se incluyen en la trituración, qué activos se deben confirmar antes de la trituración y qué activos excluir de la trituración:

1. Abra el File Sanitizer y haga clic en **Configuración**, haga clic en **Configuración avanzada de seguridad**, y luego haga clic en **Visualizar detalles**.
2. Especifique la cantidad de ciclos de trituración.

NOTA: Se realizará el número de ciclos de trituración seleccionado para cada activo. Por ejemplo, si eligió tres ciclos de trituración, un algoritmo que oculta los datos se ejecutará tres veces por separado. Si elige el nivel de seguridad más alto, la trituración puede llevar mucho tiempo. Sin embargo, mientras mayor sea el número de ciclos de trituración que especifique, es menos posible que los datos puedan recuperarse.

3. Seleccione los activos que desee triturar:
   a. En **Opciones de trituración disponibles** haga clic en un activo y luego haga clic en **Agregar**.
   b. Para agregar un activo personalizado, haga clic en **Agregar Opción Personalizada**, y entonces navegue o escriba la ruta a la carpeta o al archivo. Haga clic en **Abrir** y, a continuación, haga clic en **Aceptar**. En **Opciones de trituración disponibles** haga clic en un activo personalizado y luego haga clic en **Agregar**.

NOTA: Para remover un activo de las opciones de trituración disponibles, haga clic en el activo, y entonces haga clic en **Eliminar**.

4. Debajo de **Triture lo siguiente**, marque la casilla de verificación al lado de cada activo que desee confirmar antes de su eliminación definitiva

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

5. Para proteger archivos y carpetas de la trituración, en la sección **No triture lo siguiente**, haga clic en **Agregar** y entonces navegue o escriba la ruta a la carpeta o al archivo. Haga clic en **Abrir** y, a continuación, haga clic en **Aceptar**.

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

6. Cuando finalice la configuración del perfil de trituración, haga clic en **Aplicar** y luego haga clic en **Aceptar**.

Personalización de un perfil de borrado simple

El perfil de eliminación simple realiza una eliminación de activo estándar sin realizar la trituración. Al personalizar un perfil de eliminación simple, puede especificar qué activos se incluirán en la eliminación simple, qué activos deben confirmarse antes de ejecutar el procedimiento y qué activos deben excluirse de la eliminación simple.

NOTA: Si usa la opción de borrado simple, la purificación de espacio libre puede realizarse ocasionalmente en los activos que se han borrado manualmente o por medio de la papelera de reciclaje de Windows.

Para personalizar un perfil de eliminación simple:

1. Abra el File Sanitizer y haga clic en **Configuración**, haga clic en **Configuración de Eliminación Simple** y luego haga clic en **Visualizar detalles**.
2. Seleccione los activos que desea eliminar:
   a. En **Opciones de trituración disponibles**, haga clic en un activo, y luego haga clic en **Agregar**.
   b. Para agregar un activo personalizado, haga clic en **Agregar Opción Personalizada**, escriba un nombre de archivo o carpeta y a continuación haga clic en **Aceptar**. Haga clic en el activo personalizado y luego haga clic en **Agregar**.

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

3. Debajo de **Triture lo siguiente**, marque la casilla de verificación al lado de cada activo que desee confirmar antes de su borrado.

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

4. Debajo de **No triture lo siguiente**, haga clic en **Agregar** para seleccionar los activos específicos que desea excluir de la eliminación definitiva.

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

5. Cuando finalice la configuración del perfil de eliminación simple, haga clic en **Aplicar** y luego haga clic en **Aceptar**.

Tareas generales

Puede usar File Sanitizer para realizar las siguientes tareas:

- Usar una secuencia de teclas para iniciar la eliminación definitiva: este recurso le permite crear una secuencia de teclas (por ejemplo, ctrl+alt+s) para iniciar la eliminación definitiva. Para obtener detalles, consulte Uso de una secuencia de teclas para iniciar la trituración en la página 77.
- Use el icono de File Sanitizer para iniciar la eliminación definitiva: este recurso es similar al de arrastrar y soltar en Windows. Para obtener detalles, consulte Uso del icono de File Sanitizer en la página 78.
- Eliminar definitivamente de forma manual un activo específico o todos los activos seleccionados: estos recursos le permiten eliminar definitivamente de forma manual los elementos sin esperar que se invoque la programación de eliminación definitiva regular. Para obtener detalles, consulte Eliminación definitiva manual de un activo en la página 78 o Eliminación definitiva manual de todos los elementos seleccionados en la página 79.
- Activar manualmente la limpieza para liberar espacio en disco: este recurso le permite activar manualmente la limpieza para liberar espacio en disco. Para obtener detalles, consulte Activación manual de la limpieza para liberar espacio en la página 79.
- Abortar una operación de eliminación definitiva o de limpieza para liberar espacio en disco: este recurso le permite detener la operación de eliminación definitiva o de limpieza para liberar espacio en disco. Para obtener detalles, consulte Interrupción de una operación de eliminación definitiva o de una limpieza para liberar espacio en la página 79.
- Ver los archivos de registro: este recurso le permite ver los archivos de registro de la eliminación definitiva o de la limpieza para liberar espacio en disco, los cuales contienen los errores o fallos de la última operación de eliminación definitiva o de limpieza para liberar espacio en disco. Para obtener detalles, consulte Visualización de los archivos de registro en la página 79.

NOTA: La operación de eliminación definitiva o de limpieza para liberar espacio en disco puede tardar considerablemente. Aunque la eliminación definitiva y la limpieza para liberar espacio en disco se realizan en segundo plano, su equipo puede funcionar más lentamente debido al aumento del uso del procesador.

Uso de una secuencia de teclas para iniciar la trituración

Para especificar una secuencia de teclas, siga estos pasos:

1. Abra el File Sanitizer y haga clic en **Triturar**.
2. Seleccione la casilla de verificación **Secuencia de clave**.
3. Ingrese un carácter en el cuadro de texto.
4. Seleccione la casilla de verificación **CTRL** o la casilla **ALT** y a continuación seleccione la casilla **mayús**.

   Por ejemplo, para iniciar la eliminación definitiva automática usando la tecla s y ctrl+mayús, escriba el carácter `s` en el cuadro de texto, y luego seleccione las casillas de verificación **CTRL** y **MAYÚS**.

NOTA: Asegúrese de seleccionar una secuencia de teclas que sea diferente de otras secuencias de teclas que haya configurado.

Para iniciar la trituración con una secuencia de teclas:

1. Mantenga presionadas las teclas mayús y ctrl o la tecla alt (o cualquier combinación que haya especificado) mientras presiona el carácter elegido.
2. Si se abre un cuadro de diálogo de confirmación, haga clic en **Sí**.

Uso del icono de File Sanitizer

△ **PRECAUCIÓN:** Los activos desaparecidos no pueden recuperarse. Considere cuidadosamente qué elementos selecciona para la desaparición manual.

1. Navegue hasta el documento o carpeta que desea triturar.
2. Arrastre el activo hasta el icono **File Sanitizer** en el escritorio.
3. Cuando se abra el cuadro de diálogo de confirmación, haga clic en **Sí**.

Eliminación definitiva manual de un activo

△ **PRECAUCIÓN:** Los activos desaparecidos no pueden recuperarse. Considere cuidadosamente qué elementos selecciona para la desaparición manual.

1. Haga clic con el botón derecho en el icono **HP ProtectTools** en el área de notificación, en el extremo derecho de la barra de tareas, haga clic en **File Sanitizer**, y luego haga clic en **Triturar uno**.
2. Cuando se abra el cuadro de diálogo Examinar, navegue al activo que desea desaparecer y luego haga clic en **Aceptar**.

   NOTA: El activo seleccionado debe ser un archivo o carpeta única.

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

– o –

1. Haga clic con el botón derecho del mouse en el ícono **File Sanitizer** en el escritorio y a continuación haga clic en **Triturar uno**
2. Cuando se abra el cuadro de diálogo Examinar, navegue hasta al activo que desea triturar y luego haga clic en **Aceptar**.
3. Cuando se abra el cuadro de diálogo de confirmación, haga clic en **Sí**.

– o –

1. Abra el File Sanitizer y haga clic en **Triturar**.
2. Haga clic en el botón **Navegar**.
3. Cuando se abra el cuadro de diálogo Examinar, navegue hasta al activo que desea triturar y luego haga clic en **Aceptar**.
4. Cuando se abra el cuadro de diálogo de confirmación, haga clic en **Sí**.

Eliminación definitiva manual de todos los elementos seleccionados

1. Haga clic con el botón derecho en el icono **HP ProtectTools** en el área de notificación, en el extremo derecho de la barra de tareas, haga clic en **File Sanitizer**, y luego haga clic en **Triturar Ahora**.
2. Cuando se abra el cuadro de diálogo de confirmación, haga clic en **Sí**.

– o –

1. Haga clic con el botón derecho del mouse en el icono **File Sanitizer** en el escritorio y a continuación haga clic en **Triturar Ahora**.
2. Cuando se abra el cuadro de diálogo de confirmación, haga clic en **Sí**.

– o –

1. Abra el File Sanitizer y haga clic en **Triturar**.
2. Haga clic en el botón **Triturar Ahora**.
3. Cuando se abra el cuadro de diálogo de confirmación, haga clic en **Sí**.

Activación manual de la limpieza para liberar espacio

1. Haga clic con el botón derecho en el icono **HP ProtectTools** en el área de notificación, en el extremo derecho de la barra de tareas, haga clic en **File Sanitizer**, y luego haga clic en **Purificar Ahora**.
2. Cuando se abra el cuadro de diálogo de confirmación, haga clic en **Sí**.

– o –

1. Abra el File Sanitizer y haga clic en **Purificación de Espacio Libre**.
2. Haga clic en **Purificar Ahora**.
3. Cuando se abra el cuadro de diálogo de confirmación, haga clic en **Sí**.

Interrupción de una operación de eliminación definitiva o de una limpieza para liberar espacio

Cuando se esté realizando una operación de eliminación definitiva o de limpieza para liberar espacio, se mostrará un mensaje arriba del icono de HP ProtectTool Security Manager en el área de notificación. El mensaje informa detalles sobre el proceso de eliminación definitiva o de limpieza para liberar espacio (el porcentaje efectuado) y le ofrece la opción de interrumpir la operación.

Para cancelar 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 realiza una operación de trituración o purificación de espacio libre, se generan archivos de registro de los errores o fallas. Los archivos de registro se actualizan siempre de acuerdo con la última operación de trituración o purificación de espacio libre.

NOTA: Los archivos que se eliminan totalmente o se blanquean con éxito no aparecen en los archivos de registro.

Se crea un archivo de registro para las operaciones de trituración y otro para las operaciones de purificación de espacio libre. Ambos archivos de registro se encuentran 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

11 Device Access Manager for HP ProtectTools (sólo en algunos modelos)

Los administradores del sistema operativo Windows® usan Device Access Manager for HP ProtectTools para controlar el acceso a los dispositivos en el sistema y para proteger contra el acceso no autorizado:

- Los perfiles de los dispositivos se crean para cada usuario con el fin de definir los dispositivos para los cuales el acceso es permitido o denegado.
- Los usuarios también se organizan en grupos, por ejemplo, el grupo de Administradores de dispositivos predefinido. También se pueden definir grupos usando la opción Administración de equipos de la sección Herramientas administrativas en el Panel de control.
- Se puede conceder o negar el acceso con base en la pertenencia a un grupo.
- En el caso de clases de dispositivos como unidades de CD-ROM y unidades de DVD, se puede permitir o negar el acceso a la lectura y el acceso a la escritura por separado.

A los usuarios limitados también se les puede otorgar el permiso de leer y modificar la política de control de acceso al dispositivo.

Procedimientos de configuración

Apertura de Device Access Manager

Para abrir Device Access Manager, siga estos pasos:

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

Configuración del acceso a los dispositivos

Device Access Manager for HP ProtectTools ofrece tres opciones:

- La Configuración sencilla se usa para permitirles o negarles el acceso a clases de dispositivos a los miembros del grupo Administradores de dispositivos.
- La Configuración de clases de dispositivo se usa para conceder o negar el acceso a tipos de dispositivos o a dispositivos específicos a usuarios o grupos específicos.
- La Configuración de acceso de usuario se usa para especificar cuáles usuarios pueden ver o modificar la información de la Configuración sencilla y de la Configuración de clases de dispositivo.

Grupo de administradores de dispositivos

Cuando se instala Device Access Manager, se crea un grupo de administradores de dispositivos.

El administrador del sistema puede implementar una política simple de control de acceso a los dispositivos al negar el acceso a un conjunto de dispositivos específicos a menos que el usuario sea clasificado como confiable (con relación al acceso al dispositivo). La forma recomendada de distinguir entre usuarios “confiables para el dispositivo” y usuarios “no confiables para el dispositivo” es hacer a todos los usuarios “confiables para el dispositivo” miembros del grupo de Administradores de dispositivos. El hecho de concederle al grupo de Administradores de dispositivos acceso a los dispositivos mediante la Configuración sencilla o la Configuración de clases de dispositivos, asegurará que todos los usuarios "confiables para el dispositivo" tengan acceso total al conjunto especificado de clases de dispositivos.

NOTA: El hecho de añadir un usuario al grupo de Administradores de dispositivos no le permite a este usuario acceder automáticamente a los dispositivos. Sin embargo, la Configuración sencilla se puede usar para conceder acceso al conjunto requerido de clases de dispositivos para usuarios “confiables para el dispositivo”.

Para agregar usuarios al grupo de Administradores de dispositivos, siga estos pasos:

- Para Windows 7, Vista, o XP Professional, use el componente MMC estándar “Usuarios y grupos locales”.
- En el caso de las versiones domésticas de Windows 7, Vista® o XP, a partir de una cuenta con privilegios, escriba lo siguiente en una ventana de comandos:

```
c:\> net localgroup “Device Administrators” username /ADD
```

Configuración sencilla

Los administradores y usuarios autorizados pueden usar la Configuración sencilla para modificar el acceso a las siguientes clases de dispositivos para todos los que no son administradores de dispositivos:

NOTA: Con el fin de usar esta opción para leer la información de acceso a un dispositivo, al usuario o grupo se le debe conceder acceso de "lectura" en la **Configuración de acceso de usuario**. Con el fin de usar esta opción para modificar la información de acceso a un dispositivo, al usuario o grupo se le debe conceder acceso de "cambio" en la **Configuración de acceso de usuario**.

- Todos los medios extraíbles (discos flexibles, unidades flash USB, etc.)
- Todas las unidades de DVD/CD-ROM
- Todos los puertos en serie y paralelos
- Todos los dispositivos Bluetooth®
- Todos los dispositivos infrarrojos
- Todos los dispositivos de módem
- Todos los dispositivos PCMCIA
- Todos los dispositivos 1394

Para permitir o denegar el acceso a una clase de dispositivos a todos aquellos que no sean Administradores de dispositivos, siga estos pasos:

1. En el panel izquierdo de la **Consola administrativa de HP ProtectTools**, haga clic en **Device Access Manager** y luego en **Configuración sencilla**.
2. En el panel de la derecha, para denegar el acceso, seleccione la casilla de verificación para una clase de dispositivos o para un dispositivo específico. Desmarque la casilla de verificación para permitir el acceso a esta clase de dispositivos o a un dispositivo específico.

   Si la casilla de verificación se ve de color gris, esto indica que los valores que afectan el escenario de acceso han sido modificados dentro de la Configuración por clases de dispositivo. Para restablecer los valores a la configuración sencilla, haga clic en la casilla de verificación para desmarcarla o para seleccionarla y luego haga clic en **Sí** para confirmar.
3. Haga clic en el icono **Guardar**.

   NOTA: Si el servicio en segundo plano no está en ejecución, se abre un cuadro de diálogo para preguntarle si desearía iniciarlo. Haga clic en **Sí**.
4. Haga clic en **Aceptar**.

Inicio del servicio en segundo plano

Antes de que se puedan aplicar los perfiles de dispositivos, HP ProtectTools Security Manager abre un cuadro de diálogo para preguntarle si le gustaría iniciar el servicio en segundo plano de bloqueo/auditoría de dispositivos de HP ProtectTools. Haga clic en **Sí**. El servicio en segundo plano se inicia y a partir de entonces se iniciará automáticamente cada vez que el sistema arranque.

NOTA: Se debe definir un perfil del dispositivo antes de que se muestre el mensaje de solicitud del servicio en segundo plano.

Los administradores pueden también iniciar o detener este servicio:

1. Haga clic en **Inicio** y luego en **Panel de control**.
2. Haga clic en **Herramientas administrativas** y luego en **Servicios**.
3. Busque el servicio de **Bloqueo de dispositivos/auditoría de HP ProtectTools**.

Detener el servicio de Bloqueo de dispositivos/auditoría de HP ProtectTools no detiene el bloqueo del dispositivo. Dos componentes refuerzan el bloqueo del dispositivo:

- Servicio de Bloqueo de dispositivos/auditoría
- Controlador DAMDrv.sys

El inicio del servicio inicia el controlador del dispositivo, pero si se detiene el servicio no se detiene el controlador.

Para determinar si está en ejecución el servicio en segundo plano, abra la ventana de comando y escriba sc query flcdlock.

Para determinar si está en ejecución el controlador del dispositivo, abra la ventana de comando y escriba sc query damdrv.

Configuración por clases de dispositivo

Los administradores y los usuarios autorizados pueden ver y modificar la lista de los usuarios y grupos a los que se les ha permitido o negado el permiso para acceder a clases de dispositivos o dispositivos en específico.

NOTA: Con el fin de usar esta opción para leer la información de acceso a un dispositivo, al usuario o grupo se le debe conceder acceso de "lectura" en la **Configuración de acceso de usuario**. Con el fin de usar esta opción para modificar la información de acceso a un dispositivo, al usuario o grupo se le debe conceder acceso de "cambio" en la **Configuración de acceso de usuario**.

La Configuración por clases de dispositivo cuenta con las siguientes secciones:

- **Lista de dispositivos**: muestra todas las clases de dispositivos y los dispositivos que están instalados en el sistema o que pueden haber sido instalados en el sistema anteriormente.
  - Generalmente se aplica la protección a una clase de dispositivos. Un usuario o grupo seleccionado tendrá la capacidad de acceder a cualquier dispositivo en la clase de dispositivos.
  - La protección también se puede aplicar a dispositivos específicos.
- **Lista de usuarios**: muestra todos los usuarios y grupos de usuarios que tienen acceso permitido o negado a una clase de dispositivos seleccionada o a un dispositivo específico.
  - La entrada en la Lista de usuarios puede hacerse para un usuario específico o para un grupo del que dicho usuario forme parte.
  - Si la entrada de un usuario o un grupo en la Lista de usuarios no está disponible, la configuración ha sido heredada de la clase de dispositivo en la Lista de dispositivos o de la carpeta Clases.
  - Algunas clases de dispositivos, como DVD y CD-ROM, pueden controlarse mejor permitiendo o negando el acceso a operaciones de lectura y escritura de forma separada.

Así como sucede con otros dispositivos y clases, los derechos de lectura y escritura pueden ser heredados. Por ejemplo, el acceso de Lectura puede ser heredado de una clase superior, pero el acceso de Escritura puede negársele específicamente a un usuario o grupo.

NOTA: Si la casilla de verificación de Lectura está en blanco, entonces la entrada de control de acceso no tiene efecto en el acceso de lectura al dispositivo. Esta ni concede ni niega el acceso de lectura al dispositivo.

Ejemplo 1, si a un usuario o grupo se le niega el acceso de escritura a un dispositivo o clase de dispositivos:

Al mismo usuario, al mismo grupo, o a un miembro del mismo grupo se le puede conceder acceso de escritura o acceso de sólo lectura+escritura a un dispositivo que esté debajo de este dispositivo en la jerarquía.

Ejemplo 2, si a un usuario o grupo se le permite el acceso de escritura a un dispositivo o clase de dispositivos:

Al mismo usuario, al mismo grupo, o a un miembro del mismo grupo se le puede negar el acceso de escritura o el acceso de sólo lectura+escritura al mismo dispositivo o a un dispositivo que esté debajo de este dispositivo en la jerarquía.

Ejemplo 3, si a un usuario o grupo se le permite el acceso de lectura a un dispositivo o clase de dispositivos:

Al mismo usuario, al mismo grupo, o a un miembro del mismo grupo se le puede negar el acceso de lectura o el acceso de sólo lectura+escritura al mismo dispositivo o a un dispositivo que esté debajo de este dispositivo en la jerarquía.

Ejemplo 4, si a un usuario o grupo se le niega el acceso de lectura a un dispositivo o clase de dispositivos:

Al mismo usuario, al mismo grupo, o a un miembro del mismo grupo se le puede conceder acceso de lectura o acceso de sólo lectura+escritura a un dispositivo que esté debajo de este dispositivo en la jerarquía.

Ejemplo 5, si a un usuario o grupo se le permite el acceso de lectura+escritura a un dispositivo o clase de dispositivos:

Al mismo usuario, al mismo grupo, o a un miembro del mismo grupo se le puede negar el acceso de escritura o el acceso de sólo lectura+escritura al mismo dispositivo o a un dispositivo que esté debajo de este dispositivo en la jerarquía.

Ejemplo 6, si a un usuario o grupo se le niega el acceso de lectura+escritura a un dispositivo o clase de dispositivos:

Al mismo usuario, al mismo grupo, o a un miembro del mismo grupo se le puede conceder acceso de lectura o acceso de sólo lectura+escritura a un dispositivo que esté debajo de este dispositivo en la jerarquía.

Negación del acceso a un usuario o grupo

Para evitar que un usuario o grupo acceda a un dispositivo o clase de dispositivos, siga estos pasos:

1. En el panel izquierdo de la **Consola administrativa de HP ProtectTools**, haga clic en **Device Access Manager** y luego en **Configuración de clases de dispositivo**.
2. En la lista de dispositivos, haga clic en la clase de dispositivo que desea configurar.
   - Clase de dispositivos
   - Todos los dispositivos
   - Dispositivo individual
3. Debajo de **Usuarios/Grupos**, haga clic en el usuario o grupo al que desea negarle el acceso.
4. Haga clic en **Denegar** al lado de un usuario o grupo.
5. Haga clic en el icono **Guardar**.

NOTA: Cuando se establecen las configuraciones de negar y permitir en el mismo nivel de dispositivo para un usuario, la negación del acceso prevalece sobre el acceso permitido.

Permitir el acceso de un usuario o grupo

Para conceder permiso a un usuario o grupo para acceder a un dispositivo o clase de dispositivos, siga estos pasos:

1. En el panel izquierdo de la **Consola administrativa de HP ProtectTools**, haga clic en **Device Access Manager** y luego en **Configuración de clases de dispositivo**.
2. En la lista de dispositivos, haga clic en una de las siguientes opciones:
   - Clase de dispositivos
   - Todos los dispositivos
   - Dispositivo individual
3. Haga clic en **Agregar**.

   Se abre el cuadro de diálogo **Seleccionar usuarios o grupos**.
4. Haga clic en **Avanzado** y a continuación en **Buscar ahora** para buscar usuarios o grupos para agregar.
5. Haga clic en un usuario o grupo que se vaya a añadir a la lista de usuarios y grupos disponibles y luego haga clic en **Aceptar**.
6. Haga clic en **Aceptar** nuevamente.
7. Haga clic en **Permitir** para concederle el acceso a este usuario o grupo.
8. Haga clic en el icono **Guardar**.

Quitar el acceso de un usuario o grupo

Para quitarle el permiso a un usuario o grupo de acceder a un dispositivo o clase de dispositivos, siga estos pasos:

1. En el panel izquierdo de la **Consola administrativa de HP ProtectTools**, haga clic en **Device Access Manager** y luego en **Configuración de clases de dispositivo**.
2. En la lista de dispositivos, haga clic en la clase de dispositivo que desea configurar.
   - Clase de dispositivos
   - Todos los dispositivos
   - Dispositivo individual
3. Debajo de **Usuario/grupos**, haga clic en el usuario o grupo al que desea quitarle el acceso y luego haga clic en **Quitar**.
4. Haga clic en el icono **Guardar**.

Permitirle el acceso a una clase de dispositivos a un usuario de un grupo

Para permitirle a un usuario que acceda a una clase de dispositivos y a la vez negarle el acceso a todos los otros miembros de ese grupo de usuarios, siga estos pasos:

1. En el panel izquierdo de la **Consola administrativa de HP ProtectTools**, haga clic en **Device Access Manager** y luego en **Configuración de clases de dispositivo**.
2. En la lista de dispositivos, haga clic en la clase de dispositivo que desea configurar.
   - Clase de dispositivos
   - Todos los dispositivos
   - Dispositivo individual
3. Debajo de **Usuarios/grupos**, haga clic en el grupo al que desea negarle el acceso y luego haga clic en **Denegar**.
4. Navegue a la carpeta debajo de la clase requerida y adicione entonces al usuario específico.
5. Haga clic en **Permitir** para concederle el acceso a este usuario.
6. Haga clic en el icono **Guardar**.

Permitirle el acceso a un dispositivo específico a un usuario de un grupo

Los administradores le pueden conceder a un usuario el acceso a un dispositivo específico y a la vez negarles el acceso a todos los otros miembros del grupo de ese usuario a los dispositivos de la clase:

1. En el panel izquierdo de la **Consola administrativa de HP ProtectTools**, haga clic en **Device Access Manager** y luego en **Configuración de clases de dispositivo**.
2. En la lista de dispositivos, haga clic en la clase de dispositivos que desea configurar y luego navegue a la carpeta debajo de esta.
3. Haga clic en **Agregar**. Se abre el cuadro de diálogo **Seleccionar usuarios o grupos**.

4. Haga clic en **Avanzado** y luego en **Buscar ahora** para buscar el grupo de usuarios al que se le negará el acceso a todos los dispositivos de la clase.
5. Haga clic en el grupo y luego en **Aceptar**.
6. Navegue al dispositivo específico debajo de la clase de dispositivos al cual se le permitirá el acceso al usuario.
7. Haga clic en **Agregar**. Se abre el cuadro de diálogo **Seleccionar usuarios o grupos**.
8. Haga clic en **Avanzado** y a continuación en **Buscar ahora** para buscar usuarios o grupos para agregar.
9. Haga clic en el usuario al que se le permitirá el acceso y luego en **Aceptar**.
10. Haga clic en **Permitir** para concederle el acceso a este usuario.
11. Haga clic en el icono **Guardar**.

Restablecimiento de la configuración

△ **PRECAUCIÓN:** El restablecimiento de la configuración desecha todos los cambios que se han realizado en la configuración del dispositivo y restaura todos los valores establecidos de fábrica.

Para restablecer la configuración a los valores de fábrica, siga estos pasos:

1. En el panel izquierdo de la **Consola administrativa de HP ProtectTools**, haga clic en **Device Access Manager** y luego en **Configuración de clases de dispositivo**.
2. Haga clic en el botón **Restablecer**.
3. Haga clic en **Sí** para confirmar.
4. Haga clic en el icono **Guardar**.

Tareas avanzadas

Control del acceso a la configuración

En **Configuración de acceso de usuario**, los administradores especifican los grupos o usuarios que están autorizados a usar las páginas Configuración sencilla y Configuración de clases de dispositivo.

NOTA: Un usuario o grupo debe tener "Derechos plenos de administrador usuario" para poder modificar los valores de la Configuración de acceso de usuario.

- A un usuario o grupo se le debe conceder acceso a “Ver (apenas para lectura) los valores de la configuración” en la Configuración de acceso de usuario para ver la información de la Configuración sencilla y la Configuración de clases de dispositivo.
- A un usuario o grupo se le debe conceder acceso a “Cambiar las opciones de configuración” en la Configuración de acceso de usuario para modificar la información de la Configuración sencilla y la Configuración de clases de dispositivo.

NOTA: Incluso los miembros del grupo de Administradores necesitan tener derecho de acceso de "lectura" para ver la Configuración sencilla y la Configuración por clases de dispositivo y derecho de acceso de "cambio" para cambiar datos utilizando la Configuración sencilla y la Configuración de clases de dispositivo.

NOTA: Después de evaluar los niveles de acceso de todos los usuarios y grupos, si un usuario no ha seleccionado Permitir o Denegar para un nivel de acceso en particular, al usuario se le niega el acceso a este nivel.

Concesión de acceso a un grupo o usuario existente

Para concederle permiso a un grupo o usuario para ver o cambiar los valores de la configuración, siga estos pasos:

1. En el panel izquierdo de la **Consola administrativa de HP ProtectTools**, haga clic en **Device Access Manager** y luego en **Configuración de acceso de usuario**.
2. Haga clic en un grupo o usuario para permitirle el acceso.
3. En **Permisos**, haga clic en **Permitir** para cada tipo de permiso que se le concederá al grupo o usuario seleccionado:

   NOTA: Los permisos concedidos son acumulativos. Por ejemplo, a un usuario al que se le concede el derecho de “Cambiar las opciones de configuración”, se le concede automáticamente el permiso “Ver (sólo lectura) los valores de configuración”. A un usuario al que se le conceden “Todos los derechos del usuario-administrador” también se le conceden los permisos “Cambiar las opciones de configuración” y “Ver (sólo lectura) los valores de configuración”.

   - Todos los derechos del usuario-administrador
   - Cambiar las opciones de configuración
   - Ver (sólo lectura) los valores de la configuración
4. Haga clic en el icono **Guardar**.

Negación del acceso a un grupo o usuario existente

Para negarle el permiso a un grupo o usuario para ver o cambiar los valores de la configuración, siga estos pasos:

1. En el panel izquierdo de la **Consola administrativa de HP ProtectTools**, haga clic en **Device Access Manager** y luego en **Configuración de acceso de usuario**.
2. Haga clic en un grupo o usuario para negarle el acceso.
3. En **Permisos**, haga clic en **Denegar** para cada tipo de permiso que se le negará al grupo o usuario seleccionado:
   - Todos los derechos del usuario-administrador
   - Cambiar las opciones de configuración
   - Ver (sólo lectura) los valores de la configuración
4. Haga clic en el icono **Guardar**.

Agregar un nuevo grupo o usuario

Para concederle permiso a un nuevo grupo o usuario para ver o cambiar los valores de la configuración, siga estos pasos:

1. En el panel izquierdo de la **Consola administrativa de HP ProtectTools**, haga clic en **Device Access Manager** y luego en **Configuración de acceso de usuario**.
2. Haga clic en **Agregar**. Se abre el cuadro de diálogo **Seleccionar usuarios o grupos**.
3. Haga clic en **Avanzado** y a continuación en **Buscar ahora** para buscar usuarios o grupos para agregar.
4. Haga clic en un grupo o usuario, luego en **Aceptar** y después haga clic en **Aceptar** otra vez.
5. Haga clic en **Permitir** para concederle el acceso a este usuario.
6. Haga clic en el icono **Guardar**.

Quitar el acceso de un grupo o usuario

Para quitarle el permiso a un grupo o usuario de ver o cambiar los valores de la configuración, siga estos pasos:

1. En el panel izquierdo de la **Consola administrativa de HP ProtectTools**, haga clic en **Device Access Manager** y luego en **Configuración de acceso de usuario**.
2. Haga clic en un grupo o usuario y a continuación haga clic en **Quitar**.
3. Haga clic en el icono **Guardar**.

Documentación relacionada

Device Access Manager for ProtectTools es compatible con el producto empresarial HP ProtectTools Enterprise Device Access Manager. Al trabajar con el producto empresarial, Device Access Manager for HP ProtectTools permite el acceso apenas para lectura a sus propios recursos.

Hay más información sobre Device Access Manager for HP ProtectTools en la Web en http://www.hp.com/hps/security/products.

12 LoJack Pro for HP ProtectTools

La línea Absolute Software de los productos Computrace les permite a los usuarios rastrear sus equipos HP y mejorar la protección de los datos. Los productos Computrace LoJack reducen los extravíos de máquinas y se destinan a la recuperación de máquinas robadas.

Para activar el producto Computrace, siga estas instrucciones:

1. Haga clic en **Inicio**, **Todos los programas** y entonces en **HP ProtectTools Security Manager**.
2. Haga clic en **Recuperación en caso de robo**, y luego haga clic en **Activar ahora**.

   Su navegador web predeterminado abre la suscripción a un sitio web en el cual usted puede seleccionar y comprar uno de los tres productos Computrace disponibles con HP ProtectTools:

   - **Computrace Data Delete**: incluye la eliminación remota de datos, el congelamiento del dispositivo y rastreo básico de activos e informe.
   - **Computrace LoJack Pro**: incluye la eliminación remota de datos, el congelamiento del dispositivo, el rastreo básico de activos e informe y la administración de la recuperación en caso de robo.
   - **Computrace LoJack Pro Premium**: incluye la eliminación remota de datos, el congelamiento del dispositivo, el rastreo avanzado de activos e informes, la ubicación y el cerco geográfico y la administración de la recuperación en caso de robo.

Computrace Agent está incorporado al BIOS de las HP business notebooks, aunque el agente está desactivado cuando se envía el equipo. Después de comprar su suscripción, se puede activar el agente. El agente incorporado es capaz de reinstalar el sistema operativo y de reformatear los discos duros.

NOTA: Hay periodos de suscripción disponibles de 1 a 5 años. Consulte el acuerdo de suscripción del software de Absolute para obtener detalles adicionales. El recurso de recuperación depende de su ubicación geográfica. El rastreo por GPS tiene soporte en determinados modelos con la opción de WWAN.

13 Solución de problemas

HP ProtectTools Security Manager

Breve descripción	Detalles	Solución
Las smart cards y tokens USB no están disponibles en Security Manager si se instalan después de la instalación de Security Manager.	Para usar Smart Cards o tokens USB en Security Manager, el software de soporte (controladores, proveedores PKCS#11, etc.) debe instalarse antes de la instalación de Security Manager. Si ya ha instalado Security Manager, siga estos pasos después de la instalación del software para soporte de smart card o token:	Inicie la sesión en el Administrador de contraseñas. En HP ProtectTools Security Manager, haga clic en **Administrador de contraseñas**, luego en **Credenciales** y después en **Smart Card** Si se le indica, reinicie el equipo.
Algunas páginas web de aplicaciones crean errores que evitan que el usuario realice o complete tareas.	Algunas aplicaciones basadas en la web dejan de funcionar e informan errores debido al patrón de funcionalidad de desactivación de Single Sign On (Inicio de sesión único). Por ejemplo, un **!** dentro de un triángulo amarillo en Internet Explorer indica que se ha producido un error.	Single Sign On de Security Manager no admite todas las interfaces Web de software. Desactive el soporte de Single Sign On para las páginas Web específicas apagando el soporte de Single Sign On. Vea la documentación completa sobre Single Sign On disponible en los archivos de ayuda del software Security Manager. Si no puede desactivarse un Single Sign On (Inicio de sesión único) específico para una aplicación dada, llame a asistencia técnica de HP y solicite soporte de tercer nivel a través de su contacto de Servicio de HP.
La opción **Browse for Virtual Token** (Buscar token virtual) no aparece durante el proceso de inicio de sesión.	El usuario no puede cambiar la localidad de un token virtual registrado en el Administrador de contraseñas porque la opción de explorar fue eliminada para reducir los riesgos de seguridad.	Se eliminó la opción de buscar porque permitía que los no usuarios borraran y cambiaran el nombre de los archivos y tomaran el control de Windows.
Los administradores de dominio no pueden cambiar la contraseña de Windows ni siquiera con autorización.	Esto sucede después de que un administrador de dominio inicia sesión en un dominio y registra la identidad del dominio con el Administrador de contraseñas usando una cuenta con derechos de Administrador en el dominio y en el equipo local. Cuando el administrador de dominio trata de cambiar la contraseña de Windows en el Administrador de contraseñas, el administrador obtiene una falla de error en el inicio de sesión: **Restricción de cuenta de usuario**.	El Administrador de contraseñas no puede cambiar la contraseña de la cuenta de un usuario de dominio a través de **Cambiar contraseña de Windows**. Security Manager sólo puede cambiar las contraseñas de cuentas de equipos locales. El usuario de dominio puede cambiar su contraseña a través de la opción **Cambiar contraseña** de **Seguridad de Windows**, pero como el usuario de dominio no tiene una cuenta física en el equipo local, el Administrador de contraseñas sólo puede cambiar la contraseña utilizada para iniciar la sesión.
El Administrador de contraseñas tiene problemas de	Si el usuario inicia sesión en el Administrador de contraseñas, crea un documento en WordPerfect y lo guarda	HP está investigando una solución para mejorías futuras del producto.

Breve descripción	Detalles	Solución
incompatibilidad con la contraseña GINA en WordPerfect de Corel.	con protección por contraseña, el Administrador de contraseñas no puede detectar o reconocer, ya sea de forma manual o automática, la contraseña GINA.	
El Administrador de contraseñas no reconoce el botón **Conectar** en la pantalla.	Si las credenciales de Single Sign On (Inicio de sesión único) para Conexión remota de escritorio (Remote Desktop Connection, RDP) están configuradas en **Conectar**, cuando se reinicia Single Sign On (Inicio de sesión único), siempre ingresa **Guardar como** en lugar de **Conectar**.	HP está investigando una solución para mejorías futuras del producto.
Solamente en Windows XP Service Pack 1, el usuario no puede iniciar sesión en el Administrador de contraseñas después de pasar del modo de espera al modo de hibernación.	Después de permitirle al sistema hacer la transición entre los modos de hibernación y suspensión, el administrador o usuario no puede iniciar sesión en el Administrador de contraseñas y la pantalla de inicio de sesión en Windows se mantiene en exhibición independientemente de la credencial de inicio de sesión que se seleccione (contraseña, huella digital o Java Card).	Actualice Windows a Service Pack 2 a través de Windows Update. Consulte el artículo 813301 de la base de conocimiento de Windows en http://www.microsoft.com para obtener más información sobre el motivo del problema. Para iniciar sesión, el usuario debe seleccionar el Administrador de contraseñas e iniciar sesión. Después de iniciar sesión en el Administrador de contraseñas, se le solicita al usuario que inicie sesión en Windows (puede ser que el usuario tenga que seleccionar la opción de inicio de sesión en Windows) para completar el proceso de inicio de sesión. Si el usuario inicia primero la sesión en Windows, debe iniciar sesión manualmente en el Administrador de contraseñas.
El proceso de seguridad **Restore Identity (Restaurar identidad)** pierde la asociación con el token virtual.	Cuando el usuario restaura la identidad, el Administrador de contraseñas puede perder la asociación con la ubicación del token virtual en la pantalla de inicio de sesión. Aunque el Administrador de contraseñas tenga el token virtual registrado, el usuario debe volver a registrar el token para restaurar la asociación.	Esto es actualmente debido al diseño. Al desinstalar Security Manager sin conservar las identidades, se destruye la parte del sistema (servidor) del token, de modo que el token no se puede usar más para iniciar sesión, incluso si la parte cliente del token se restaura mediante la restauración de identidad. HP está investigando opciones de resolución a largo plazo.

Device Access Manager for HP ProtectTools

Se ha negado a algunos usuarios el acceso a dispositivos dentro de Device Access Manager, pero los dispositivos todavía están accesibles.

- **Explicación**: Se utilizó Configuración sencilla y/o Configuración de clases de dispositivo dentro de Device Access Manager para denegar a usuarios el acceso a dispositivos. A pesar de que se negó el acceso, los usuarios aún pueden acceder a los dispositivos.
- **Solución:**
  - Verifique que el servicio Bloqueo de dispositivos/auditoría de HP ProtectTools se haya iniciado.
  - Como usuario administrativo, haga clic en **Panel de control** y a continuación en **Sistema y mantenimiento**. En la ventana de herramientas administrativas, haga clic en **Servicios** y busque el servicio **Bloqueo de dispositivos/auditoría de HP ProtectTools**. Asegúrese de que el servicio se haya iniciado y que el tipo de inicio esté en **Automático**.

Un usuario tiene acceso inesperado a un dispositivo o se niega a un usuario el acceso a un dispositivo de forma inesperada.

- **Explicación**: Se utilizó Configuración sencilla y/o Configuración de clases de dispositivo dentro de Device Access Manager para denegar a usuarios el acceso a dispositivos. Cuando un usuario está usando el sistema, puede acceder a dispositivos a los que cree que Device Access Manager le ha negado el acceso y se le niega acceso a dispositivos que cree que Device Access Manager debería permitir.
- **Solución:**
  - Use Configuración de clases de dispositivo dentro de Device Access Manager para investigar las configuraciones de dispositivo del usuario.
  - Haga clic en **Security Manager**, en **Device Manager** y, a continuación, haga clic en **Configuración de clases de dispositivo**. Expanda los niveles del árbol de clase de dispositivo y revise las configuraciones aplicables a este usuario. Verifique si hay permisos negados al usuario o a cualquier grupo de Windows del que el usuario forme parte, como Usuarios, Administradores, etc.

Permitir o denegar: ¿qué tiene precedencia?

- **Explicación**: en Configuración de clases de dispositivos, se definió la siguiente configuración:
  - Se otorgó permiso a un grupo de Windows (como BUILTIN\Administradores) y se negó el permiso a otro grupo de Windows (como BUILTIN\Usuarios) en el mismo nivel de jerarquía de clase de dispositivo (como las unidades de DVD/CD-ROM).
  - Si un usuario es miembro de ambos grupos (por ejemplo Administrador), ¿cuál tiene precedencia?
- **Solución:**
  - Se ha negado el acceso al dispositivo. Denegar tiene precedencia sobre Permitir.
  - Se negó el acceso debido a la forma en que Windows concede el permiso efectivo para el dispositivo. Se niega a un grupo y se permite a otro, pero el usuario es miembro de ambos grupos. Se niega el acceso al usuario porque se le dio prioridad a la negación sobre el permiso.

- Una forma de resolver este problema es denegar el acceso al grupo de Usuarios en el nivel de las unidades de DVD/CD-ROM y permitir el acceso al grupo de Administradores a un nivel por debajo de las unidades de DVD/CD-ROM.
- Una solución alternativa es crear grupos de Windows específicos, uno para permitir el acceso a las unidades de DVD/CD y otro para negar el acceso a dichas unidades. Entonces se agregarán los usuarios específicos al grupo apropiado.

Se utilizó la vista Configuración sencilla para definir la política de control de acceso a los dispositivos pero los usuarios administrativos no pueden acceder a los dispositivos.

- **Explicación**: Configuración sencilla niega el acceso a los usuarios y los invitados y permite el acceso a los administradores del dispositivo.
- **Solución:** Agregue el usuario administrativo al grupo de Administradores del dispositivo.

Varios

Software afectado: breve descripción	Detalles	Solución
Security Manager-Advertencia recibida: **Esta aplicación de seguridad no puede instalarse sin que esté instalado previamente HP ProtectTools Security Manager**.	Todas las aplicaciones de seguridad como Java Card Security y la biometría son plug-ins expansibles para la interfaz de Security Manager. Security Manager se debe instalar antes de que se pueda cargar un plug-in de seguridad aprobado por HP.	El software Security Manager debe estar instalado antes de instalar cualquier complemento de seguridad.
HP ProtectTools Security Manager: intermitentemente, se devuelve un error cuando se cierra la interfaz de Security Manager.	Intermitentemente (1 en 12 casos), se crea un error al utilizar el botón Cerrar en el ángulo superior derecho de la pantalla para cerrar Security Manager antes de que todas las aplicaciones complementarias hayan completado la carga.	Esto responde a una dependencia del tiempo en el tiempo de carga de los servicios complementarios cuando se cierra y reinicia Security Manager. Debido a que PTHOST.exe es el shell que contiene a las otras aplicaciones (complementarias), depende de la capacidad del complemento para completar su tiempo de carga (servicios). El cierre del shell antes de que el complemento haya tenido tiempo de completar la carga es la causa fundamental. Permita que Security Manager complete el mensaje de carga de los servicios (que se ve en la parte superior de la ventana de Security Manager) y todos los complementos enumerados en la columna izquierda. Para evitar una falla, permita un tiempo razonable para que se carguen estos complementos.
HP ProtectTools: el acceso irrestricto o privilegios de administrador no controlados plantean un riesgo de seguridad.	Son posibles numerosos riesgos con el acceso irrestricto al equipo cliente, incluidos los siguientes: • Eliminación de la PSD • Modificación malintencionada de la configuración del usuario • Desactivación de las políticas y funciones de seguridad	Se estimula a los administradores a seguir las “mejores prácticas” en la restricción de los privilegios de los usuarios finales y en la restricción del acceso de los usuarios. A los usuarios no autorizados no se les debe conceder privilegios administrativos.

Glosario

Activación La tarea debe completarse antes de que se pueda acceder a las funciones de Drive Encryption. Drive Encryption se activa mediante el asistente de configuración de HP ProtectTools. Sólo un administrador puede activar Drive Encryption. El proceso de activación consiste en la activación del software, la encriptación de la unidad, la creación de una cuenta de usuario y la creación de la copia de seguridad inicial de la clave de encriptación en un dispositivo de almacenamiento extraíble.

Activo Un componente de datos que consiste en información o archivos personales, datos históricos y relacionados con la web, etc., que se encuentra en la unidad de disco duro.

Administrador *Ver* administrador de Windows.

Administrador de Windows Un usuario con todos los derechos para modificar los permisos y administrar a otros usuarios.

Archivo de recuperación de emergencia Área de almacenamiento protegida que permite volver a encriptar claves de usuarios básicos, de una clave de propietario de plataforma a otra.

ATM Automatic Technology Manager, que permite que los administradores de red administren sistemas de forma remota a nivel del BIOS.

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 encendido Recurso de seguridad que requiere alguna forma de autenticación, como una Java Card, un chip de seguridad o una contraseña, al encender el equipo.

Autoridad de certificación Servicio que emite los certificados requeridos para administrar una infraestructura de clave pública.

Biométrica Categoría de autenticación de credenciales que utiliza un rasgo físico, como una huella digital, para identificar al usuario.

Botón de envío seguro Un botón de software que se muestra en la barra de herramientas de los mensajes de correo electrónico de Microsoft Outlook. Al hacer clic en el botón usted puede firmar y/o encriptar un mensaje de correo electrónico de Microsoft Outlook.

Botón Firme y Codifique Un botón de software que se muestra en la barra de herramientas de las aplicaciones Microsoft Office. Al hacer clic en el botón usted puede firmar, encriptar o quitar la encriptación de un documento de Microsoft Office.

Certificado digital Credenciales electrónicas que confirman la identidad de una persona o compañía al asociar la identidad del dueño del certificado digital con un par de claves electrónicas utilizadas para firmar información digital.

Certificado Privacy Manager Un certificado digital que requiere autenticación cada vez que lo usa para operaciones criptográficas, como firmar y encriptar mensajes de correo electrónico y documentos de Microsoft Office.

Ciclo de eliminación definitiva El número de veces que se ejecuta el algoritmo de eliminación definitiva en cada activo. Mientras mayor sea el número de ciclos de eliminación definitiva seleccionado, más seguro será el equipo.

Clase de dispositivos Todos los dispositivos de un tipo particular, como las unidades de discos.

Codificación Acción de codificar y descodificar datos para que sólo puedan decodificarlos determinadas personas.

Comunicación de mensajería instantánea confiable Una sesión de comunicación durante la cual un remitente confiable envía mensajes confiables a un contacto confiable.

Consola Una ubicación central desde la cual es posible acceder y administrar los recursos y configuraciones en la consola administrativa de HP ProtectTools.

Contacto confiable Una persona que aceptó una invitación de contacto confiable.

Contraseña de Anulación Una contraseña que se crea cuando un usuario solicita un certificado digital. La contraseña se requiere cuando el usuario desea revocar su certificado digital. Esto asegura que sólo el usuario pueda revocar el certificado.

Copia de seguridad El uso del recurso de copia de seguridad guarda una copia de la información importante de un programa en una ubicación externa al programa. Se puede usar para restaurar la información en una fecha posterior en el mismo equipo o en otro.

Credenciales Método que permite al usuario probar que está autorizado a realizar una tarea determinada en el proceso de autenticación.

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.

Descodificación Procedimiento utilizado en criptografía para convertir datos codificados en texto común.

Destinatario contacto confiable Una persona que recibe una invitación para convertirse en un contacto confiable.

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.

Drive Encryption Protege sus datos mediante la encriptación de la(s) unidad(es) de disco, haciendo ilegible la información para quienes carecen de la autorización apropiada.

DriveLock Recurso de seguridad que vincula la unidad de disco duro a un usuario y requiere que el usuario escriba la contraseña correcta de DriveLock al encender el equipo.

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

Eliminación definitiva automática Eliminación definitiva programada que el usuario configura en File Sanitizer.

Eliminación definitiva manual Eliminación definitiva inmediata de un activo o de activos seleccionados que omite la programación de eliminación definitiva automática.

Eliminación simple Eliminación de la referencia a un activo en Windows. El contenido del activo permanece en la unidad de disco duro hasta que el dato oscurecido es sobregrabado mediante la limpieza para liberar espacio.

Encriptación Procedimiento, como el uso de un algoritmo, empleado en criptografía para convertir texto común en texto cifrado para evitar que personas no autorizadas lean los datos. Existen muchos tipos de encriptación de datos y la encriptación es la base de la seguridad de la red. Algunos tipos comunes son el estándar de encriptación de datos y la encriptación de clave pública.

Escena Una foto de un usuario registrado que se utilizará para la autenticación.

Firma digital Datos enviados junto a un archivo que verifican quién envió el material y si no se modificó el archivo después de firmado.

Firmante sugerido Un usuario que ha sido designado por el propietario de un documento de Microsoft Word o Microsoft Excel para agregar una línea de firma al documento.

Grupo Un grupo de usuarios que tienen el mismo nivel de acceso o negación a una clase de dispositivos o a un dispositivo específico.

HP Connection Manager Una ubicación central desde la cual es posible acceder y administrar los recursos y configuraciones en Security Manager for HP ProtectTools.

HP SpareKey Copia de seguridad de la clave de encriptación de la unidad.

Huella digital Una extracción digital de la imagen de su huella digital. La imagen de su huella digital real nunca se almacena en Security Manager.

Identidad En HP ProtectTools Security Manager, es un grupo de credenciales y configuraciones manipulado como una cuenta o un perfil para un determinado usuario.

Inicio de sesión Un objeto dentro de Security Manager que consiste en un nombre de usuario y una contraseña (y posiblemente otra información seleccionada) que se puede usar para iniciar sesión en sitios Web y otros programas.

Invitación de contacto confiable Un mensaje de correo electrónico enviado a una persona, solicitándole que se transforme en un contacto seguro.

Java Card Una tarjeta extraíble que se inserta en el equipo. Contiene información de identificación para inicio de sesión. Para iniciar una sesión en la pantalla de inicio de sesión de Drive Encryption con una Java Card, es necesario que inserte la Java Card y que digite su nombre de usuario y el PIN de la Java Card.

Limpieza para liberar espacio La grabación segura de datos aleatorios sobre activos eliminados para distorsionar el contenido de los activos eliminados.

Línea de firma Un lugar para la exhibición visual de una firma digital. Cuando se firma un documento, se muestra el nombre del firmante y el método de verificación. También se puede incluir la fecha y el título del firmante.

Lista de contactos confiables Una lista de los contactos confiables.

Mensaje confiable Una sesión de comunicación durante la cual un remitente confiable envía mensajes confiables a un contacto confiable.

Método de inicio de sesión seguro El método usado para realizar el inicio de sesión en el equipo.

Migración Tarea que permite la administración, restauración y transferencia de certificados de Privacy Manager y de contactos confiables.

Modo de dispositivo SATA Modo de transferencia de datos entre un equipo y dispositivos de almacenamiento masivo, como unidades de disco duro o unidades ópticas.

Pantalla de inicio de sesión de Drive Encryption Una pantalla de inicio de sesión que aparece antes de que se inicie Windows. Los usuarios deben introducir su nombre de usuario y la contraseña de Windows o el PIN de la Java Card. En la mayoría de los casos, al ingresar correctamente la información en la pantalla de inicio de sesión de Drive Encryption se le permite acceder directamente a Windows sin tener que volver a entrar en la pantalla de inicio de sesión de Windows.

Perfil de eliminación definitiva Un método de borrado especificado y una lista de activos.

PIN Número de identificación personal.

PKI Estándar Infraestructura de claves públicas (PKI) que define las interfaces para la creación, uso y administración de certificados y claves criptográficas.

Política de control de acceso a los dispositivos La lista de los dispositivos a los cuales a un usuario se le permite o niega el acceso.

Proveedor de servicios criptográficos (CSP) Proveedor o biblioteca de algoritmos criptográficos que pueden utilizarse en una interfaz bien definida para realizar determinadas funciones criptográficas.

PSD Unidad segura personal (PSD), que proporciona un área de almacenamiento protegido para información confidencial.

Registro único Recurso que almacena información de autenticación y permite utilizar Security Manager para acceder a Internet y a las aplicaciones de Windows que requieren autenticación por contraseña.

Reinicio Proceso de reinicio del equipo.

Remitente confiable Un contacto confiable que envía mensajes de correo electrónico y documentos de Microsoft Office firmados y/o encriptados.

Restaurar Un proceso que copia información de un programa desde un archivo de copia de seguridad guardado anteriormente en este programa.

Revelar Una tarea que permite que el usuario desencripte una o más sesiones históricas de chat, mostrando los nombres de pantalla de contacto en texto común y haciendo que la sesión pueda visualizarse.

Secuencia de clave Una combinación de teclas específica que, cuando se la presiona, inicia una eliminación definitiva automática, por ejemplo ctrl+alt+s.

Seguridad en el inicio de sesión en Windows Protege su(s) cuenta(s) de Windows al exigir el uso de credenciales específicas para el acceso.

Selle para contactos confiables Una tarea que agrega una firma digital, encripta el mensaje de correo electrónico y lo envía después de autenticarse usando su método de inicio de sesión seguro elegido.

Servicio en segundo plano El servicio en segundo plano de bloqueo/auditoría de dispositivos de HP ProtectTools debe estar ejecutándose para que las políticas de control de acceso a los dispositivos puedan aplicarse. Puede verse desde el interior de la aplicación Servicios, debajo de la opción Herramientas administrativas en el Panel de control. Si no está ejecutándose, HP ProtectTools Security Manager intenta iniciarse cuando se aplican las políticas de control de acceso a los dispositivos.

Sesión de historial de chat Un archivo encriptado que contiene un registro de ambos lados de una conversación en una sesión de chat.

Sistema de archivos de encriptación (EFS) Sistema que encripta todos los archivos y las subcarpetas de una carpeta seleccionada.

Smart card Pequeño componente de hardware, similar en forma y tamaño a una tarjeta de crédito, que almacena información de identificación sobre el dueño. Utilizada para autenticar al propietario en un equipo.

Tarjeta de ID Un dispositivo en la barra lateral de Windows que sirve para identificar visualmente su escritorio con su nombre de usuario y una imagen elegida. Haga clic en la tarjeta de ID para abrir la consola administrativa de HP ProtectTools.

Token Ver método de inicio de sesión seguro.

Token USB Dispositivo de seguridad que almacena información de identificación sobre un usuario. Como un lector biométrico o una Java Card, es utilizado para autenticar al propietario en un equipo.

Token virtual Recurso de seguridad que funciona de manera muy similar a una smart card o un lector de tarjetas. El token se guarda en el disco duro del equipo o en el registro de Windows. Cuando se inicia la sesión con un token virtual, se le solicita un PIN de usuario para completar la autenticación.

TXT Trusted Execution Technology (Tecnología de ejecución confiable).

Usuario Cualquiera inscrito en Drive Encryption. Los usuarios que no son administradores tienen derechos limitados en Drive Encryption. Sólo pueden inscribirse (con aprobación del administrador) e iniciar sesión.

Usuario autorizado El usuario al que se le han concedido permisos en la Configuración de acceso de usuario para ver o modificar los valores de la configuración en la Configuración sencilla o la Configuración de clases de dispositivo.

Visualizador del historial de Live Messenger Un componente de Privacy Manager Chat que le permite buscar y ver sesiones históricas de chat encriptadas.

Índice

A

abrir
- Consola administrativa de HP ProtectTools 12
- Device Access Manager for HP ProtectTools 82
- Drive Encryption for HP ProtectTools 42
- File Sanitizer for HP ProtectTools 73
- HP ProtectTools Security Manager 26
- Privacy Manager for HP ProtectTools 49

acceso
- concesión de acceso a grupos o usuarios existentes 89
- control 81
- negación 86
- negación del acceso a grupos o usuarios existentes 90
- permitir 86
- prevención de no autorizado 4

acceso no autorizado, prevención 4

activación
- Drive Encryption 43
- limpieza para liberar espacio 79

Actualizaciones y mensajes 24, 40

adición
- firmantes sugeridos 59
- grupo 90
- línea de firma 58
- línea de firma del firmante sugerido 59
- usuario 90

administración
- contraseñas 22, 32, 33
- credenciales 37
- usuarios 17

administración central 69

Administrador de contraseñas 32, 33

aplicaciones, configuración 20

Asistente
- Configuración de HP ProtectTools 9

Asistente de configuración 9

autenticación 15

B

borrado simple 75

C

Certificado de Privacy Manager
- configuración de un predeterminado 51
- eliminación 52
- instalación 50
- recepción 50
- renovación 51
- restauración 52
- revocación 52
- solicitud 50
- visualización de detalles 51

certificado digital
- configuración de un predeterminado 51
- eliminación 52
- instalación 50
- recepción 50
- renovación 51
- restauración 52
- revocación 52
- solicitud 50
- visualización de detalles 51

ciclo de trituración 75

clase de dispositivos
- configuración 84
- permitirle el acceso a un usuario 87

claves de la copia de seguridad, creación 46

configuración
- acceso al dispositivo 82
- adición 27, 40
- aplicaciones 20, 27, 40
- clase de dispositivos 84
- configuraciones 89
- Consola administrativa de HP ProtectTools 14
- control de acceso 89
- ficha General 21
- icono 36
- Privacy Manager for Microsoft Outlook 56
- Privacy Manager para un documento de Microsoft Office 58
- Privacy Manager para Windows Live Messenger 63
- programación de limpieza para liberar espacio 74
- programación de una eliminación definitiva 73
- restablecimiento 88
- sencilla 83

configuración del dispositivo
- especificación 18
- huella digital 18
- rostro 18
- Smart Card 18

configuraciones
- adición 22
- aplicaciones 22

avanzadas 19
usuario avanzado 30
Configuraciones de la ficha Aplicaciones 22, 40
configuraciones del panel de control 27
Configuración sencilla 83
Consola administrativa de HP ProtectTools
abrir 12
configuración 14
uso 13
Contactos confiables
agregado 53
eliminación 55
verificación del estado de revocación 55
visualización de detalles 55
contraseña
administración 6
cambio 30
HP ProtectTools 6
pautas 8
políticas 5
segura 8
seguridad 36
Contraseña de inicio de sesión de Windows 6
control del acceso al dispositivo 81
copia de seguridad
Certificados de Privacy Manager 68
Contactos confiables 68
credenciales de HP ProtectTools 8
datos 39
creación
claves de la copia de seguridad 46
perfil de eliminación definitiva 74
credenciales 37, 38
credenciales, registro 28

CH

chat en la ventana de Comunicaciones 63

D

datos
copia de seguridad 39
restauración 39
restricción del acceso a 4
definición
de cuál activo se confirmará antes de borrarlo 76
de cuál activo se confirmará antes de su eliminación 75
desactivación de Drive Encryption 43
Descubrir más 40
desencriptación de unidades 41, 46
Device Access Manager for HP ProtectTools
abrir 82
solución de problemas 95
dispositivo, permitirle el acceso a un usuario 87
Drive Encryption for HP ProtectTools
abrir 42
activación 43
administración de Drive Encryption 46
copias de seguridad y recuperación 46
desactivación 43
desencriptación de unidades individuales 46
encriptación de unidades individuales 46
inicio de sesión después de la activación de Drive Encryption 43

E

eliminación
acceso de grupo 90
acceso de usuario 90
encriptación de un documento de Microsoft Office 60
eliminación definitiva manual
todos los elementos seleccionados 79
un activo 78
encriptación
Documento de Microsoft Office 60
unidades 41, 44, 46
Envío por correo electrónico de un documento de Microsoft Office encriptado 60
escena
registro 28
especificación de las configuraciones de seguridad 16
estado de la encriptación, mostrar 44
Estado de las aplicaciones de seguridad 40
Excel, agregar una línea de firma 58
exclusión de activos del borrado automático 76

F

Ficha General, configuración 21
File Sanitizer for HP ProtectTools
icono 78
procedimientos de configuración 73
File Sanitizer para HP ProtectTools
abrir 73
firma
Documento de Microsoft Office 58
mensaje de correo electrónico 57
firmante sugerido
adición 59
agregar una línea de firma 59
funciones de seguridad 6

G

grupo
eliminación 87
negar acceso 86
permitir acceso 86

H

herramientas, agregar 23
herramientas de administración, agregar 23
historial del chat, visualización 64
HP ProtectTools, recursos 2

HP ProtectTools Security Manager
abrir 26
Contraseña de copia de seguridad y recuperación 6
procedimientos de configuración 28
solución de problemas 93
huellas digitales
configuración 18
registro 28

I
inicio de sesión en el equipo 43
inicio de una sesión de chat en Privacy Manager 62
inicios de sesión
adición 33
administración 35
categorías 35
edición 34
Inicios de sesión
menú 35
interrupción de una operación de eliminación o limpieza 79

J
Java Card Security for HP ProtectTools, PIN 6

L
limpieza para liberar espacio 74
LoJack Pro 92

M
mensaje de correo electrónico
firma 57
Sellado para contactos confiables 57
ver un mensaje sellado 57
Microsoft Excel, agregar una línea de firma 58
Microsoft Office
eliminación de la encriptación 60
encriptación de un documento 60
envío por correo electrónico de un documento encriptado 60
firma de un documento 58
ver un documento encriptado 61
ver un documento firmado 61
Microsoft Word, agregar una línea de firma 58

N
negar acceso 86

O
objetivos, seguridad 4
objetivos clave de seguridad 4

P
perfil de eliminación definitiva predefinido 74
permitir acceso 86
personalización
perfil de borrado simple 75
perfil de eliminación definitiva 75
preasignado, certificado 50
preferencias, configuración 38
Privacy Manager
uso con Microsoft Outlook 56
uso con un documento de Microsoft Office 2007 57
uso en Windows Live Messenger 61
Privacy Manager for HP ProtectTools
abrir 49
administración de certificados de Privacy Manager 49
administración de contactos confiables 53
Certificado de Privacy Manager 49
métodos de autenticación 48
métodos de inicio de sesión seguro 48
migración de certificados de Privacy Manager y de contactos confiables a otro equipo 68
procedimientos de configuración 49
requisitos del sistema 48
protección de activos de la trituración automática 75

R
recuperación, realización 47
recursos de HP ProtectTools 2
registro
escenas 28
huellas digitales 28
registro de credenciales 28
requisitos del sistema 48
restablecimiento 88
restauración
Certificados de Privacy Manager y contactos confiables 68
credenciales de HP ProtectTools 8
datos 39
restricción
acceso al dispositivo 81
acceso a los datos sensibles 4
robo, protección contra 4
rostro
configuraciones 18
registro de escenas 28

S
secuencia de teclas 77
seguridad
funciones 6
objetivos clave 4
resumen 40
selección
activos que se eliminarán definitivamente 74
perfil de eliminación definitiva 74
sellado 57
servicio en segundo plano 83
Smart Card
configuración 18
solicitud de un certificado digital 50
solución de problemas
Device Access Manager 95
Security Manager 93
varios 97

T
Tarjeta de identificación 38

U

uso
  Consola administrativa de HP ProtectTools 13
usuario
  eliminación 87
  negar acceso 86
  permitir acceso 86

V

visualización
  archivos de registro 79
  documento de Microsoft Office encriptado 61
  documento de Microsoft Office firmado 61
  historial de chat 64
  mensaje de correo electrónico sellado 57

W

Windows Live Messenger, chat 63
Word, agregar una línea de firma 58