HP ProtectTools

Pasos iniciales

Primera edición: enero de 2011

Número de referencia del documento: 638391-E51

Tabla de contenido

1 Introducción a la seguridad

El software HP ProtectTools Security Manager proporciona recursos de seguridad que sirven de protección contra el acceso no autorizado al equipo, a la red y a los datos más importantes.

Aplicación	Recursos
Consola administrativa de HP ProtectTools (para administradores)	• Requiere derechos de administrador de Microsoft Windows para permitir el acceso. • Proporciona acceso a módulos que son configurados por un administrador y no están disponibles para los usuarios. • Permite la configuración inicial de seguridad y configura opciones o requisitos para todos los usuarios.
HP ProtectTools Security Manager (para usuarios)	• Permite que los usuarios configuren las opciones proporcionadas por un administrador. • Permite que los administradores les proporcionen a los usuarios el control limitado 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 de HP ProtectTools (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 los usuarios. • 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)	• Organizar, configurar y cambiar contraseñas. • Configurar y cambiar credenciales de usuario, como una contraseña de Windows, una huella digital y una smart card. • Configurar y cambiar la trituración, purificación y otras configuraciones de File Sanitizer. • Ver las configuraciones de Device Access Manager. • Configurar Computrace for HP ProtectTools. • Configurar preferencias y opciones de Copias de seguridad y restauración.
Credential Manager for HP ProtectTools (Password Manager)	• Guardar, organizar y proteger sus nombres de usuario 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 Password Manager. La próxima vez que visite el sitio, Password Manager rellenará y enviará la información automáticamente. • Crear contraseñas más seguras para brindar una mayor seguridad de cuenta. Password Manager completa y envía la información automáticamente.
Drive Encryption for HP ProtectTools (sólo en algunos modelos)	• Brinda encriptación de volumen completo para la unidad de disco duro. • Fuerza a que se realice la autenticación de preinicio a fin de desencriptar y acceder a los datos.
File Sanitizer for HP ProtectTools	• Tritura activos digitales (información confidencial, que incluye archivos de aplicaciones, contenido de historial, contenido relacionado con la Web u otros datos confidenciales) en su equipo y purifica los activos eliminados de su unidad de disco duro periódicamente.

Módulo	Recursos clave
Device Access Manager for HP ProtectTools (sólo en algunos modelos)	• Permite que los administradores de TI controlen el acceso a los dispositivos según los perfiles de usuario. • Evita que usuarios no autorizados eliminen datos utilizando medios de almacenamiento externos y que introduzcan virus en el sistema desde medios externos. • Permite que los administradores desactiven el acceso a dispositivos grabables para usuarios o grupos de usuarios específicos.
Privacy Manager for HP ProtectTools (sólo en algunos modelos)	• Se utiliza para obtener certificados de autoridad, que verifican la fuente, integridad y seguridad de la comunicación cuando se utilizan documentos de Microsoft Office o el correo electrónico de Microsoft.
Computrace for HP ProtectTools (se adquiere por separado)	• Brinda rastreo seguro de activos. • Supervisa la actividad del usuario, así como también los cambios de hardware y software. • Permanece activo incluso en caso de que se vuelva a formatear o se sustituya la unidad de disco duro. • Requiere la adquisición por separado de suscripciones de rastreo y localización para su activación.
Embedded Security for HP ProtectTools (sólo en algunos modelos)	• Utiliza un chip de seguridad incorporado de Módulo de plataforma segura (TPM) para brindar protección contra el acceso no autorizado a los datos y credenciales del usuario guardados en un equipo. • Permite la creación de una unidad segura personal (PSD), que resulta útil para proteger la información de los archivos y carpetas del usuario. • Admite aplicaciones de terceros (como Microsoft Outlook e Internet Explorer) para operaciones protegidas de certificados digitales.

Descripción del producto de seguridad HP ProtectTools y ejemplos de uso comunes

La mayoría de los productos de seguridad de HP ProtectTools cuentan con autenticación de usuario (normalmente una contraseña) y una copia de seguridad administrativa para lograr acceder en caso de que las contraseñas se pierdan, no estén disponibles o se olviden o en cualquier momento en que la seguridad corporativa requiera el acceso.

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

Credential Manager for HP ProtectTools

Credential Manager (parte de Security Manager) guarda nombres de usuarios y contraseñas y puede utilizarse para hacer lo siguiente:

- Guardar nombres y contraseñas de inicio de sesión para el acceso a Internet o correo electrónico.
- Iniciar la sesión de un usuario automáticamente en un sitio web o correo electrónico.
- Administrar y organizar autenticaciones.
- Seleccionar un activo de Web o de red y acceder directamente al enlace.
- Visualizar nombres y contraseñas cuando es necesario.

Ejemplo 1: Una agente de compra de un importante fabricante realiza la mayoría de sus transacciones corporativas por medio de Internet. También visita con frecuencia varios sitios web populares que requieren información de inicio de sesión. Como se preocupa profundamente por la seguridad, no utiliza la misma contraseña en cada cuenta. La agente de compra ha decidido utilizar Credential Manager para asociar enlaces web a diferentes nombres de usuario y contraseñas. Cuando va a un sitio web para iniciar sesión, Credential Manager le presenta las credenciales automáticamente. Si desea visualizar los nombres de usuario y contraseñas, Credential Manager puede configurarse para revelarlas.

También es posible utilizar Credential Manager para administrar y organizar las autenticaciones. Esta herramienta permitirá que un usuario seleccione un activo de Web o de red y acceda directamente al enlace. El usuario también puede visualizar nombres y contraseñas cuando es necesario.

Ejemplo 2: Un contador que trabaja mucho ha sido ascendido y ahora administrará todo el departamento contable. El personal debe iniciar sesión en una gran cantidad de cuentas web de clientes, y cada una de estas utiliza distinta información de inicio de sesión. Es necesario compartir esta información de inicio de sesión con otros colegas, por lo que la confidencialidad es un problema. El contador decide organizar todos los enlaces web, nombres de usuarios de compañías y contraseñas en Credential Manager for HP ProtectTools. Una vez finalizada esa tarea, el contador despliega Credential Manager para que los empleados puedan trabajar en las cuentas web y nunca sepan las credenciales de inicio de sesión que están utilizando.

Drive Encryption for HP ProtectTools

Se utiliza Drive Encryption para restringir el acceso a los datos en toda la unidad de disco duro del equipo o en una unidad secundaria. Drive Encryption también puede administrar unidades de autoencriptación.

Ejemplo 1: Un médico desea asegurarse de que sólo él pueda acceder a los datos de la unidad de disco duro de su equipo. Este médico activa Drive Encryption, que requiere autenticación de preinicio antes del inicio de sesión de Windows. Una vez configurada la unidad de disco duro, no puede accederse a esta sin una contraseña antes de que se inicie el sistema operativo. El médico puede aumentar aún más la seguridad de la unidad si opta por encriptar los datos con la opción SED (unidad de autoencriptación).

Tanto Embedded Security for HP ProtectTools como Drive Encryption for HP ProtectTools no permiten el acceso a los datos encriptados incluso cuando se retira la unidad, ya que ambos se encuentran vinculados a la placa base original.

Ejemplo 2: Un administrador hospitalario desea asegurarse de que sólo los doctores y el personal autorizado puedan acceder a los datos de su equipo local, sin compartir sus contraseñas personales. El departamento de TI agrega al administrador, a los médicos y a todo el personal autorizado como usuarios de Drive Encryption. Ahora sólo el personal autorizado puede iniciar el equipo o dominio con su nombre de usuario y contraseña personales.

File Sanitizer for HP ProtectTools

Se utiliza File Sanitizer for HP ProtectTools para eliminar permanentemente datos, incluida la actividad del navegador de Internet, los archivos temporales, los datos eliminados previamente o cualquier otra información. Puede configurarse File Sanitizer para que funcione manual o automáticamente según una programación definida por el usuario.

Ejemplo 1: Un abogado a menudo se ocupa de la información confidencial de sus clientes y desea asegurarse de que los datos de los archivos eliminados no puedan recuperarse. Este abogado utiliza File Sanitizer para “triturar” los archivos eliminados a fin de que sea casi imposible recuperarlos.

Normalmente cuando Windows elimina datos, no borra efectivamente los datos de la unidad de disco duro. En cambio, marca los sectores de la unidad de disco duro disponibles para el uso futuro. Hasta que los datos se sobrescriban, será posible recuperarlos fácilmente utilizando herramientas comunes disponibles en Internet. File Sanitizer sobrescribe los sectores con datos aleatorios (múltiples veces cuando sea necesario), lo que hace que los datos eliminados sean ilegibles e irrecuperables.

Ejemplo 2: Una investigadora desea triturar los datos eliminados, los archivos temporales, la actividad del navegador, etc. automáticamente cuando cierra su sesión. Utiliza File Sanitizer para programar la “trituración” de modo que pueda seleccionar los archivos comunes o los archivos personalizados que se eliminarán permanentemente de forma automática.

Device Access Manager for HP ProtectTools

Es posible utilizar Device Access Manager for HP ProtectTools para bloquear el acceso no autorizado a unidades flash USB donde puedan copiarse los datos. También puede restringirse el acceso a unidades de CD/DVD, al control de dispositivos USB, a conexiones de red, etc. Un administrador también puede programar cuándo o por cuánto tiempo puede accederse a las unidades. Un ejemplo sería una situación en la que proveedores externos necesitan acceder a los equipos de la compañía, pero no deben poder copiar los datos a una unidad USB. Device Access Manager for HP ProtectTools permite que un administrador restrinja y controle el acceso al hardware.

Ejemplo 1: Un gerente de una compañía de suministros médicos a menudo trabaja con registros médicos personales y con información de su compañía. Los empleados necesitan acceder a estos datos; sin embargo, es sumamente importante que no se extraigan los datos del equipo por medio de una unidad USB o de cualquier otro medio de almacenamiento externo. La red es segura, pero los equipos tienen grabadoras de CD y puertos USB que podrían permitir copiar o sustraer los datos. El gerente utiliza Device Access Manager para desactivar los puertos USB y grabadoras de CD a fin de

que no puedan utilizarse. Aunque los puertos USB se bloquean, el mouse y los teclados siguen funcionando.

Ejemplo 2: Una compañía de seguros no desea que sus empleados instalen o carguen software personal o datos provenientes de su hogar. Algunos empleados necesitan acceder al puerto USB en todos los equipos. El gerente de TI utiliza Device Access Manager para permitirles el acceso a algunos empleados, mientras se les bloquea el acceso externo a otros.

Privacy Manager for HP ProtectTools

Se utiliza Privacy Manager for HP ProtectTools cuando es necesario proporcionar seguridad a las comunicaciones de correo electrónico por Internet. El usuario puede crear y enviar correos electrónicos que sólo un destinatario autenticado puede abrir. Con Privacy Manager, la información no puede verse comprometida ni ser interceptada por un impostor.

Ejemplo 1: Un corredor de bolsa desea asegurarse de que sus correos electrónicos sólo vayan a clientes específicos y de que nadie pueda falsear la cuenta de correo electrónico e interceptarla. El corredor de bolsa se registra a sí mismo y a sus clientes con Privacy Manager. Privacy Manager le emite un Certificado de autenticación (CA) a cada usuario. Con esta herramienta, el corredor de bolsa y sus clientes deben autenticarse antes de intercambiar correos electrónicos.

Privacy Manager for HP ProtectTools facilita el envío y la recepción de correos electrónicos cuando se ha verificado y autenticado el destinatario. También puede encriptarse el servicio de correo. El proceso de encriptación es similar al utilizado durante las compras típicas con tarjeta de crédito en Internet.

Ejemplo 2: Un CEO desea asegurarse de que sólo los miembros del directorio puedan visualizar la información que envía por correo electrónico. El CEO utiliza la opción de encriptar el correo electrónico enviado y recibido de los directores. Un Certificado de autenticación de Privacy Manager permite que el CEO y los directores tengan una copia de la clave de encriptación para que sólo ellos puedan desencriptar el correo electrónico confidencial.

Computrace for HP ProtectTools (anteriormente LoJack Pro)

Computrace for HP ProtectTools (se adquiere por separado) es un servicio capaz rastrear la ubicación de un equipo sustraído cada vez que el usuario accede a Internet.

Ejemplo 1: El director de una escuela instruyó al departamento de TI para que este hiciera un seguimiento de todos los equipos de la escuela. Una vez realizado el inventario de los equipos, el administrador de TI registró todos los equipos con Computrace para que pudieran rastrearse en caso de que alguna vez se sustrajeran. Recientemente la escuela se dio cuenta de que faltaban varios equipos, por lo que el administrador de TI alertó a las autoridades y a los oficiales de Computrace. Las autoridades localizaron y devolvieron los equipos a la escuela.

Computrace for HP ProtectTools igualmente puede ayudar a administrar y localizar equipos de forma remota, así como también puede ayudar a monitorizar el uso y las aplicaciones del equipo.

Ejemplo 2: Una compañía inmobiliaria necesita controlar y actualizar equipos en todo el mundo. Utiliza Computrace para monitorizar y actualizar los equipos sin tener que enviar a un profesional de TI a cada equipo.

Embedded Security for HP ProtectTools (sólo en algunos modelos)

Embedded Security for HP ProtectTools brinda la capacidad de crear una unidad segura personal. Esta capacidad permite que el usuario cree una partición virtual de la unidad en el equipo, la cual permanece completamente oculta hasta que se accede a dicha partición. Es posible utilizar

Embedded Security en cualquier lugar donde sea necesario proteger la confidencialidad de determinados datos, al paso que el resto de los datos no esté encriptado.

Ejemplo 1: Un gerente de depósito tiene un equipo al que múltiples trabajadores acceden de forma intermitente durante todo el día. El gerente desea encriptar y ocultar los datos confidenciales del depósito en el equipo. Desea que los datos estén seguros para que incluso en caso de que alguien sustraiga la unidad de disco duro no pueda desencriptar ni leer los datos. El gerente de depósito decide activar Embedded Security y mover los datos confidenciales a la unidad segura personal. El gerente de depósito puede introducir una contraseña y acceder a los datos confidenciales como si estuvieran en cualquier otra unidad de disco duro. Cuando cierra la sesión o reinicia la unidad segura personal, esta no puede verse ni abrirse sin la contraseña adecuada. Los trabajadores nunca ven los datos confidenciales cuando acceden al equipo.

Embedded Security protege las claves de encriptación en un chip TPM (Módulo de plataforma segura) de hardware ubicado en la placa base. Es la única herramienta de encriptación que cumple los requisitos mínimos para resistir a los ataques a contraseña, cuando alguien intenta adivinar la contraseña de desencriptación. Embedded Security también puede encriptar toda la unidad y el correo electrónico.

Ejemplo 2: Un corredor de bolsa desea transportar datos sumamente confidenciales a otro equipo utilizando una unidad portátil. Desea asegurarse de que sólo estos dos equipos puedan abrir la unidad, incluso en caso de que la contraseña esté comprometida. El corredor de bolsa utiliza la migración de TPM de Embedded Security para permitir que un segundo equipo tenga las claves de encriptación necesarias para desencriptar los datos. Durante el proceso de transporte, incluso con la contraseña sólo los dos equipos físicos pueden desencriptar los datos.

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 confidenciales
- Prevención de acceso no autorizado desde ubicaciones internas o externas
- Creación de políticas de contraseñas seguras

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:

- Si el recurso de autenticación de preinicio está activado, ayuda a evitar el acceso al sistema operativo. Consulte los siguientes capítulos:
  - Security Manager for HP ProtectTools
  - Embedded Security for HP ProtectTools
  - Drive Encryption for HP ProtectTools
- El recurso de Unidad segura personal, provisto por el módulo Embedded Security for HP ProtectTools, encripta los datos confidenciales para ayudar a garantizar que no pueda accederse a estos sin autenticación. Consulte el siguiente capítulo:
  - Embedded Security for HP ProtectTools
- Computrace puede rastrear la ubicación de un equipo después de un robo. Consulte el siguiente capítulo:
  - Computrace for HP ProtectTools

Restricción del acceso a los datos confidenciales

Suponga que un auditor contratado está trabajando in situ y se le ha otorgado acceso al equipo para examinar datos financieros confidenciales; usted no desea que el auditor pueda imprimir los archivos ni guardarlos en un dispositivo grabable, como un CD. El siguiente recurso ayuda a restringir el acceso a los datos:

- Device Access Manager for HP ProtectTools permite que los administradores de TI restrinjan el acceso a los dispositivos grabables para que la información confidencial no pueda imprimirse ni copiarse desde la unidad de disco duro a los medios extraíbles.

Prevención de acceso no autorizado desde ubicaciones internas o externas

El acceso no autorizado a un equipo corporativo que no es seguro representa un riesgo real para los recursos de la red corporativa, como la información de servicios financieros, un ejecutivo o el equipo

de I&D, y también para la información privada, como los registros de pacientes o los registros financieros 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. Consulte los siguientes capítulos:
  - Password Manager for HP ProtectTools
  - Embedded Security for HP ProtectTools
  - Drive Encryption for HP ProtectTools
- Password Manager 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 permite que los gerentes de TI restrinjan el acceso a los dispositivos grabables para que la información confidencial no pueda copiarse desde la unidad de disco duro.
- File Sanitizer permite la eliminación segura de los datos al triturar archivos y carpetas críticas o purificar activos eliminados en la unidad de disco duro (sobrescribiendo datos que se han eliminado pero aún pueden recuperarse).
- Privacy Manager le permite obtener Certificados de autoridad cuando utiliza el correo electrónico de Microsoft o documentos de Microsoft Office, haciendo que el proceso de enviar y guardar información importante sea seguro.

Creación de políticas de contraseñas sólidas

Si entra en vigencia una directiva empresarial que exija el uso de una política de contraseñas seguras para docenas de aplicaciones basadas en la Web y bases de datos, Security Manager proporciona un repositorio protegido para las contraseñas y la comodidad de un inicio de sesión único.

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 compañía o red y determina los recursos de seguridad que se desplegarán, como Drive Encryption o Embedded Security.

  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 de TI: aplica y administra los recursos de seguridad definidos por el oficial de seguridad. También puede activar o desactivar algunos recursos. Por ejemplo, si el oficial de seguridad ha decidido implementar smart cards, el administrador de TI puede activar tanto el modo de contraseña como el modo de smart card.

- Usuario: utiliza los recursos de seguridad. Por ejemplo, si el oficial de seguridad y el administrador de TI han activado smart cards para el sistema, el usuario puede configurar el PIN de la smart card y utilizar la tarjeta para realizar la 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 Copias de seguridad y restauración de Security Manager	Security Manager, por usuario individual	Protege el acceso al archivo de copia de seguridad y recuperación de Security Manager.

Contraseña de HP ProtectTools	Definir el módulo siguiente	Función
PIN de smart card		Puede utilizarse como autenticación multifactor. Puede utilizarse como autenticación de Windows. Autentica a los usuarios de Drive Encryption si se selecciona el token de smart card.
Contraseña de token de recuperación de emergencia	Embedded Security, por administrador de TI	Protege el acceso al token de recuperación de emergencia, que es un archivo de copia de seguridad para el chip de seguridad incorporado.
Contraseña del propietario	Embedded Security, por administrador de TI	Protege el sistema y el chip TPM del acceso no autorizado a todas las funciones de propietario de Embedded Security.
Contraseña de administrador del BIOS	Utilidad de configuración del equipo, por administrador de TI	Protege el acceso a la utilidad de configuración del equipo.

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 para la contraseña ni ninguna otra información personal, como su fecha de nacimiento, nombres de mascotas o el apellido de soltera de su madre, incluso si lo deletrea en sentido inverso.
- 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 del Asistente de configuración

El Asistente de configuración de Security Manager lo guía a través de la activación de los recursos de seguridad disponibles que se aplican a todos los usuarios de este equipo. También puede administrar estos recursos en la página Recursos de seguridad de la Consola administrativa.

Para configurar los recursos de seguridad por medio del Asistente de configuración de Security Manager:

1. Abra HP ProtectTools Security Manager mediante el icono de gadget de escritorio de HP ProtectTools, en la barra lateral de Windows, o el icono de la barra de tareas del área de notificación, en el extremo derecho de la barra de tareas.

El color del banner del icono de gadget de escritorio de HP ProtectTools 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.

Aparecerá un mensaje en la parte inferior del icono de gadget para indicar una de las siguientes condiciones:

- **Configurar ahora**: el administrador debe hacer clic en el icono de gadget para ejecutar el Asistente de configuración de Security Manager con el propósito de configurar las credenciales de autenticación para el equipo.

  El Asistente de configuración es una aplicación independiente.

- **Registrar ahora**: un usuario debe hacer clic en el icono de gadget a fin de ejecutar el Asistente de pasos iniciales de Security Manager para registrar las credenciales de autenticación.

  El Asistente de pasos iniciales aparece en el panel de control de Security Manager.

- **Verificar ahora**: haga clic en el icono de para mostrar detalles adicionales en la página Estado de las Aplicaciones de seguridad.

NOTA: El icono de gadget de escritorio de HP ProtectTools no se encuentra disponible en Windows XP.

– o –

Haga clic en **Inicio**, en **Todos los programas**, en **HP** y después en **Consola administrativa de HP ProtectTools**. En el panel izquierdo, haga clic en **Asistente de configuración**.

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

3. Compruebe su identidad escribiendo su contraseña de Windows y luego haga clic en **Siguiente**.

   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. En la página de SpareKey, seleccione tres preguntas de seguridad, ingrese una respuesta para cada pregunta y luego haga clic en **Siguiente**.

   Puede seleccionar preguntas diferentes o cambiar sus respuestas en la página de SpareKey de **Credential Manager**, en el panel de control de Security Manager.

NOTA: Esta configuración de SpareKey se aplica sólo al usuario administrativo.

5. Active los recursos de seguridad seleccionando sus casillas de verificación y luego haga clic en **Siguiente**.

   Mientras más recursos seleccione, más seguro estará su equipo.

NOTA: Esta configuración se aplica a todos los usuarios. Si no se selecciona ninguna casilla de verificación, el Asistente de configuración no les pedirá a los usuarios que registren esas credenciales.

- **Seguridad de inicio de sesión en Windows**: protege sus cuentas de Windows al requerir el uso de credenciales específicas para el acceso.
- **Drive Encryption**: protege sus datos al encriptar sus unidades de disco duro, haciendo que quienes no tengan la debida autorización no puedan leer la información.
- **Seguridad de preinicio**: protege su equipo al prohibir el acceso de personas no autorizadas antes del inicio de Windows.

NOTA: La seguridad de preinicio no está disponible si el BIOS no la admite.

6. El Asistente de configuración le solicitará que se inscriba o “registre” las credenciales.

   Si no dispone de un lector de huellas digitales, una Smart Card o una cámara web, se le pide que introduzca su contraseña de Windows. Después de registrarse, puede entonces utilizar cualquier credencial registrada para verificar su identidad cada vez que se requiere la autenticación.

NOTA: El registro de estas credenciales se aplica sólo al usuario administrativo.

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

   Aparecerá la página de inicio del panel de control de Security Manager.

3 Consola administrativa de HP ProtectTools Security Manager

El software HP ProtectTools Security Manager proporciona recursos de seguridad que sirven de protección contra el acceso no autorizado al equipo, a la red y a los datos más importantes. Se administra HP ProtectTools Security Manager por medio del recurso Consola administrativa.

Se dispone de aplicaciones adicionales (sólo en algunos modelos) en el panel de control de Security Manager para ayudar en la recuperación del equipo en caso de que este se extravíe o de que se lo roben.

Utilizando la consola, el administrador local puede efectuar las siguientes tareas:

- Activación o desactivación de recursos de seguridad
- Especificación de las credenciales de autenticación requeridas
- Administración de los usuarios del equipo
- Ajuste de los parámetros específicos del dispositivo
- Configuración de las aplicaciones de Security Manager instaladas
- Adición de aplicaciones de Security Manager adicionales

Apertura de la Consola administrativa de HP ProtectTools

Para las tareas administrativas, por ejemplo establecer políticas del sistema o configurar software, abra la consola de la siguiente manera:

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

  – o –

  En el panel izquierdo de Security Manager, haga clic en **Administración** y luego en **Consola administrativa**.

Utilización de la Consola administrativa

La Consola administrativa de HP ProtectTools es la ubicación central para administrar los recursos y las aplicaciones de HP ProtectTools Security Manager.

▲ Para abrir la Consola administrativa de HP ProtectTools, haga clic en **Inicio**, luego en **Todos los programas**, **HP** y luego en **Consola administrativa de HP ProtectTools**.

– o –

En el panel izquierdo de Security Manager, haga clic en **Administración** y luego en **Consola administrativa**.

La consola consta de los siguientes componentes:

- **Inicio**: le permite configurar las siguientes opciones de seguridad:
  - **Aumente la seguridad del sistema**
  - **Se requiere autenticación robusta**
  - **Administrar usuarios de HP ProtectTools**
  - **Vea cómo puede administrar de forma centralizada HP ProtectTools**
- **Sistema**: le permite configurar los siguientes recursos de seguridad y la autenticación para usuarios y dispositivos:
  - **Seguridad**
  - **Usuarios**
  - **Credenciales**
- **Aplicaciones**: le permite configurar parámetros para HP ProtectTools Security Manager y para las aplicaciones de Security Manager.
- **Datos**: proporciona un menú que se expande de enlaces a aplicaciones de Security Manager que protegen sus datos.
- **Administración central**: muestra fichas para acceder a soluciones, actualizaciones de productos y mensajes adicionales.
- **Asistente de configuración**: lo guía a través de la configuración de HP ProtectTools Security Manager.
- **Acerca de**: muestra información sobre HP ProtectTools Security Manager, por ejemplo el número de versión y el aviso de copyright.
- **Área principal**: muestra pantallas específicas de la aplicación.

  ?: muestra la ayuda de software de la Consola administrativa. Este icono se encuentra en la parte superior derecha del marco de la ventana, al lado de los iconos para minimizar y maximizar.

Configuración de su sistema

Se accede al grupo **Sistema** desde el panel de menú que está a la izquierda 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 **Sistema**:

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

Configuración de autenticación para su equipo

En la aplicación Autenticación, puede establecer las políticas que rigen el acceso al equipo. Puede especificar las credenciales necesarias para autenticar cada clase de usuario durante el inicio de sesión en Windows o en sitios web y programas a lo largo de una sesión de usuario.

Para configurar la autenticación en su equipo:

1. En el panel izquierdo de la Consola administrativa, haga clic en **Seguridad** y luego 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 luego haga clic en **Aplicar**.
3. Para configurar la autenticación de la sesión, haga clic en la ficha **Política de sesión**, efectúe los cambios y luego haga clic en **Aplicar**.

Política de inicio de sesión

A fin de definir las políticas que rigen las credenciales necesarias para autenticar a un usuario durante el inicio de sesión en Windows:

1. En el panel izquierdo de la Consola administrativa, haga clic en **Seguridad** y luego en **Autenticación**.
2. En la ficha **Política de inicio de sesión**, haga clic en la flecha hacia abajo y luego seleccione una categoría de usuario:
   - **Para administradores de este equipo**
   - **Para los usuarios que no sean administradores**
3. Especifique las credenciales de autenticación necesarias para la categoría seleccionada de usuario.
4. Elija si ALGUNA de las credenciales especificadas es necesaria o si TODAS las credenciales especificadas son necesarias a fin de autenticar a un usuario.
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 panel izquierdo de la Consola administrativa, haga clic en **Seguridad** y luego en **Autenticación**.
2. En la ficha **Política de sesión**, haga clic en la flecha hacia abajo y luego seleccione una categoría de usuario:
   - **Para administradores de este equipo**
   - **Para los usuarios que no sean administradores**
3. Haga clic en la flecha hacia abajo y luego seleccione las credenciales de autenticación requeridas para la categoría de usuario seleccionada:
   - **Requerir una de las credenciales especificadas**

     NOTA: Desmarcar las casillas de verificación de todas las credenciales tiene el mismo efecto que seleccionar **No requerir autenticación**.
   - **Requerir todas las credenciales especificadas**
   - **No requerir autenticación**: la selección de esta opción borra todas las credenciales de la ventana.
4. Haga clic en **Aplicar**.

Configuración

1. Seleccione la casilla de verificación para activar la siguiente configuración o desmárquela para desactivarla:

   Permitir inicio de sesión en One Step: 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.
2. Haga clic en **Aplicar**.

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 por medio de Security Manager. Además, se verifica si registraron o no las credenciales adecuadas que les permiten cumplir con dichas políticas.

Para administrar usuarios, seleccione las siguientes configuraciones:

- Para agregar usuarios adicionales, haga clic en **Agregar**.
- Para eliminar un usuario, haga clic en el usuario y luego en **Eliminar**.

- Para configurar credenciales adicionales para el usuario, haga clic en el usuario y luego en **Registrar**.
- A fin de ver las políticas para un usuario específico, seleccione el usuario y luego vea las políticas en la ventana inferior.

Credenciales

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

SpareKey

Puede configurar si permite o no la autenticación de SpareKey para inicio de sesión en Windows y administrar las preguntas de seguridad que se presentarán a los usuarios durante su registro de SpareKey.

1. Seleccione la casilla de verificación para activar o desmárquela para desactivar el uso de la autenticación de SpareKey para el inicio de sesión de Windows.
2. Seleccione las preguntas de seguridad que se presentarán a los usuarios durante su registro de SpareKey. Puede especificar hasta tres preguntas personalizadas o puede permitir que los usuarios ingresen su propia contraseña.
3. Haga clic en **Aplicar**.

Huellas digitales

Si el equipo tiene un lector de huellas digitales instalado o conectado, la página Huellas digitales muestra las siguientes fichas:

- **Registro**: elija 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, incluidos los administradores. Si la política de inicio de sesión requiere solamente las huellas digitales, se puede evitar que todos los usuarios puedan iniciar sesión en el equipo.

- **Sensibilidad**: mueva el control deslizante para ajustar la sensibilidad utilizada por el lector de huellas digitales cuando escanea sus huellas digitales.

  Si su huella digital no se reconoce uniformemente, puede ser necesario que seleccione una configuración de menor sensibilidad. Un parámetro de configuración mayor aumenta la sensibilidad a las variaciones de las huellas digitales pasadas por el lector y, por lo tanto, disminuye la posibilidad de una aceptación falsa. La configuración **Media-Alta** brinda una buena combinación de seguridad y comodidad.

- **Opciones avanzadas**: seleccione una de las siguientes opciones para configurar el lector de huellas digitales a fin de ahorrar energía y mejorar la respuesta visual:

  - **Optimizado**: el lector de huellas digitales se activa cuando es necesario. Puede observar una leve demora cuando el lector se utiliza por primera vez.
  - **Ahorrar energía**: el lector de huellas digitales demora un poco más en responder, pero la configuración requiere menos energía.
  - **Energía total**: el lector de huellas digitales está siempre preparado para ser utilizado, pero esta configuración usa más energía.

Smart card

Si el equipo tiene una smart card instalada o conectada, la página de Smart Card tiene dos fichas:

- **Configuración**: configure el equipo para que este se bloquee automáticamente cuando se extrae una Smart Card.

  NOTA: El equipo se bloquea sólo si se utilizó la Smart Card como credencial de autenticación al iniciar la sesión en Windows. La extracción de una Smart Card que no se utilizó para iniciar la sesión en Windows no bloquea el equipo.

- **Administración**: seleccione a partir de las siguientes opciones:

  - **Inicializar la smart card**: prepara una smart card para utilizar con HP ProtectTools. Si una smart card se inicializó previamente fuera de HP ProtectTools (contiene un par de claves asimétricas y certificado asociado), no es necesario inicializarla de nuevo, a menos que se desee realizar la inicialización con un certificado específico.
  - **Cambiar PIN de smart card**: le permite cambiar el PIN utilizado con la smart card.

- **Borrar datos de HP ProtectTools únicamente**: borra sólo el certificado de HP ProtectTools creado durante la inicialización de la tarjeta. Ningún otro dato se borra de la tarjeta.
- **Borrar todos los datos de la smart card**: borra todos los datos de la smart card especificada. La tarjeta ya no puede utilizarse con HP ProtectTools ni con cualquier otra aplicación.

NOTA: No se dispone de recursos que no sean compatibles con su smart card.

▲ Haga clic en **Aplicar**.

Rostro

Si el equipo tiene una cámara web instalada o conectada y si el programa Face Recognition está instalado, puede establecer el nivel de seguridad de Face Recognition para equilibrar la facilidad de uso y la dificultad de violar la seguridad del equipo.

1. Haga clic en **Inicio**, en **Todos los programas**, en **HP** y después en **Consola administrativa de HP ProtectTools**.
2. Haga clic en **Credenciales** y, a continuación, haga clic en **Rostro**.
3. Si desea más practicidad, haga clic en la barra deslizante para moverla hacia la izquierda o, si necesita más precisión, haga clic en la barra deslizante para moverla 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 hacia la posición **Practicidad**.
   - **Equilibrio**: para brindar una buena simetría entre seguridad y capacidad de uso, o en caso de que tenga información confidencial o su equipo se encuentre en un área donde puedan producirse intentos de iniciar sesión sin autorización, haga clic en la barra deslizante para moverla a la posición **Equilibrio**.
   - **Precisión**: para dificultar que un usuario logre acceder si las escenas de registro o las condiciones de iluminación actuales están por debajo de lo normal y es menos probable que se produzca una falsa aceptación, haga clic en la barra deslizante para moverla a la posición **Precisión**.
4. Haga clic en **Avanzada** y luego configure la seguridad adicional. Para obtener más información, consulte Configuración de usuario avanzada en la página 42.
5. Haga clic en **Aplicar**.

Configuración de sus aplicaciones

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 panel izquierdo de la Consola administrativa, en **Aplicaciones**, haga clic en **Configuración**.
2. Seleccione la casilla de verificación que está al lado de una configuración específica para activarla o desmarque esta casilla para desactivarla.
3. Haga clic en **Aplicar**.

Ficha General

Se encuentran disponibles las siguientes configuraciones 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 iniciar la sesión.
- **No iniciar automáticamente el Asistente de pasos iniciales para usuarios**: seleccione esta opción para evitar que la configuración del usuario se abra automáticamente al iniciar la 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 de forma predeterminada es la siguiente:

- **Estado de las aplicaciones**: activa el estado que se mostrará para todas las aplicaciones.
- **Password Manager**: activa Password Manager para todos los usuarios del equipo.
- **Privacy Manager**: activa Privacy Manager para todos los usuarios del equipo.
- **Activar el enlace de Administración central**: permite que todos los usuarios de este equipo agreguen aplicaciones a HP ProtectTools Security Manager haciendo clic en **Administración central**.

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

Administración central

Puede disponerse de aplicaciones adicionales para agregar nuevas herramientas de administración a Security Manager. El administrador de este equipo puede desactivar este recurso en la página Configuración. La página Administración central tiene dos fichas:

- **Soluciones de negocios**: si se dispone de una conexión a Internet, es posible acceder al sitio web de DigitalPersona (http://www.digitalpersona.com/ para comprobar si hay nuevas aplicaciones.
- **Actualizaciones y mensajes**
  - Para solicitar información sobre nuevas aplicaciones y actualizaciones, seleccione la casilla de verificación **Manténgame informado sobre las nuevas aplicaciones y actualizaciones**.
  - Para definir un cronograma de actualizaciones automáticas, seleccione el número de días.
  - Para verificar si hay actualizaciones, haga clic en **Verificar ahora**.

4 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 las preferencias de programa.
- Utilice huellas digitales para obtener más 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.

Apertura de Security Manager

Puede abrir Security Manager de cualquiera de las siguientes maneras:

- Haga clic en **Inicio**, **Todos los programas**, **HP** y luego haga clic 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 del mouse en el icono **HP ProtectTools** y haga clic en **Abrir HP ProtectTools Security Manager**.
- Haga clic en el icono de gadget de escritorio de **HP ProtectTools**.
- Presione la combinación de teclas de acceso rápido ctrl+tecla de logotipo de Windows+h para abrir el menú **Enlaces rápidos de Security Manager**.

  Para obtener información adicional sobre el cambio de la combinación de las teclas de acceso rápido, consulte Configuración en la página 37.

Uso del panel de control de Security Manager

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

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

El panel de control muestra los siguientes componentes:

- **Tarjeta de identificación**: muestra el nombre del usuario de Windows y una imagen seleccionada que identifica la cuenta del usuario que inició la sesión.
- **Aplicaciones de seguridad**: muestra un menú expansible de los enlaces para la configuración de las siguientes categorías de seguridad:
  - **Inicio**: administre contraseñas, configure sus credenciales de autenticación o verifique el estado de las aplicaciones de seguridad.
  - **Estado**: verifique el estado de las aplicaciones de HP ProtectTools.

NOTA: Las aplicaciones que no están instaladas en el equipo no se muestran en la siguiente lista.

- **Mis inicios de sesión**: administre sus credenciales de autenticación con Password Manager, Credential Manager, Contraseña, SpareKey, Smart Card, Rostro y Huellas digitales.
- **Mis datos**: administre la seguridad de sus datos con Drive Encryption y File Sanitizer.
- **Mi PC**: administre la seguridad de su equipo con Device Access Manager.
- **Mis comunicaciones**: administre la seguridad de sus comunicaciones con Privacy Manager.
- **Administración**: permite que los administradores accedan a las siguientes opciones:
  - **Consola administrativa**: permite que los administradores administren la seguridad y los usuarios.
  - **Administración central**: permite que los administradores accedan a soluciones, actualizaciones de productos y mensajes adicionales.
- **Opciones avanzadas**: muestra comandos para acceder a recursos adicionales, que incluyen:
  - **Preferencias**: le permite personalizar las configuraciones de Security Manager.
  - **Copia de seguridad y restauración**: le permite realizar copias de seguridad o restaurar datos.
  - **Acerca de**: muestra información sobre HP ProtectTools Security Manager, por ejemplo el número de versión y el aviso de copyright.
- **Área principal**: muestra pantallas específicas de la aplicación.
- **?**: muestra la Ayuda del software Security Manager. Este icono está en la parte superior derecha de la ventana, al lado de los iconos para minimizar y maximizar.

Estado de las aplicaciones de seguridad

Puede visualizar el estado de sus aplicaciones de seguridad instaladas en dos lugares:

- **Gadget de escritorio de HP ProtectTools**

  El color del banner de la parte superior del icono de gadget de HP ProtectTools cambia para reflejar el estado general de la seguridad de sus aplicaciones de seguridad instaladas.

  - **Rojo**: Advertencia
  - **Amarillo**: Atención: no configurado
  - **Azul**: OK

  Aparecerá un mensaje en la parte inferior del icono de para indicar una de las siguientes condiciones:

  - **Configurar ahora**: el administrador debe hacer clic en el icono de para ejecutar el Asistente de configuración de Security Manager con el propósito de configurar las credenciales de autenticación para el equipo.

    El Asistente de configuración es una aplicación independiente.

  - **Registrar ahora**: un usuario debe hacer clic en el icono de a fin de ejecutar el Asistente de pasos iniciales de Security Manager para registrar las credenciales de autenticación.

    El Asistente de pasos iniciales aparece en el panel de control de Security Manager.

  - **Verificar ahora**: haga clic en el icono de para mostrar detalles adicionales en la página de estado de las Aplicaciones de seguridad.

- **Página de estado de las Aplicaciones de seguridad**: haga clic en **Estado**, en el panel de control de Security Manager, para mostrar el estado general de sus aplicaciones de seguridad instaladas y el estado específico de cada aplicación.

Mis inicios de sesión

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

- **Password Manager**: crea y administra Enlaces rápidos, que le permiten abrir e iniciar sesión en sitios web y programas mediante la autenticación con su contraseña de Windows, su huella digital o una Smart Card.
- **Credential Manager**: brinda un medio para cambiar fácilmente su contraseña de Windows, registrar sus huellas digitales o configurar una smart card.

Los administradores pueden agregar más aplicaciones haciendo clic en **Administración** y luego en **Administración central**, en el ángulo inferior izquierdo del panel de control.

Password Manager

Iniciar sesión en Windows, sitios web y aplicaciones es más fácil y más seguro cuando utiliza Password Manager. Puede utilizarlo para crear contraseñas más seguras 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.

Password Manager ofrece las siguientes opciones:

- Agregar, editar o eliminar inicios de sesión desde la ficha **Administrar**.
- Utilizar los Enlaces rápidos para abrir su navegador predeterminado e iniciar sesión en un sitio web o programa, una vez que se haya configurado.
- Arrastrar y soltar 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 segura y compleja para utilizar en sitios nuevos.

El icono de **Administrador de contraseñas** aparece en el ángulo superior izquierdo de una página web o pantalla de inicio de sesión de una aplicación. Cuando aún no se ha creado un inicio de sesión para ese sitio web o aplicación, aparece un signo más en el icono.

▲ Haga clic en el icono de **Password Manager** para mostrar un menú de contexto donde puede elegir entre las siguientes opciones.

Para páginas web o programas en los cuales aún no se creó un inicio de sesión

Las siguientes opciones se muestran en el menú de contexto:

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

Para páginas web o programas en los cuales ya se creó un 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 inicio de sesión**: le permite agregar una cuenta a un inicio de sesión.
- **Abrir Password Manager**: abre Password Manager.
- **Ayuda**: muestra la Ayuda del software Security Manager.

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 fácilmente un inicio de sesión para un sitio web o un programa introduciendo la información de inicio de sesión una vez. En adelante, Password Manager introduce automáticamente la información por usted. Puede utilizar estos inicios de sesión después de navegar en el sitio web o en un programa, o haga clic en un inicio de sesión en el menú **Inicios de sesión** para que Password Manager abra el sitio web o el programa e inicie la sesión por usted.

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 de **Password Manager** 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] a Password Manager**.
   - Para un programa, haga clic en **Agregar esta pantalla de inicio de sesión a Password Manager**.
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 están identificados con un borde naranja en negrita. También puede mostrar este cuadro de diálogo haciendo clic en **Agregar inicio de sesión**, en la ficha **Password Manager**. Algunas opciones dependen de los dispositivos de seguridad conectados al equipo: por ejemplo, la utilización de la tecla de acceso rápido ctrl +tecla del logotipo de 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 en forma automática los datos para el inicio de sesión**.
   d. Para activar la seguridad de VeriSign VIP, seleccione la casilla de verificación **Deseo seguridad VIP en este sitio**.

Esta opción aparece sólo para sitios donde se encuentra disponible VeriSign Identity Protection (VIP). Cuando el sitio lo admita, también podrá optar por tener su Código de seguridad VIP completado automáticamente con su método habitual de autenticación.

e. Haga clic en **Aceptar**, haga clic en el método de autenticación que desea utilizar (huellas digitales, contraseña o rostro) y luego inicie la sesión con el método de autenticación seleccionado.

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

f. Si Password Manager no detecta los campos de inicio de sesión, haga clic en **Más campos**.

- Seleccione la casilla de verificación de cada campo que se requiere para el inicio de sesión o desmarque la casilla de verificación de los campos que no se requieren.
- Si Password Manager no puede detectar todos los campos de inicio de sesión, aparece un mensaje que le pregunta si desea continuar. Haga clic en **Sí**.
- Se abre un cuadro de diálogo con sus campos de inicio de sesión completados. Haga clic en el icono de cada campo y arrástrelo hasta el campo de inicio de sesión correspondiente. A continuación, 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, deberá 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.

- Haga clic en **Cerrar**.

Cada vez que accede a ese sitio web o abre ese programa, aparece el icono de **Password Manager** en el ángulo superior izquierdo de un sitio web o pantalla de inicio de sesión de la aplicación, 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 de **Password Manager** 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 **Password Manager**.
3. Edite su información de inicio de sesión.

   - Para seleccionar un campo de inicio de sesión de **Nombre de usuario** con una de las opciones formateadas previamente, haga clic en las flechas hacia abajo a la derecha del campo.
   - Para seleccionar un campo de inicio de sesión de **Contraseña** con una de las opciones formateadas previamente, haga clic en las flechas hacia abajo a la derecha del campo.

- Para activar la seguridad de VeriSign VIP, seleccione la casilla de verificación **Deseo seguridad VIP en este sitio**.

  Esta opción aparece sólo para sitios donde se encuentra disponible la seguridad VeriSign VIP. Cuando el sitio lo admita, también podrá optar por tener su Código de seguridad VIP completado automáticamente con su método habitual de autenticación.

- Para agregar campos adicionales de la pantalla a su inicio de sesión, haga clic en **Más campos**.

- Para ver la contraseña para este inicio de sesión, haga clic en **Mostrar contraseña**.

- Para tener los campos de inicio de sesión completados, pero no enviados, desmarque la casilla de verificación **Enviar en forma automática los datos para el inicio de sesión**.

4. Haga clic en **Aceptar**.

Uso del menú de inicios de sesión

Password Manager ofrece una forma rápida y fácil de abrir los sitios web y los programas para los que creó inicios de sesión. Para abrir la pantalla de inicio de sesión, haga doble clic en el inicio de sesión de un programa o sitio web del menú **Inicios de sesión** o de la ficha **Administrar**, de Password Manager. A continuación, complete sus datos de inicio de sesión.

Cuando crea un inicio de sesión, este se agrega automáticamente a su menú de **Password Manager**.

Para mostrar el menú **Inicios de sesión**:

1. Presione la combinación de teclas de acceso rápido de **Password Manager** (ctrl+tecla del logotipo de Windows+h es la configuración de fábrica). Para cambiar la combinación de teclas de acceso rápido en el panel de control de Security Manager, haga clic en **Password Manager** y luego en **Configuración**.

2. Pase su dedo por el lector de huellas digitales (en equipos con un lector de huellas digitales incorporado o conectado) o introduzca su contraseña de Windows.

Organización de inicios de sesión en categorías

Cree una o más categorías para mantener sus inicios de sesión en orden. 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 **Password Manager**.

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 resaltan cuando mueve el puntero de su mouse 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

Password Manager hace que sea fácil administrar su 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 enumeran en la ficha **Administrar**. Si se crearon múltiples inicios de sesión para el mismo sitio web, cada inicio de sesión se enumera bajo el nombre del sitio web y aparece con sangría en la lista de inicios de sesión.

Para administrar sus inicios de sesión:

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

- **Agregar un inicio de sesión**: haga clic en **Agregar inicio de sesión** y siga las instrucciones que aparecen en la pantalla.
- **Sus inicios de sesión**: haga clic en un inicio de sesión existente, seleccione una de las siguientes opciones y luego siga las instrucciones que aparecen en la pantalla:
  - **Abrir**: abra un sitio web o programa para el que tiene un inicio de sesión existente.
  - **Agregar**: agregue un inicio de sesión. Para obtener más información, consulte Adición de inicios de sesión en la página 31.
  - **Editar**: edite un inicio de sesión. Para obtener más información, consulte Edición de inicios de sesión en la página 32.
  - **Eliminar**: elimine un sitio web o programa para el que tiene un inicio de sesión existente.
- **Agregar categoría**: haga clic en **Agregar categoría** y luego siga las instrucciones que aparecen en la pantalla. Para obtener más información, consulte Organización de inicios de sesión en categorías en la página 33.

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 de **Password Manager** para mostrar su menú de contexto.
3. Haga clic en **Agregar un inicio de sesión** y luego siga las instrucciones que aparecen en la pantalla.

Evaluación de la solidez de su contraseña

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

Password Manager 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 de Password Manager

Password Manager 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 usted no creó un inicio de sesión, Password Manager le pide que agregue un inicio de sesión para la pantalla mostrando el icono de **Password Manager** con un signo más.

1. Haga clic en la flecha del icono y luego en **Configuraciones del icono** para personalizar la forma en que Password Manager 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 Password Manager le pida que agregue 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 para que Password Manager no le vuelva a pedir que agregue un inicio de sesión en esta pantalla de inicio de sesión.

     A fin de agregar un inicio de sesión para una pantalla que se ha excluido previamente:

     - Mientras se muestra el inicio de sesión del sitio web o la página del programa previamente excluidos, abra el panel de control de Security Manager y luego haga clic en **Password Manager**.
     - Haga clic en **Agregar inicio de sesión**.

       Se abre el cuadro de diálogo Agregar inicio de sesión con la pantalla de inicio de sesión del sitio web o el programa indicado en el campo **Pantalla actual**.
     - Haga clic en **Continuar**.

       Aparece la pantalla Agregar inicio de sesión a Password Manager.
     - Siga las instrucciones que aparecen en pantalla. Para obtener más información, consulte Adición de inicios de sesión en la página 31.
     - El icono de **Password Manager** aparece cada vez que se abre este inicio de sesión del sitio web o pantalla del programa.
2. A fin de desactivar la opción de mostrar un mensaje para agregar inicios de sesión para las pantallas de inicio de sesión, seleccione la casilla de verificación.
3. Para acceder a las configuraciones adicionales de Password Manager, haga clic en **Password Manager** y entonces en **Configuración**, en el panel de control de Security Manager.

VeriSign Identity Protection (VIP)

Puede crear tokens de VeriSign VIP Access para utilizar con los sitios web compatibles con VeriSign VIP. Estos tokens son utilizados por Password Manager para crear inicios de sesión automatizados que incorporan el uso de los tokens arrastrados y soltados en las pantallas de inicio de sesión compatibles con VeriSign VIP o ingresados manualmente en los campos específicos.

Puede activar VeriSign VIP y crear un token desde el panel de control de Security Manager o en cualquier sitio web compatible con VeriSign VIP. A fin de utilizar el token, debe registrarlo en cada sitio web donde se utilizará.

Después del registro y el primer uso de un token, este puede agregarse (opcionalmente) y enviarse con sus credenciales de inicio de sesión normales. Para los sitios que no permiten agregar el token, puede arrastrar y soltar o ingresar manualmente la información del token.

Para activar VeriSign VIP y crear un token de VeriSign VIP desde el panel de control de Security Manager:

1. Abra el panel de control de Security Manager. Para obtener más información, consulte Apertura de Security Manager en la página 27.
2. Haga clic en **Password Manager** y luego en **VIP**.
3. Haga clic en **Obtener VIP**.

   Se crea un token de VeriSign VIP y se muestra en la página de VeriSign VIP. El token se mostrará ahora cada vez que acceda a esta página.

Para activar VeriSign VIP y crear un token de VeriSign VIP desde un sitio web:

1. Password Manager lo alerta cada vez que visita un sitio web compatible con VeriSign VIP.
2. Cree un inicio de sesión para la pantalla. Para obtener más información, consulte Adición de inicios de sesión en la página 31.
3. En el cuadro de diálogo Crear inicio de sesión, seleccione **Deseo protección adicional para la cuenta con VIP**.

Para registrar un token de VeriSign VIP para un sitio web:

1. Inicie sesión en un sitio web compatible con VeriSign VIP manualmente o con un inicio de sesión de Password Manager.
2. Para crear un inicio de sesión para este sitio, haga clic en el globo de VeriSign VIP que aparece.
3. En el cuadro de diálogo Agregar inicio de sesión a Password Manager, seleccione **Deseo seguridad VIP en este sitio**.

   Esta opción aparece sólo para sitios donde se encuentra disponible la seguridad VeriSign VIP. Cuando el sitio lo admita, también podrá optar por tener su Código de seguridad VIP completado automáticamente con su método habitual de autenticación.

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 de **Password Manager** 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 usted 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. **Abrir Password Manager con ctrl+win+h**: la tecla de acceso rápido predeterminada que abre el menú **Enlaces rápidos de Password Manager** es ctrl+tecla del logotipo de Windows+h. Para cambiar las teclas de acceso rápido, haga clic en esta opción e introduzca una nueva combinación de teclas. Las combinaciones pueden incluir una o más de las siguientes opciones: ctrl, alt o mayús y cualquier tecla alfabética o numérica.
3. Haga clic en **Aplicar** para guardar los cambios.

Credential Manager

Utiliza sus credenciales de Security Manager para verificar que realmente es usted. El administrador 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. Las credenciales, requisitos y estado actual compatibles aparecen cuando hace clic en **Credential Manager** en **Mis inicios de sesión** y pueden incluir lo siguiente:

- Contraseña
- SpareKey
- Huellas digitales
- Smart Card
- Rostro

Para registrar o cambiar una credencial, haga clic en el enlace y 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 **Credential Manager** y luego 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 contraseña nueva**.
4. Haga clic en **Cambiar** para cambiar inmediatamente su contraseña actual por la nueva que introdujo.

Configuración de su SpareKey

La SpareKey le permite acceder a su equipo (en plataformas compatibles) al responder a tres preguntas de seguridad de una lista previamente definida por el administrador.

HP ProtectTools Security Manager le solicita que configure su SpareKey personal durante la configuración inicial en el Asistente de pasos iniciales.

Para configurar su SpareKey:

1. En la página de SpareKey del asistente, seleccione tres preguntas de seguridad y luego ingrese una respuesta para cada pregunta.
2. Haga clic en **Siguiente**.

Puede seleccionar preguntas diferentes o cambiar sus respuestas, en la página de SpareKey en **Credential Manager**.

Una vez configurada su SpareKey, puede acceder a su equipo con su SpareKey desde una pantalla de inicio de sesión de preinicio o la pantalla de bienvenida de Windows.

Registro de sus huellas digitales

Si su equipo tiene un lector de huellas digitales incorporado o conectado, HP ProtectTools Security Manager le solicita que configure o “registre” sus huellas digitales durante la configuración inicial en el Asistente de pasos iniciales. También puede registrar sus huellas digitales en la página de Huellas digitales de **Credential Manager**, en el panel de control de Security Manager.

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 previamente, haga clic en el dedo correspondiente.

2. Cuando haya seleccionado un dedo para registrar, se le solicitará que lo pase por el lector de huellas digitales hasta que la huella digital se haya registrado correctamente. Un dedo registrado aparece resaltado en verde en el contorno.
3. Debe registrar por lo menos dos dedos; se prefieren los dedos índices o medios. Repita los pasos 1 y 2 para otro dedo.
4. Haga clic en **Siguiente** y luego siga las instrucciones que aparecen en pantalla.

PRECAUCIÓN: Cuando se registran las huellas digitales a través del proceso Pasos iniciales, la información de la huella digital no se guarda hasta que hace clic en **Siguiente**. Si deja el equipo inactivo durante un tiempo o cierra el programa, los cambios que haya realizado **no** se guardan.

Configuración de una smart card

Los administradores deben inicializar y registrar la smart card antes de que esta pueda utilizarse para la autenticación.

Inicialización de la smart card

HP ProtectTools Security Manager es compatible con diversas variedades de smart card. El número y el tipo de caracteres utilizados como números de PIN son variables. El fabricante de la smart card debe proporcionar herramientas para instalar un certificado de seguridad y PIN de administración que HP ProtectTools utilizará en su algoritmo de seguridad.

NOTA: El software ActivIdentity debe estar instalado.

1. Inserte la tarjeta en el lector.
2. Haga clic en **Inicio**, en **Todos los programas** y luego en **ActivClient PIN Initialization Tool** (Herramienta de inicialización de PIN de ActivClient).
3. Introduzca y confirme un PIN.
4. Haga clic en **Siguiente**.

   El software de smart card proporcionará una clave de desbloqueo. La mayoría de las smart cards se bloquearán si se introduce el PIN de forma incorrecta 5 veces. Se utiliza la clave para desbloquear la tarjeta.
5. Haga clic en **Inicio**, en **Todos los programas**, en **HP** y después en **Consola administrativa de HP ProtectTools**.
6. Haga clic en **Credenciales** y luego en **Smart Card**.
7. Haga clic en la ficha **Administración**.
8. Asegúrese de que **Configurar la smart card** esté seleccionado.
9. Introduzca su PIN, haga clic en **Aplicar** y luego siga las instrucciones que aparecen en pantalla.
10. Después de que se haya inicializado correctamente la smart card, usted deberá registrarla.

Registro de la smart card

Después de la inicialización de la smart card, los administradores pueden registrarla como un método de autenticación en la Consola administrativa de HP ProtectTools:

1. En **Administración central**, haga clic en **Asistente de configuración**.
2. En la página “¡Bienvenido!”, haga clic en **Siguiente** y luego escriba su contraseña de Windows.
3. En la página de SpareKey, haga clic en **Saltar la configuración de SpareKey**, a menos que desee actualizar la información de SpareKey.
4. En la página Active los recursos de seguridad, haga clic en **Siguiente**.
5. En la página Elija sus credenciales, asegúrese de que la opción **Configurar su smart card** esté seleccionada y, a continuación, haga clic en **Siguiente**.
6. En la página Smart card, escriba su PIN y luego haga clic en **Siguiente**.
7. Haga clic en **Finalizar**.

Los usuarios también pueden registrar una smart card en Security Manager. Para obtener más información, consulte la ayuda de software de Security Manager for HP ProtectTools.

Configuración de la smart card

Si el equipo tiene una smart card instalada o conectada, la página de Smart Card tiene dos fichas:

- **Configuración**: configure el equipo para que este se bloquee automáticamente cuando se extrae una Smart Card.

NOTA: El equipo se bloquea sólo si se utilizó la Smart Card como credencial de autenticación al iniciar la sesión en Windows. La extracción de una Smart Card que no se utilizó para iniciar la sesión en Windows no bloquea el equipo.

- **Administración**: seleccione a partir de las siguientes opciones:
  - **Inicializar la smart card**: prepara una smart card para utilizar con HP ProtectTools. Si una smart card se inicializó previamente fuera de HP ProtectTools (contiene un par de claves asimétricas y certificado asociado), no es necesario inicializarla de nuevo, a menos que se desee realizar la inicialización con un certificado específico.
  - **Cambiar PIN de smart card**: le permite cambiar el PIN utilizado con la smart card.
  - **Borrar datos de HP ProtectTools únicamente**: borra sólo el certificado de HP ProtectTools creado durante la inicialización de la tarjeta. Ningún otro dato se borra de la tarjeta.
  - **Borrar todos los datos de la smart card**: borra todos los datos de la smart card especificada. La tarjeta ya no puede utilizarse con HP ProtectTools ni con cualquier otra aplicación.

NOTA: No se dispone de recursos que no sean compatibles con su smart card.

▲ Haga clic en **Aplicar**.

Registro de escenas para inicio de sesión mediante reconocimiento de rostros

Si su equipo tiene una cámara web incorporada o conectada, HP ProtectTools Security Manager le solicita que configure o “registre” sus escenas durante la configuración inicial en el Asistente de pasos iniciales. También puede registrar sus escenas en la página de Inicio de sesión mediante reconocimiento de rostros de **Credential Manager**, en el panel de control de Security Manager.

Debe registrar una o más escenas con el fin de utilizar el inicio de sesión mediante el reconocimiento de rostros. Después de que se haya registrado con éxito, también podrá registrar una nueva escena en caso de que haya tenido dificultad durante el inicio de sesión debido a que hayan cambiado una o más de las siguientes condiciones:

- 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: En caso de dificultades para registrar escenas, trate de acercarse a la cámara web.

Para registrar una escena desde el Asistente de pasos iniciales:

1. En la página de Rostros del asistente, haga clic en **Avanzada**, y luego configure la seguridad adicional. Para obtener más información, consulte Configuración de usuario avanzada en la página 42.
2. Haga clic en **Aceptar**.
3. Haga clic en **Inicio** o si ha registrado escenas previamente, haga clic en **Registrar una nueva escena**.
4. Si no seleccionó ninguna opción de seguridad adicional, se le pedirá que seleccione una opción de seguridad adicional. Siga las instrucciones que aparecen en pantalla y luego haga clic en **Siguiente**. Para obtener más información, consulte Configuración de usuario avanzada en la página 42.
5. Haga clic en el icono de la **Cámara** y luego siga las instrucciones que aparecen en la pantalla para registrar su escena.

   Siga las instrucciones que aparecen en la pantalla y asegúrese de mirar su imagen mientras se capturan las escenas.
6. Haga clic en **Siguiente**.
7. Haga clic en **Finalizar**.

También puede registrar escenas desde el panel de control de Security Manager:

1. Abra el panel de control de Security Manager. Para obtener más información, consulte Apertura de Security Manager en la página 27.
2. En **Mis inicios de sesión**, haga clic en **Credential Manager** y luego en **Rostro**.
3. Haga clic en **Avanzada** y luego configure la seguridad adicional. Para obtener más información, consulte Configuración de usuario avanzada en la página 42.
4. Haga clic en **Aceptar**.
5. Haga clic en **Inicio** o si ha registrado escenas previamente, haga clic en **Registrar una nueva escena**.
6. Si no seleccionó ninguna opción de seguridad adicional, se le pedirá que seleccione una opción de seguridad adicional. Siga las instrucciones que aparecen en pantalla y luego haga clic en **Siguiente**. Para obtener más información, consulte Configuración de usuario avanzada en la página 42.
7. Haga clic en el icono de la **Cámara** y luego siga las instrucciones que aparecen en la pantalla para registrar su escena.

   Siga las instrucciones que aparecen en la pantalla y asegúrese de mirar su imagen mientras se capturan las escenas.

Para obtener más información, consulte la ayuda del software Face Recognition haciendo clic en el icono de **?** azul en la parte superior derecha de la página de Inicio de sesión mediante reconocimiento de rostros.

Configuración de usuario avanzada

Estas opciones también aparecen en la página de Seguridad adicional si no se ha seleccionado seguridad adicional.

1. Abra el panel de control de Security Manager. Para obtener más información, consulte Apertura de Security Manager en la página 27.
2. En **Mis inicios de sesión**, haga clic en **Credential Manager** y luego en **Rostro**.
3. Haga clic en **Avanzada** para configurar las siguientes opciones de seguridad:

   a. Ficha **Seguridad**: seleccione una de las siguientes opciones:

   - **Sin seguridad adicional**: seleccione esta opción si no desea agregar seguridad adicional para el inicio de sesión mediante reconocimiento de rostros.
   - **Usar PIN para seguridad adicional**: seleccione esta opción para solicitar un PIN específico del usuario para el inicio de sesión mediante reconocimiento de rostros.
     - Haga clic en **Crear PIN**.
     - Escriba su contraseña de Windows.
     - Escriba el nuevo PIN y luego confirme el nuevo PIN reingresándolo.

       Una vez creado un PIN, puede seleccionar entre las opciones que se presentan a continuación: **Cambiar**, **Restablecer** o **Eliminar un PIN**.
   - **Usar Bluetooth para seguridad adicional**: seleccione esta opción para emparejar su teléfono compatible con Bluetooth con Face Recognition. Durante el inicio de sesión de Windows, una vez que está autenticado su rostro, Face Recognition también verifica la presencia del teléfono Bluetooth emparejado. Si el teléfono se encuentra presente (con Bluetooth activado), entonces se le permite que inicie sesión en Windows.
     - Asegúrese de que Bluetooth esté activado tanto en el equipo como en el teléfono.

       Si un teléfono compatible con Bluetooth no se encuentra presente, se le pedirá que active el teléfono Bluetooth emparejado y reinicie el proceso de inicio de sesión. Después de 30 segundos, la ventana de inicio de sesión de Face Recognition hace una pausa. Para iniciar el proceso de inicio de sesión, haga clic en el icono de la **Cámara**. Si el teléfono compatible con Bluetooth no se encuentra presente, puede utilizar su contraseña normal de Windows para iniciar sesión.
     - Haga clic en **Agregar**.
     - Cuando aparezca su dispositivo Bluetooth, selecciónelo y luego haga clic en **Siguiente**.

Haga clic en **Aceptar**.

b. Ficha **Otras configuraciones**: seleccione las casillas de verificación para activar una o más de las siguientes opciones o desmarque la casilla de verificación para desactivar una opción. Esta configuración se aplica sólo al usuario actual.

- **Reproducir sonido en los eventos de reconocimiento de rostros**: reproduce un sonido cuando el inicio de sesión mediante reconocimiento de rostros se realiza con éxito o falla.
- **Solicitar actualizar las escenas cuando falla el inicio de sesión**: si el inicio de sesión mediante reconocimiento de rostros falla, pero usted logra introducir su contraseña correctamente, se le puede solicitar que guarde una serie de imágenes para aumentar las posibilidades de un inicio de sesión mediante reconocimiento de rostros correcto en el futuro.
- **Solicitar registrar una escena nueva cuando falla el inicio de sesión**: si el inicio de sesión mediante reconocimiento de rostros falla, pero usted logra introducir su contraseña con éxito, se le puede solicitar que registre una nueva escena para aumentar las posibilidades de un inicio de sesión mediante reconocimiento de rostros exitoso en el futuro.

Haga clic en **Aceptar**.

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.

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. Abra el panel de control de Security Manager. Para obtener más información, consulte Apertura de Security Manager en la página 27.
2. Haga clic en la Tarjeta de identificación en el ángulo superior izquierdo del panel de control.
3. Haga clic en la casilla donde aparece su nombre de usuario de Windows para esta cuenta, introduzca el nuevo nombre y luego haga clic en **Guardar**.

Para cambiar la imagen que se muestra:

1. Abra el panel de control de Security Manager. Para obtener más información, consulte Apertura de Security Manager en la página 27.
2. Haga clic en la Tarjeta de identificación en el ángulo superior izquierdo del panel de control.
3. Haga clic en **Elegir imagen**, haga clic en una imagen y a continuación haga clic en **Guardar**.

Configuración de sus preferencias

Puede personalizar configuraciones para HP ProtectTools Security Manager. En el panel de control de Security Manager, haga clic en **Avanzadas** y a continuación haga clic en **Preferencias**. Las configuraciones disponibles aparecen en dos fichas: **General** y **Huella digital**.

Ficha General

Apariencia: **muestra el icono en el área de notificación de la barra de tareas**

- 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.

Ficha Huella digital

NOTA: La ficha **Huella digital** está disponible sólo si el equipo tiene un lector de huellas digitales y el controlador correcto está instalado.

- **Acciones rápidas**: utilice Acciones rápidas para seleccionar la tarea de Security Manager que se realizará cuando mantenga presionada una tecla designada mientras pasa su dedo por el lector de huellas digitales.

  Para asignar una Acción rápida 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.

- **Respuesta del escáner de huellas digitales**: aparece sólo cuando se dispone de un lector de huellas digitales. Utilice esta configuración para ajustar la respuesta que se produce cuando pasa su dedo por el lector de huellas digitales.

  - **Activar respuesta de sonido**: Security Manager le da una respuesta de audio cuando pasa su dedo por el lector de huellas digitales, reproduciendo diferentes sonidos para eventos específicos del programa. Puede asignar nuevos sonidos a estos eventos por medio de la ficha **Sonidos** 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 todas las huellas digitales pasadas por el lector, independientemente de la calidad, seleccione la casilla de verificación.

    Para mostrar sólo las huellas digitales de buena calidad pasadas por el lector, desmarque la casilla de verificación.

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 debe realizar 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, lo cual también se denomina 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. Abra el panel de control de Security Manager. Para obtener más información, consulte Apertura de Security Manager en la página 27.
2. En el panel izquierdo del panel de control, haga clic en **Avanzadas** y luego en **Copia de seguridad y restauración**.
3. Haga clic en **Copia de seguridad de datos**.
4. Seleccione los módulos que desea incluir en la copia de seguridad. En la mayoría de los casos, seleccionará todos los módulos.
5. Verifique su identidad.

6. Introduzca un nombre para el archivo de almacenamiento. De forma predeterminada, el archivo se guarda en su carpeta de Documentos. Haga clic en **Examinar** para especificar una ubicación diferente.
7. Introduzca una contraseña para proteger el archivo.
8. Haga clic en **Finalizar**.

Para restaurar sus datos:

1. Abra el panel de control de Security Manager. Para obtener más información, consulte Apertura de Security Manager en la página 27.
2. En el panel izquierdo del panel de control, haga clic en **Avanzadas** y luego en **Copia de seguridad y restauración**.
3. Haga clic en **Restaurar datos**.
4. Seleccione el archivo de almacenamiento que se creó anteriormente. Introduzca la ruta en el campo proporcionado o haga clic en **Examinar**.
5. Introduzca la contraseña utilizada para proteger el archivo.
6. Seleccione los módulos para los cuales desea restaurar los datos. En la mayoría de los casos, seleccionará todos los módulos indicados.
7. Verifique su contraseña de Windows.
8. Haga clic en **Finalizar**.

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

Drive Encryption for HP ProtectTools brinda una completa protección de datos mediante la encriptación la unidad de disco duro de su equipo. Cuando Drive Encryption está activado, debe iniciar la 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 Security Manager permite que los administradores de Windows activen Drive Encryption, hagan una copia de seguridad de la clave de encriptación y seleccionen o anulen la selección de unidades. Para obtener más información, consulte la ayuda del software HP ProtectTools Security Manager.

Es posible realizar las siguientes tareas con Drive Encryption:

- Selección de la configuración de Drive Encryption:
  - Activación de una contraseña protegida por TPM
  - Encriptación o desencriptación de unidades o particiones individuales mediante el uso de encriptación de software
  - Encriptación o desencriptación de unidades de autoencriptación individuales mediante el uso de encriptación de hardware
  - Adición de seguridad extra por medio de la desactivación de la suspensión o del modo de espera para asegurar que siempre se requiera la autenticación de preinicio de Drive Encryption

NOTA: Sólo las unidades de disco duro interna SATA y externa eSATA pueden encriptarse.

- Creación de claves de copia de seguridad
- Recuperación de una clave de Drive Encryption
- Activación de la autenticación de preinicio de Drive Encryption mediante el uso de una contraseña, una huella digital registrada o un PIN de smart card

Apertura de Drive Encryption

Los administradores pueden acceder a Drive Encryption desde la Consola administrativa de HP ProtectTools.

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

Tareas generales

Activación de Drive Encryption para unidades de disco duro estándares

Las unidades de disco duro estándares se encriptan por medio de encriptación de software. Siga estos pasos para activar Drive Encryption:

1. Utilice el Asistente de configuración de HP ProtectTools Security Manager para activar Drive Encryption.
2. Siga las instrucciones que aparecen en pantalla hasta que se muestre la página **Active los recursos de seguridad** y luego continúe con el paso 4 presentado a continuación.

– o –

1. Haga clic en **Inicio**, en **Todos los programas**, en **HP** y después en **Consola administrativa de HP ProtectTools**.
2. En el panel izquierdo, haga clic en el icono **+** que está a la izquierda de **Seguridad** para mostrar las opciones disponibles.
3. Haga clic en **Recursos**.
4. Seleccione la casilla de verificación **Drive Encryption** y entonces haga clic en **Siguiente**.

NOTA: Si no se selecciona ninguna unidad de disco duro para la encriptación, se activará la autenticación de preinicio de Drive Encryption, pero no se encriptará(n) la(s) unidad(es).

5. En **Unidades que se encriptarán**, seleccione la casilla de verificación de la unidad de disco duro que desea encriptar y luego haga clic en **Siguiente**.
6. Para hacer una copia de seguridad de la clave de encriptación, 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. Un disquete, una memoria USB, una tarjeta de memoria Secure Digital (SD) o una MMC pueden utilizarse para hacer copias de seguridad.

7. En **Crear copia de seguridad de las claves de Drive Encryption**, seleccione la casilla de verificación del dispositivo de almacenamiento donde se guardará la clave de encriptación.
8. Haga clic en **Siguiente**.

NOTA: El equipo se reiniciará.

Se ha activado Drive Encryption. La encriptación de la unidad puede tardar varias horas, según el tamaño de la unidad.

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

Activación de Drive Encryption para unidades de autoencriptación

Las unidades de autoencriptación que cumplen la especificación OPAL de Trusted Computing Group para la administración de unidades de autoencriptación pueden encriptarse mediante el uso de la

encriptación de software o de hardware. Siga estos pasos a fin de activar Drive Encryption para unidades de autoencriptación:

1. Utilice el Asistente de configuración de HP ProtectTools Security Manager para activar Drive Encryption.
2. Siga las instrucciones que aparecen en pantalla hasta que se muestre la página **Active los recursos de seguridad** y luego continúe con el paso 4 de “Encriptación de software” o “Encriptación de hardware”, presentados a continuación.

NOTA: Si su equipo no tiene una unidad de autoencriptación que cumpla con la especificación OPAL de Trusted Computing Group para la administración de unidades de autoencriptación, entonces la opción de encriptación de hardware no se encuentra disponible y la encriptación de software se utiliza de forma predeterminada.

Si hay una combinación de unidades de autoencriptación y unidades de disco duro estándares, entonces la opción de encriptación de hardware no se encuentra disponible y la encriptación de software se utiliza de forma predeterminada.

– o –

Encriptación de software

1. Haga clic en **Inicio**, en **Todos los programas**, en **HP** y después en **Consola administrativa de HP ProtectTools**.
2. En el panel izquierdo, haga clic en el icono **+** que está a la izquierda de **Seguridad** para mostrar las opciones disponibles.
3. Haga clic en **Recursos**.
4. Seleccione la casilla de verificación **Drive Encryption** y entonces haga clic en **Siguiente**.
5. En **Unidades que se encriptarán**, seleccione la casilla de verificación de la unidad de disco duro que desea encriptar y luego haga clic en **Siguiente**.
6. Para hacer una copia de seguridad de la clave de encriptación, 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. Un disquete, una memoria USB, una tarjeta de memoria Secure Digital (SD) o MMC pueden utilizarse para copias de seguridad.

7. En **Crear copia de seguridad de las claves de Drive Encryption**, seleccione la casilla de verificación del dispositivo de almacenamiento donde se guardará la clave de encriptación.
8. Haga clic en **Aplicar**.

   NOTA: El equipo se reiniciará.

   Se ha activado Drive Encryption. La encriptación de la unidad puede tardar varias horas, según el tamaño de la unidad.

Encriptación de hardware

1. Haga clic en **Inicio**, en **Todos los programas**, en **HP** y después en **Consola administrativa de HP ProtectTools**.
2. En el panel izquierdo, haga clic en el icono **+** que está a la izquierda de **Seguridad** para mostrar las opciones disponibles.
3. Haga clic en **Recursos**.
4. Seleccione la casilla de verificación **Drive Encryption** y entonces haga clic en **Siguiente**.

NOTA: Si sólo se muestra una unidad, la casilla de verificación de la unidad se selecciona automáticamente y se pone de color gris.

Si se muestra más de una unidad, las casillas de verificación de las unidades se seleccionan automáticamente pero no se ponen de color gris.

El botón **Siguiente** no estará disponible hasta que se haya seleccionado por lo menos una unidad.

5. Asegúrese de que la casilla de verificación **Utilizar encriptación de unidad de hardware** esté seleccionada en la parte inferior de la pantalla.
6. En **Unidades que se encriptarán**, seleccione la casilla de verificación de la unidad de disco duro que desea encriptar y luego haga clic en **Siguiente**.
7. Para hacer una copia de seguridad de la clave de encriptación, 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. Un disquete, una memoria USB, una tarjeta de memoria Secure Digital (SD) o MMC pueden utilizarse para copias de seguridad.

8. En **Crear copia de seguridad de las claves de Drive Encryption**, seleccione la casilla de verificación del dispositivo de almacenamiento donde se guardará la clave de encriptación.
9. Haga clic en **Aplicar**.

NOTA: Será necesario reiniciar el equipo.

Se ha activado Drive Encryption. La encriptación de la unidad puede tardar varios minutos.

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

Desactivación de Drive Encryption

Los administradores pueden utilizar el Asistente de configuración de HP ProtectTools Security Manager para desactivar Drive Encryption. Para obtener más información, consulte la ayuda del software HP ProtectTools Security Manager.

▲ Siga las instrucciones que aparecen en pantalla hasta que se muestre la página **Active los recursos de seguridad** y luego continúe con el paso 4 presentado a continuación.

- o -

1. Haga clic en **Inicio**, en **Todos los programas**, en **HP** y después en **Consola administrativa de HP ProtectTools**.
2. En el panel izquierdo, haga clic en el icono **+** que está a la izquierda de **Seguridad** para mostrar las opciones disponibles.
3. Haga clic en **Recursos**.
4. Desmarque la casilla de verificación **Drive Encryption** y luego haga clic en **Siguiente**.

   Comenzará la desactivación de Drive Encryption.

NOTA: Si se utilizó encriptación de software, se iniciará la desencriptación. Esta puede tardar varias horas, según el tamaño de la unidad. Cuando la desencriptación haya terminado, se desactivará Drive Encryption.

Si se utilizó encriptación de hardware, la unidad se desencriptará instantáneamente, lo cual puede tardar varios minutos, y luego se desactivará Drive Encryption.

Una vez desactivada la unidad, será necesario reiniciar el equipo.

Inicio de sesión después de la activación de Drive Encryption

Cuando encienda el equipo después haber activado Drive Encryption y registrado su cuenta de usuario, deberá iniciar la sesión en la pantalla de inicio de sesión de Drive Encryption:

NOTA: En caso de encriptación de hardware, asegúrese de que el equipo esté apagado. Si el equipo no se apaga y luego se reinicia, no aparece la pantalla de autenticación de preinicio de Drive Encryption.

NOTA: Al salir de la suspensión o del modo de espera, no se muestra la autenticación de preinicio de Drive Encryption para la encriptación de software o hardware, a menos que esta se encuentre desactivada.

Al salir de la hibernación, se muestra la autenticación de preinicio de Drive Encryption.

NOTA: Si el administrador de Windows ha activado la seguridad de preinicio en HP ProtectTools Security Manager, usted puede iniciar sesión en el equipo inmediatamente después de encenderlo, en vez de hacerlo en la pantalla de inicio de sesión de Drive Encryption.

1. Haga clic en su nombre de usuario y a continuación escriba su contraseña de Windows o el PIN de smart card, o deslice un dedo cuya huella digital esté registrada.

NOTA: Son compatibles las siguientes smart cards:

Smart cards

- Smart Card ActivIdentity 64K V2C
- SIM ActivIdentity 48010-B DEC06
- Clave USB ActivIdentity V3.0 ZFG-48001-A

Lectores de PCMCIA

- Lector interno de Express Card 54 SCR3340
- SCR 201
- SCR 243 (también de la marca HP)
- ActivCard
- Omnikey 4040
- Cisco

Lectores USB

- ActivCard USB v2
- ActivCard USB v3
- ActivCard USB SCR 3310
- Omnikey Cardman 3121
- Omnikey Cardman 3021
- ACR32
- Terminal de smart card HP

2. Haga clic en **Aceptar**.

NOTA: Si utiliza una clave de recuperación para iniciar sesión en la pantalla de inicio de sesión de Drive Encryption, se le solicita que se autentique con su contraseña, PIN de smart card o huella registrada en la pantalla de inicio de sesión de Windows.

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

Se recomienda enfáticamente que utilice el Asistente de configuración de HP ProtectTools Security Manager para proteger sus datos mediante la encriptación de su unidad de disco duro:

1. En el panel izquierdo, haga clic en el icono **+** que está a la izquierda de **Drive Encryption** para mostrar las opciones disponibles.
2. Haga clic en **Configuración**.
3. Para las unidades encriptadas de software, seleccione las particiones de la unidad para encriptar.

NOTA: Esto también se aplica a un escenario de unidades mixtas en el cual están presentes una o más unidades de disco duro estándares y una o más unidades de autoencriptación.

– o –

▲ Para las unidades encriptadas de hardware, seleccione la(s) unidad(es) para encriptar. Debe seleccionarse por lo menos una unidad.

Mostrar el estado de la encriptación

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

NOTA: Los administradores pueden cambiar el estado de Drive Encryption utilizando la Consola administrativa de HP ProtectTools.

1. Abra HP ProtectTools Security Manager.
2. En **Mis datos**, haga clic en **Drive Encryption**.

   En caso de encriptación de software, se muestra uno de los siguientes códigos de estado en **Estado de la unidad**:

   - Activado
   - Desactivado
   - No encriptado
   - Encriptado
   - Encriptando
   - Desencriptando

   En caso de encriptación de hardware, se muestra el siguiente código de estado en **Estado de la unidad**:

   - Encriptado

   Si la unidad de disco duro está en proceso de encriptarse o desencriptarse, una barra de progreso muestra el porcentaje completado y el tiempo restante para la conclusión de la encriptación o desencriptación.

Tareas avanzadas

Administración de Drive Encryption (tarea de administrador)

Los administradores pueden utilizar la página Configuración de Drive Encryption para ver y cambiar el estado de Drive Encryption (activado, inactivo o se activó la encriptación de hardware) y ver el estado de encriptación de todas las unidades de disco duro del equipo.

NOTA: No se puede cambiar la encriptación de hardware en la página Configuración.

- Si el estado es Desactivado, Drive Encryption aún no ha sido activado por el administrador de Windows y no está protegiendo la unidad de disco duro. Utilice el Asistente de configuración de HP ProtectTools Security Manager para activar Drive Encryption.
- Si el estado es Activado, se ha activado y configurado Drive Encryption. La unidad está en uno de los siguientes estados:

Encriptación de software

- No encriptado
- Encriptado
- Encriptando
- Desencriptando

- Encriptado

Encriptación o desencriptación de unidades individuales (sólo encriptación de software)

Los administradores pueden utilizar la página Configuración para encriptar una o más unidades de disco duro en el equipo o desencriptar una unidad que ya se ha encriptado.

1. Abra la Consola administrativa de HP ProtectTools.
2. En el panel izquierdo, haga clic en el icono **+** que está a la izquierda de **Drive Encryption** para mostrar las opciones disponibles.
3. Haga clic en **Configuración**.
4. En **Estado de la unidad**, seleccione o anule la selección de la casilla de verificación que está al lado de cada unidad de disco duro que desea encriptar o desencriptar y luego haga clic en **Aplicar**.

NOTA: Cuando se está encriptando o desencriptando la unidad, la barra de progreso muestra el tiempo restante para la conclusión del proceso durante la sesión actual.

Si el equipo se apaga o inicia la suspensión, el modo de espera o la hibernación durante el proceso de encriptación y luego se reinicia, el tiempo restante de la barra de progreso se restablece y vuelve al comienzo, pero la encriptación real se reanuda a partir del punto en el que se detuvo por última vez. La barra de progreso, mostrada como un porcentaje, y el tiempo restante cambian más rápidamente para reflejar el progreso anterior.

NOTA: No se admiten particiones dinámicas. Si una partición se muestra como disponible pero no puede encriptarse cuando se selecciona, la partición es dinámica. Una partición dinámica es consecuencia de la reducción de una partición para crear una nueva partición, lo cual se realiza en Administración de discos.

Si una partición se va a convertir en una partición dinámica, aparece una advertencia.

Copias de seguridad y recuperación (tarea de administrador)

Cuando Drive Encryption está activado, los administradores pueden utilizar la página Copia de seguridad de clave de encriptación para hacer copias de seguridad de claves de encriptación en medios extraíbles y realizar una recuperación.

Copias de seguridad de claves de encriptación

Los administradores pueden hacer una copia de seguridad de las claves de encriptación para una unidad encriptada en un dispositivo de almacenamiento extraíble.

PRECAUCIÓN: Asegúrese de mantener el dispositivo de almacenamiento que contiene la clave de copia de seguridad en un lugar seguro, porque si olvida su contraseña, pierde su smart card o no tiene una huella registrada, este dispositivo le brinda su único acceso a su unidad de disco duro.

1. Abra la Consola administrativa de HP ProtectTools.
2. En el panel izquierdo, haga clic en el icono **+** que está a la izquierda de **Drive Encryption** para mostrar las opciones disponibles.

3. Haga clic en **Copia de seguridad de clave de encriptación**.
4. Inserte el dispositivo de almacenamiento utilizado para hacer copia de seguridad de la clave de encriptación.
5. En **Unidad**, seleccione la casilla de verificación del dispositivo en el que desea hacer una copia de seguridad de su clave de encriptación.
6. Presione **Crear copia de seguridad de las claves**.
7. Lea la información de la página que se muestra y luego haga clic en **Siguiente**. La clave de encriptación se guarda en el dispositivo de almacenamiento que seleccionó.

Recuperación de claves de encriptación

Los administradores pueden recuperar una clave de encriptación a partir del dispositivo de almacenamiento extraíble en el cual esta se guardó anteriormente:

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 **Opciones**.
4. 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.

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

Privacy Manager for HP ProtectTools le permite utilizar métodos de inicio de sesión (autenticación) de seguridad avanzada para verificar la fuente, integridad y seguridad de las comunicaciones cuando se utiliza correo electrónico o documentos de Microsoft® Office.

Privacy Manager aprovecha la infraestructura de seguridad proporcionada por HP ProtectTools Security Manager, que incluye los siguientes métodos de inicio de sesión con seguridad:

- Autenticación por huella digital
- Contraseña de Windows®
- Smart Card
- Face Recognition

Puede utilizar cualquiera de los métodos de inicio de sesión de seguridad en Privacy Manager.

Apertura de Privacy Manager

Para abrir Privacy Manager:

- Para acceder a los recursos específicos de Outlook en Microsoft Outlook, haga clic en **Enviar con seguridad** en el grupo **Privacidad** de la ficha **Mensaje**.
- Para acceder a la mayoría de los recursos en documentos de Microsoft Office, haga clic en **Firme y codifique** en el grupo **Privacidad** de la ficha **Inicio**.
- Para acceder a recursos adicionales, acceda al panel de control de HP ProtectTools Security Manager.
  - Haga clic en **Inicio**, en **Todos los programas**, en **HP**, en **HP ProtectTools Security Manager** y luego en **Privacy Manager**.

    – o –
  - Haga clic en el icono de de escritorio de **HP ProtectTools**.

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

Procedimientos de configuración

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.

El Administrador de certificados le permite realizar las siguientes tareas:

- Solicitud de un certificado de Privacy Manager en la página 60
- Obtención de un certificado corporativo previamente asignado de Privacy Manager en la página 61
- Configuración de un certificado de Privacy Manager predeterminado en la página 63
- Importación de un certificado de terceros en la página 61
- Visualización de detalles de un certificado de Privacy Manager en la página 62
- Renovación de un certificado de Privacy Manager en la página 62
- Configuración de un certificado de Privacy Manager predeterminado en la página 63
- Eliminación de un certificado de Privacy Manager en la página 63
- Restauración de un certificado de Privacy Manager en la página 63
- Revocación de su certificado de Privacy Manager en la página 64

Solicitud de un certificado de Privacy Manager

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

1. Abra Privacy Manager y luego haga clic en **Certificados**.
2. Haga clic en **Solicitar un certificado de Privacy Manager**.
3. En la pantalla Bienvenido, lea el texto y luego haga clic en **Siguiente**.
4. En la página Contrato de licencia, lea el contrato de licencia.
5. Asegúrese de que la casilla de verificación que está al lado de **Haga clic aquí para aceptar los términos de este contrato de licencia** esté seleccionada y luego haga clic en **Siguiente**.
6. En la página Detalles de su certificado, ingrese la información necesaria y luego haga clic en **Siguiente**.
7. En la página Solicitud de certificado aceptada, haga clic en **Finalizar**.

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

Obtención de un certificado corporativo previamente asignado de Privacy Manager

1. En Outlook, abra el mensaje de correo electrónico que recibió indicando que un certificado corporativo se le ha asignado previamente.
2. Haga clic en **Obtener**.

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

Para instalar el certificado, consulte Configuración de un certificado de Privacy Manager en la página 61.

Configuración 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 luego haga clic en el botón **Configuración**, en el extremo inferior derecho del mensaje en Outlook 2007 o Outlook 2010, o en el extremo superior izquierdo en Outlook 2003.
2. Autentíquese utilizando su método de inicio de sesión de seguridad elegido.
3. En la página Certificado instalado, haga clic en **Siguiente**.
4. En la página Copia de seguridad del certificado, escriba una ubicación y un nombre para el archivo de la copia de seguridad o haga clic en **Buscar** 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 utilizando su método de inicio de sesión de seguridad elegido.
7. Si elige empezar el proceso de invitación de Contacto Confiable, siga las instrucciones que aparecen en pantalla a partir del paso 2 del tópico Adición de Contactos Confiables usando sus contactos de Microsoft Outlook en la página 66.

   – o –

   Si hace clic en **Cancelar**, consulte Administración de contactos confiables en la página 64 para obtener información sobre la adición de un Contacto Confiable posteriormente.

Importación de un certificado de terceros

Puede importar un certificado de terceros en Privacy Manager por medio del Asistente de importación para certificados.

Para utilizar este recurso, la configuración **Permitir el uso de certificados de terceros** de la Consola administrativa de HP ProtectTools debe estar activada en la página Configuración de **Privacy Manager**.

1. Abra Privacy Manager y luego haga clic en **Certificados**.
2. Seleccione la ficha **Administrador de certificados** y luego haga clic en **Importar certificados**.

   Este botón no se muestra si no se permite la importación de certificados.
3. Elija si desea importar un certificado ya instalado en este equipo o un certificado guardado como un archivo PFX (Personal Information Exchange/PKCS#12) y luego haga clic en **Siguiente**.

   - Para importar un certificado ya instalado en este equipo, seleccione el certificado deseado y luego haga clic en **Siguiente**.
   - Para seleccionar un certificado PFX, haga clic en **Explorar**, navegue a la ubicación del archivo PFX y luego haga clic en **Siguiente**. Escriba la contraseña del archivo PFX y luego haga clic en **Siguiente**.
4. Cuando el proceso de importación haya finalizado, haga clic en **Siguiente**.
5. Se le brinda la opción de realizar una copia de seguridad del certificado importado.

   Se recomienda que realice una copia de seguridad de su certificado en una ubicación que no sea la unidad de disco duro de su equipo.

Visualización de detalles de un certificado de Privacy Manager

1. Abra Privacy Manager y luego haga clic en **Certificados**.
2. Haga clic en un certificado de Privacy Manager.
3. Haga clic en **Detalles del 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 a la fecha de vencimiento, se le notificará cuando necesite renovarlo:

1. Abra Privacy Manager y luego haga clic en **Certificados**.
2. Haga clic en **Renovar certificado**.
3. Siga las instrucciones que aparecen en pantalla para obtener un nuevo certificado de Privacy Manager.

NOTA: El proceso de renovación del certificado de Privacy Manager no reemplaza su antiguo certificado de Privacy Manager. Debe obtener un nuevo certificado de Privacy Manager e instalarlo utilizando los mismos procedimientos que están en Solicitud de un certificado de Privacy Manager en la página 60.

Para los certificados corporativos emitidos por su compañía con Microsoft Certificate Authority, el administrador de CA debe renovar su certificado utilizando la misma clave privada que el certificado original o emitirle un nuevo certificado con la misma clave privada.

Configuración de un certificado de Privacy Manager predeterminado

Sólo los certificados de Privacy Manager son visibles desde Privacy Manager, incluso si se instalan en su equipo certificados adicionales de otras autoridades de certificación.

Si tiene más de un certificado de Privacy Manager en su equipo instalado desde Privacy Manager, puede especificar uno como certificado predeterminado:

1. Abra Privacy Manager y luego haga clic en **Certificados**.
2. Haga clic en el certificado de Privacy Manager que desee utilizar como predeterminado y luego haga clic en **Configuración predeterminada**.
3. Haga clic en **Aceptar**.

NOTA: No está obligado a utilizar su certificado de Privacy Manager predeterminado. Desde las distintas funciones de Privacy Manager, puede seleccionar cualquiera de sus certificados de Privacy Manager para utilizar.

Eliminación de un certificado de Privacy Manager

Si elimina un certificado de Privacy Manager, no puede abrir ningún archivo ni visualizar ningún dato que encriptó con dicho certificado. Si eliminó accidentalmente un certificado de Privacy Manager, puede restaurarlo con el archivo de copia de seguridad que creó cuando instaló el certificado. Consulte Restauración de un certificado de Privacy Manager en la página 63 para obtener más información.

Para eliminar un certificado de Privacy Manager:

1. Abra Privacy Manager y luego haga clic en **Certificados**.
2. Haga clic en el certificado de Privacy Manager que desee eliminar y luego haga clic en **Opciones avanzadas**.
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 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 luego haga clic en **Migración**.
2. Haga clic en **Restaurar**.
3. En la página Archivo de migración, haga clic en **Buscar** para buscar el archivo .dppsm que creó durante el proceso de realización de la 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**.

Consulte Configuración de un certificado de Privacy Manager en la página 61 o Copia de seguridad de certificados de Privacy Manager y Contactos Confiables en la página 74 para obtener más información.

Revocación de su certificado de Privacy Manager

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

NOTA: No se elimina un certificado de Privacy Manager revocado. El certificado aún puede utilizarse para visualizar archivos que están encriptados.

1. Abra Privacy Manager y luego haga clic en **Certificados**.
2. Haga clic en **Avanzadas**.
3. Haga clic en el certificado de Privacy Manager que desee revocar y luego haga clic en **Revocar**.
4. Cuando se abra el cuadro de diálogo de confirmación, haga clic en **Sí**.
5. Autentíquese utilizando su método de inicio de sesión de seguridad elegido.
6. Siga las instrucciones que aparecen en 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)

Adición de contactos confiables

La adición de contactos confiables es un proceso que consta de tres pasos:

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

Puede enviar invitaciones de Contacto confiable por correo electrónico 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: A fin de responder a su invitación para convertirse en un Contacto confiable, los destinatarios del Contacto confiable deben tener Privacy Manager instalado en sus equipos o tener el cliente alternativo instalado. Para obtener información sobre la instalación del cliente alternativo, acceda al sitio web de DigitalPersona en http://digitalpersona.com/privacymanager/download.

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 con Seguridad** 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. Ingrese las direcciones de correo electrónico de los destinatarios a los que desea 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 indicará que debe tener un certificado de Privacy Manager para poder enviar una solicitación de Contacto Confiable. Haga clic en **Aceptar** para iniciar el asistente de solicitación de certificado. Consulte Solicitud de un certificado de Privacy Manager en la página 60 para obtener más información.

7. Autentíquese utilizando su método de inicio de sesión de seguridad elegido.

NOTA: Cuando el destinatario del Contacto Confiable recibe el mensaje de correo electrónico, el destinatario debe abrir el correo electrónico, hacer clic en **Aceptar** en el extremo inferior derecho del correo electrónico y luego hacer clic en **OK** cuando se abre el cuadro del 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 que está al lado de **Enviar con Seguridad**, en la barra de herramientas, y luego haga clic en **Invitar a mis contactos de Outlook**.

2. Cuando se abra la página Invitación de Contactos Confiables, seleccione las direcciones de correo electrónico de los destinatarios que desee agregar como Contactos Confiables y luego haga clic en **Siguiente**.

3. Cuando se abra la página Enviando 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 indicará que debe tener un certificado de Privacy Manager para poder enviar una solicitación de Contacto Confiable. Haga clic en **Aceptar** para iniciar el asistente de solicitación de certificado. Consulte Solicitud de un certificado de Privacy Manager en la página 60 para obtener más información.

6. Autentíquese utilizando su método de inicio de sesión de seguridad elegido.

NOTA: Cuando el destinatario del Contacto Confiable recibe el mensaje de correo electrónico, el destinatario debe abrir el correo electrónico, hacer clic en **Aceptar** en el extremo inferior derecho del correo electrónico y luego hacer clic en **OK** cuando se abre 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 luego haga clic en **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 luego 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 luego 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 revocación**.
5. Haga clic en **Cerrar**.

Tareas generales

Puede usar Privacy Manager con los siguientes productos de Microsoft:

- Microsoft Outlook
- Microsoft Office

Uso de Privacy Manager en Microsoft Outlook

Cuando Privacy Manager está instalado, aparece un botón de Privacidad en la barra de herramientas de Microsoft Outlook y un botón Enviar con seguridad en la barra de herramientas de cada mensaje de correo electrónico de Microsoft Outlook. Cuando haga clic en la flecha hacia abajo que está al lado de **Privacidad** o **Enviar con seguridad**, puede elegir entre las siguientes opciones:

- **Firmar y enviar mensaje** (botón Enviar con seguridad únicamente): esta opción agrega una firma digital al correo electrónico y lo envía después de que usted se autentica con su método de inicio de inicio de seguridad seleccionado.
- **Sellar para Contactos confiables y enviar mensaje** (botón Enviar con seguridad únicamente): esta opción agrega una firma digital, encripta el correo electrónico y lo envía después de que usted se autentica con su método de inicio de inicio de seguridad seleccionado.
- **Invitar contactos**: esta opción le permite enviar una invitación de Contactos confiables. Consulte Adición de un contacto confiable en la página 65 para obtener más información.
- **Invitar contactos de Outlook**: esta opción le permite enviar una invitación de Contactos Confiables 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 66 para obtener más información.
- **Abrir el software Privacy Manager**: las opciones Certificados, Contactos Confiables y Configuración le permiten abrir el software Privacy Manager para agregar, ver o cambiar las configuraciones actuales. Para obtener más información, consulte Administración de certificados de Privacy Manager en la página 60, Administración de contactos confiables en la página 64 o Configuración de Privacy Manager para Microsoft Outlook en la página 68.

Configuración de Privacy Manager para Microsoft Outlook

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

   – o –

   En la barra de herramientas principal de Microsoft Outlook, haga clic en la flecha hacia abajo que está al lado de **Enviar con seguridad** (**Privacidad** en Outlook 2003) y luego haga clic en **Configuración**.

   – o –

   En la barra de herramientas de un mensaje de correo electrónico de Microsoft, haga clic en la flecha hacia abajo al lado de **Enviar con Seguridad** y luego haga clic en **Configuración**.

2. Seleccione las acciones que desee realizar cuando envía un correo electrónico seguro, y luego haga clic en **Aceptar**.

Firma y envío de un mensaje de correo electrónico

1. En Microsoft Outlook, haga clic en **Nuevo** o **Responder**.
2. Escriba su mensaje de correo electrónico.
3. Haga clic en la flecha hacia abajo al lado de **Enviar con Seguridad** (**Privacy** en Outlook 2003), y luego haga clic en **Firme y envíe mensaje**.
4. Autentíquese utilizando su método de inicio de sesión de seguridad elegido.

Selladura y envío de un mensaje de correo electrónico

Los mensajes de correo electrónico sellados que están firmados y sellados digitalmente (encriptados) pueden ser vistos únicamente por las personas que 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 **Responder**.
2. Escriba su mensaje de correo electrónico.
3. Haga clic en la flecha hacia abajo al lado de **Enviar con Seguridad** (**Privacy** en Outlook 2003), y luego haga clic en **Selle para Contactos Confiables y envíe mensaje**.
4. Autentíquese utilizando su método de inicio de sesión de seguridad elegido.

Visualización de un mensaje de correo electrónico sellado

Cuando abre un mensaje de correo electrónico sellado, se muestra la etiqueta de seguridad en el encabezado del correo electrónico. La etiqueta de seguridad proporciona la siguiente información:

- Qué credenciales se utilizaron para verificar la identidad de la persona que firmó 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

Después de instalar su certificado de Privacy Manager, aparece un botón Firme e Codifique a la derecha de la barra de herramientas de todos los documentos de Microsoft Word, Microsoft Excel y Microsoft PowerPoint. Cuando haga clic en la flecha abajo al lado de **Firme y Codifique**, puede elegir las siguientes opciones:

- **Firmar documento**: esta opción agrega su firma digital al documento.
- **Agregar línea de firma antes de firmar** (Microsoft Word y Microsoft Excel únicamente): de forma predeterminada, se agrega una línea de firma cuando se firma o encripta un documento de Microsoft Word o Microsoft Excel. Para desactivar esta opción, haga clic en **Agregar línea de firma** para quitar la marca de verificación.
- **Encriptar documento**: esta opción agrega su firma digital y encripta el documento.
- **Eliminar encriptación**: esta opción elimina la encriptación del documento.
- **Abrir el software Privacy Manager**: las opciones Certificados, Contactos Confiables y Configuración le permiten abrir el software Privacy Manager para agregar, ver o cambiar las

configuraciones actuales. Para obtener más información, consulte Administración de certificados de Privacy Manager en la página 60, Administración de contactos confiables en la página 64 o Configuración de Privacy Manager para Microsoft Office en la página 70.

Configuración de Privacy Manager para Microsoft Office

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

   – o –

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

2. Seleccione las acciones que desee configurar, y luego 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 hacia abajo al lado de **Firme y Codifique** y luego haga clic en **Firme documento**.
3. Autentíquese utilizando su método de inicio de sesión de seguridad elegido.
4. Cuando se abra el cuadro de diálogo de confirmación, lea el texto y luego haga clic en **Aceptar**.

Si luego 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 haga clic en **Marcar como final**.
3. Cuando se abra el cuadro de diálogo de confirmación, haga clic en **Sí** y continúe trabajando.
4. Cuando haya finalizado su edición, firme el documento de nuevo.

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

Privacy Manager le permite agregar una línea de firma cuando firma 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 hacia abajo al lado de **Firme y Codifique** y luego haga clic en **Agregar Línea de Firma antes de Firmar**.

   NOTA: Cuando se selecciona esta opción aparece una marca de verificación al lado de Agregar Línea de Firma Antes de Firmar. Esta opción se activa en forma predeterminada.

4. Haga clic en la flecha hacia abajo al lado de **Firme e Codifique** y luego haga clic en **Firme documento**.
5. Autentíquese utilizando su método de inicio de sesión de seguridad elegido.

Adición de firmantes sugeridos a un documento de Microsoft Word o Microsoft Excel

Puede agregar más de una línea de firma a su documento designando firmantes sugeridos. Un firmante sugerido es un usuario designado por el propietario de un documento de Microsoft Word o Microsoft Excel para agregar línea de firma al documento. Los firmantes sugeridos pueden ser usted u otra persona que desee firmar su documento. Por ejemplo, si prepara un documento que necesita ser firmado por todos los miembros de su departamento, puede incluir líneas de firma para dichos usuarios en la parte inferior de la página final del documento, con instrucciones para firmar 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 hacia abajo al lado de **Línea de firma** y luego haga clic en **Privacy Manager Signature Provider**.

   Se abrirá el cuadro de diálogo de configuración de firma.
4. En el cuadro debajo de **Signatario sugerido**, escriba el nombre del firmante sugerido.
5. En el cuadro debajo de **Instrucciones para el signatario**, escriba un mensaje para este firmante sugerido.

   NOTA: Este mensaje aparecerá en lugar de un título y es eliminado o reemplazado por el título 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 título.

   NOTA: El propietario del documento asigna firmantes sugeridos a su documento. Deben seleccionarse las casillas de verificación **Mostrar fecha de firma en la línea de firma** y/o **Mostrar cargo del firmante en la línea de firma** a fin de que el firmante sugerido pueda mostrar la fecha y/o cargo en la línea de firma.
8. Haga clic en **Aceptar**.

Adición de una línea de firma del firmante sugerido

Cuando los firmantes sugeridos abran 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 correspondiente.
2. Autentíquese utilizando su método de inicio de sesión de seguridad elegido.

   La línea de firma se mostrará 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 para sus Contactos confiables. Cuando encripta un documento y lo cierra, usted y el (los) Contacto(s) confiable(s) que seleccione en la lista deben 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 que está al lado de **Firmar y encriptar** y luego haga clic en **Encriptar documento**.

   Aparece el cuadro de diálogo de contactos confiables seleccionados.
4. Haga clic en el nombre de un contacto confiable que podrá abrir el documento y visualizar su contenido.

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

5. Haga clic en **Aceptar**.

Si decide más adelante editar el documento, siga los pasos de Eliminación de la encriptación de un documento de Microsoft Office en la página 72. Cuando se elimina la encriptación, usted puede 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 elimine la codificación de un documento de Microsoft Office, usted y sus contactos confiables ya no estarán obligados a autenticarse para abrir y visualizar el contenido del documento.

Para eliminar la codificación de un documento de Microsoft Office:

1. Abra un documento encriptado de Microsoft Word, Microsoft Excel o Microsoft PowerPoint.
2. Autentíquese utilizando su método de inicio de sesión de seguridad elegido.
3. Haga clic en el menú **Inicio**.
4. Haga clic en la flecha hacia abajo que está al lado de **Firmar y encriptar** y luego haga clic en **Eliminar encriptación**.

Envío de un documento de Microsoft Office encriptado

Puede adjuntar un documento de Microsoft Office encriptado a un mensaje de correo electrónico sin firmar ni encriptar el correo electrónico mismo. Para hacerlo, cree y envíe un correo electrónico con un documento firmado o encriptado, como lo haría para un correo electrónico normal con un documento adjunto.

Sin embargo, para obtener una seguridad óptima, se recomienda encriptar el mensaje de correo electrónico cuando adjunte un documento firmado o encriptado de Microsoft Office.

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

1. En Microsoft Outlook, haga clic en **Nuevo** o **Responder**.
2. Escriba su mensaje de correo electrónico.
3. Adjunte un documento de Microsoft Office.
4. Consulte Selladura y envío de un mensaje de correo electrónico en la página 69 para obtener otras instrucciones.

Visualización de un documento de Microsoft Office firmado

NOTA: No necesita tener un certificado de Privacy Manager para poder visualizar un documento firmado de Microsoft Office.

Cuando un documento firmado de Microsoft Office se abre, aparece un icono de Firmas digitales en la barra de estado, en la parte inferior de la ventana del documento.

1. Haga clic en el icono **Firmas digitales** para exhibir el cuadro de diálogo de las Firmas, que muestra el nombre de todos los usuarios que firmaron el documento y la fecha en que cada uno lo hizo.
2. Para ver detalles adicionales sobre cada firma, haga clic con el botón derecho del mouse en un nombre del cuadro de diálogo de las Firmas y luego seleccione **Detalles de la firma**.

Visualización de un documento de Microsoft Office encriptado

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

Si se ha perdido su certificado, debe restaurar el certificado de Privacy Manager que se utilizó para encriptar el archivo a fin de visualizar un documento de Microsoft Office encriptado.

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.

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 seguridad 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 luego haga clic en **Migración**.
2. Haga clic en **Crear copia de seguridad**.
3. En la página Seleccionar datos, seleccione las categorías de datos que se incluirán en el archivo de migración y luego haga clic en **Siguiente**.
4. En la página Archivo de migración, escriba un nombre de archivo o haga clic en **Explorar** para buscar una ubicación y luego 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 utilizando su método de inicio de sesión de seguridad 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 luego 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 luego 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, 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 pueden estar activados o desactivados:

- **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 o Microsoft Outlook.

7 File Sanitizer for HP ProtectTools

File Sanitizer le permite triturar archivos con seguridad (por ejemplo, información o archivos personales, datos de historial, datos relacionados con la Web u otros componentes de datos) en su equipo y purificar los activos eliminados en su unidad de disco duro periódicamente.

NOTA: Esta versión de File Sanitizer es compatible únicamente con la unidad de disco duro del equipo.

Eliminación definitiva

La trituración es diferente de una eliminación de Windows® estándar (también conocida como eliminación simple en File Sanitizer). Cuando tritura un activo con File Sanitizer, los archivos se sobrescriben con datos insignificantes, lo que hace 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 en el que podrían utilizarse métodos forenses para recuperarlo.

Al optar por la eliminación total de un archivo (**Seguridad alta**, **Seguridad media** o **Seguridad baja**), se seleccionan automáticamente una lista predefinida de activos y un método de eliminación para efectuar el procedimiento. También puede personalizar un perfil de eliminación total al especificar el número de ciclos de eliminación, qué activos se incluirán en la eliminación total, qué activos deben confirmarse antes de ejecutar el procedimiento y qué activos deben excluirse de la eliminación total. Para obtener más información, consulte Selección o creación de un perfil de trituración en la página 80.

Puede configurar una trituración automática o también puede activar el procedimiento de trituración manualmente usando el icono de **HP ProtectTools** en el área de notificación, en el extremo derecho de la barra de tareas. Para obtener más información, consulte Configuración de una programación de trituración en la página 79, Trituración manual de un activo en la página 84 o Trituración manual de todos los elementos seleccionados en la página 85.

NOTA: Un archivo .dll se tritura y elimina del sistema sólo si ha sido movido 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 puede realizarse ocasionalmente para los activos que usted elimina cuando selecciona **Configuración de eliminación simple** en File Sanitizer, cuando mueve los activos a la papelera de reciclaje de Windows o cuando elimina los archivos manualmente. La purificación de espacio libre no ofrece seguridad adicional para los activos triturados.

Puede configurar una limpieza automática para liberar espacio o también puede activar el procedimiento manualmente usando el icono de **HP ProtectTools** en el área de notificación, en el extremo derecho de la barra de tareas. Para obtener más información, consulte Configuración de una programación de purificación de espacio libre en la página 79 o Activación manual de purificación de espacio libre en la página 85.

Apertura de File Sanitizer

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

– o –

- Haga doble clic en el icono de **File Sanitizer** de su escritorio.

– o –

- Haga clic con el botón derecho del mouse en el icono de **HP ProtectTools** del 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**.

Procedimientos de configuración

Configuración de una programación de trituración

Puede seleccionar un perfil de trituración predefinido o crear un perfil de trituración. Para obtener más información, consulte Selección o creación de un perfil de trituración en la página 80. También puede triturar activos manualmente en cualquier momento. Para obtener más información, consulte Uso de una secuencia de teclas para iniciar la trituración en la página 83.

NOTA: Una tarea programada comienza a una hora específica. Si el sistema está apagado o se encuentra en suspensión o modo de espera a la hora programada, File Sanitizer no intentará reiniciar la tarea.

1. Abra File Sanitizer y luego haga clic en **Triturar**.
2. Seleccione una o más opciones de trituración:
   - **Apagado de Windows**: tritura todos los activos seleccionados cuando se cierra Windows.

     NOTA: Se abre un cuadro de diálogo al cerrar que le pregunta si desea continuar con la trituración de los activos seleccionados o si desea omitir el procedimiento.

     Haga clic en **Sí** para omitir el procedimiento de trituración o en **No** para continuar con la trituración.
   - **Abrir navegador web**: tritura todos los archivos seleccionados relacionados con Internet, como el historial de sitios visitados, cuando abre un navegador web.
   - **Salir del navegador web**: tritura todos los activos seleccionados relacionados con la Web, como el historial de sitios visitados, cuando cierra un navegador web.
   - **Secuencia de teclas**: le permite especificar una secuencia de teclas para iniciar la trituración. Para obtener detalles, consulte Uso de una secuencia de teclas para iniciar la trituración en la página 83.

   NOTA: Un archivo .dll se tritura y elimina del sistema sólo si ha sido movido a la papelera de reciclaje.
3. A fin de programar un horario futuro para triturar los activos seleccionados, marque la casilla de verificación **Activar Programador**, ingrese su contraseña de Windows y, a continuación, seleccione un día y un horario.
4. Haga clic en **Aplicar**.

Configuración de una programación de purificación de espacio libre

La purificación de espacio libre puede realizarse ocasionalmente para los activos que usted elimina cuando selecciona **Configuración de eliminación simple** en File Sanitizer, cuando mueve los activos a la Papelera de reciclaje de Windows o cuando elimina los archivos manualmente. La purificación de espacio libre no ofrece seguridad adicional para los activos triturados.

NOTA: Una tarea programada comienza a una hora específica. Si el sistema se apaga o se encuentra en suspensión o modo de espera a la hora programada, File Sanitizer no intentará reiniciar la tarea.

1. Abra File Sanitizer y luego haga clic en **Purificación**.
2. A fin de programar un horario futuro para purificar los activos eliminados en su unidad de disco duro, marque la casilla de verificación **Activar Programador**, introduzca su contraseña de Windows y a continuación seleccione un día y un horario.
3. Haga clic en **Aplicar**.

NOTA: La operación de purificación de espacio libre puede llevar un plazo de tiempo considerable. Si bien la purificación de espacio libre se realiza en segundo plano, un mayor uso del procesador puede afectar el rendimiento de su equipo.

Selección o creación de un perfil de trituración

Puede especificar un método de eliminación y seleccionar los activos que se triturarán eligiendo un perfil predefinido o creando su propio perfil.

Selección de un perfil de trituración predefinido

Al optar por un perfil de trituración predefinido, se seleccionan automáticamente un método de eliminación y una lista de activos predefinidos. También puede visualizar la lista predefinida de activos que se seleccionan para la trituración.

1. Abra File Sanitizer y luego haga clic en **Configuración**.
2. Haga clic en un perfil de trituración predefinido:
   - **Seguridad máxima**
   - **Seguridad media**
   - **Seguridad baja**
3. Para visualizar los activos seleccionados para trituración, haga clic en **Ver detalles**.
   a. **Se triturarán los elementos seleccionados y se mostrará un mensaje de confirmación. Los elementos no seleccionados se triturarán sin un mensaje de confirmación.** Seleccione la casilla de verificación para mostrar un mensaje de confirmación antes de triturar el elemento o desmarque la casilla de verificación para triturar el elemento sin mostrar un mensaje de confirmación.

   NOTA: Incluso si la casilla de verificación de un activo no está seleccionada, este se triturará.

   b. Haga clic en **Aplicar**.
4. Haga clic en **Aplicar**.

Personalización de un perfil de trituración

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 File Sanitizer, haga clic en **Configuración**, en **Configuración avanzada de seguridad** y, a continuación, en **Ver detalles**.
2. Seleccione la cantidad de ciclos de trituración.

NOTA: Se realizará la cantidad seleccionada de ciclos de trituración para cada activo. Por ejemplo, si elige 3 ciclos de trituración, se ejecuta un algoritmo que oculta los datos 3 veces por separado. Si elige los ciclos de trituración de seguridad más alta, la trituración puede llevar un plazo de tiempo considerable; sin embargo, cuanto mayor sea la cantidad de ciclos de trituración que especifique, menos probable es que puedan recuperarse los datos.

3. Para seleccionar los activos que se triturarán:
   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 nombre del archivo.
   c. Haga clic en **Abrir** y, a continuación, haga clic en **Aceptar**.
   d. En **Opciones de trituración disponibles**, haga clic en un activo personalizado y luego haga clic en **Agregar**.

   Para quitar un activo de las opciones de trituración disponibles, haga clic en el activo y entonces haga clic en **Eliminar**.
4. **Se triturarán los elementos seleccionados y se mostrará un mensaje de confirmación. Los elementos no seleccionados se triturarán sin un mensaje de confirmación.** Seleccione la casilla de verificación para mostrar un mensaje de confirmación antes de triturar el elemento o desmarque la casilla de verificación para triturar el elemento sin mostrar un mensaje de confirmación.

NOTA: Incluso si la casilla de verificación de un activo no está seleccionada, este se triturará.

   Para quitar un activo de la lista de trituración, haga clic en el activo y, a continuación, haga clic en **Eliminar**.
5. Para proteger los archivos o carpetas de la trituración automática:
   a. En **No triturar lo siguiente**, haga clic en **Agregar** y luego navegue o escriba la ruta a la carpeta o al archivo.
   b. Haga clic en **Abrir** y, a continuación, haga clic en **Aceptar**.

   Para quitar un activo de la lista de exclusiones, haga clic en el activo y, a continuación, haga clic en **Eliminar**.
6. Haga clic en **Aplicar**.

Personalización de un perfil de eliminación simple

El perfil de eliminación simple realiza una eliminación de activos estándar sin trituración. Puede personalizar un perfil de eliminación simple al especificar qué activos se incluirán, qué activos deben confirmarse antes de la eliminación y qué activos deben excluirse.

NOTA: Si selecciona **Configuraciones de eliminación simple**, la purificación de espacio libre puede realizarse ocasionalmente en los activos que se han eliminado manualmente o por medio de la papelera de reciclaje de Windows.

1. Abra File Sanitizer, haga clic en **Configuración**, en **Configuraciones de eliminación simple** y luego en **Ver detalles**.
2. Seleccione los activos que desea eliminar:
   a. En **Opciones de eliminación disponibles**, haga clic en un activo, y luego haga clic en **Agregar**.
   b. Para agregar un activo personalizado, haga clic en **Agregar opción personalizada**, navegue o escriba la ruta a la carpeta o al archivo y luego haga clic en **Aceptar**.
   c. Haga clic en el perfil personalizado y luego haga clic en **Agregar**.

   Para eliminar un activo de las opciones de eliminación disponibles, haga clic en el activo y entonces haga clic en **Eliminar**.
3. **Se triturarán los elementos seleccionados y se mostrará un mensaje de confirmación. Los elementos no seleccionados se triturarán sin un mensaje de confirmación.** Seleccione la casilla de verificación para mostrar un mensaje de confirmación antes de triturar el elemento o desmarque la casilla de verificación para triturar el elemento sin mostrar un mensaje de confirmación.

   NOTA: Incluso si la casilla de verificación de un activo no está seleccionada, este se triturará.

   Para quitar un activo de la lista de eliminación, haga clic en el activo y luego haga clic en **Eliminar**.
4. Para proteger activos de la eliminación automática:
   a. En **No eliminar lo siguiente**, haga clic en **Agregar** y luego navegue o escriba la ruta a la carpeta o al archivo.
   b. Haga clic en **Abrir** y, a continuación, haga clic en **Aceptar**.

   Para quitar un activo de la lista de exclusiones, haga clic en el activo y, a continuación, haga clic en **Eliminar**.
5. Haga clic en **Aplicar**.

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 83.
- 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 84.
- 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 Trituración manual de un activo en la página 84 o Trituración manual de todos los elementos seleccionados en la página 85.
- 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 purificación de espacio libre en la página 85.
- 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 Detención de una operación de trituración o purificación de espacio libre en la página 85.
- 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 85.

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

1. Abra File Sanitizer y luego haga clic en **Triturar**.
2. Seleccione la casilla de verificación **Secuencia de teclas**.
3. Escriba un carácter en el cuadro disponible.
4. Seleccione el cuadro **CTRL** o el cuadro **ALT**, y luego seleccione el cuadro **MAYÚS**.

   Por ejemplo, para iniciar la eliminación automática con la tecla s y ctrl+mayús, escriba s en el cuadro y a continuación seleccione las opciones **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 al icono de **File Sanitizer** en el escritorio.
3. Cuando se abra el cuadro de diálogo de confirmación, haga clic en **Sí**.

Trituración 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 único.

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 File Sanitizer y luego 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**.

Trituración 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 File Sanitizer y luego 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 purificación de espacio libre

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 File Sanitizer y luego 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**.

Detención de una operación de trituración o purificación de espacio libre

Cuando una operación de trituración o purificación de espacio libre está en progreso, aparece un mensaje sobre el icono de HP ProtectTools Security Manager en el área de notificación, en el extremo derecho de la barra de tareas. El mensaje proporciona detalles sobre el proceso de trituración o purificación de espacio libre (porcentaje completado) y le brinda la opción de detener la operación.

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

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 archivo de registro para las operaciones de purificación de espacio libre. Ambos archivos de registro se encuentran en la unidad de disco duro:

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

Para los sistemas de 64 bits, los archivos de registro se encuentran en la unidad de disco duro:

- C:\Program Files (x86)\Hewlett-Packard\File Sanitizer*[Username]*_ShredderLog.txt
- C:\Program Files (x86)\Hewlett-Packard\File Sanitizer*[Username]*_DiskBleachLog.txt

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

HP ProtectTools Device Access Manager controla el acceso a los datos al desactivar los dispositivos de transferencia de datos.

NOTA: Device Access Manager no controla algunos dispositivos de entrada/interfaz humana, como el mouse, el teclado, el TouchPad y el lector de huellas digitales. Para obtener más información, consulte Clases de dispositivos no administrados en la página 98.

Los administradores del sistema operativo Windows® usan HP ProtectTools Device Access Manager para controlar el acceso a los dispositivos de un sistema y para protegerlos del acceso no autorizado:

- Los perfiles de dispositivo se crean para cada usuario con el fin de definir los dispositivos a los que se les permite o se les niega la autorización de acceso.
- La autenticación Just In Time (JITA) permite que usuarios predefinidos se autentiquen con el fin de acceder a los dispositivos que de otro modo están denegados.
- Es posible excluir los administradores y los usuarios de confianza de las restricciones de acceso al dispositivo impuestas por Device Access Manager al agregarlos al grupo Administradores de dispositivos. Esta pertenencia al grupo se administra con la Configuración avanzada.
- El acceso al dispositivo se puede otorgar o denegar a partir de la pertenencia a un grupo o para usuarios individuales.
- En el caso de clases de dispositivos como las unidades de CD-ROM y de DVD, se puede permitir o denegar el acceso para lectura y escritura por separado.

Apertura de Device Access Manager

1. Inicie sesión como administrador.
2. Haga clic en **Inicio**, en **Todos los programas**, en **HP** y después en **Consola administrativa de HP ProtectTools**.
3. En el panel izquierdo, haga clic en **Device Access Manager**.

Los usuarios pueden ver la política de HP ProtectTools Device Access Manager utilizando HP ProtectTools Security Manager. Esta consola proporciona una vista de sólo lectura.

Procedimientos de configuración

Configuración del acceso a los dispositivos

HP ProtectTools Device Access Manager ofrece cuatro vistas:

- **Configuración sencilla**: permite o niega el acceso a clases de dispositivos, según la pertenencia al grupo Administradores de dispositivos.
- **Configuración de clases de dispositivo**: permite o niega el acceso a tipos de dispositivos o dispositivos específicos para grupos o usuarios específicos.
- **Configuración JITA**: configura la autenticación Just In Time (JITA), permitiendo que algunos usuarios accedan a las unidades de DVD/CD-ROM o medios extraíbles autenticándose por sí mismos.
- **Configuración avanzada**: configura una lista de las letras de unidades para las cuales Device Access Manager no restringirá el acceso, como la unidad C o del sistema. La pertenencia al grupo Administradores de dispositivos también puede administrarse desde esta vista.

Configuración sencilla

Los administradores pueden usar la vista **Configuración sencilla** para permitirles o denegarles el acceso a las siguientes clases de dispositivos a todos los que no sean administradores de dispositivos:

- 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 módems
- Todos los dispositivos PCMCIA/ExpressCard
- Todos los dispositivos 1394

Para permitirles o denegarles el acceso a una clase de dispositivos a todos los 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 derecho, para negar el acceso, seleccione la casilla de verificación de una clase de dispositivo o un dispositivo específico. Desmarque la casilla de verificación para permitir el acceso a esa clase de dispositivo o dispositivo específico.

   Si la casilla de verificación está de color gris, los valores que afectan el escenario de acceso se alteraron desde dentro de la vista **Configuración de clases de dispositivo**. Para restaurar la configuración de fábrica, haga clic en **Restablecer** en la vista **Configuración de la clase de dispositivo**.
3. Haga clic en **Aplicar**.

NOTA: Si no se está ejecutando el servicio en segundo plano, se abre una caja de diálogo para preguntar si le gustaría iniciarlo. Haga clic en **Sí**.

4. Haga clic en **Aceptar**.

Inicio del servicio en segundo plano

La primera vez que se defina y aplique una nueva política, el servicio en segundo plano Bloqueo/auditoría de dispositivo de HP ProtectTools comenzará automáticamente y se configurará para comenzar automáticamente cada vez que se inicie el sistema.

NOTA: Se debe definir un perfil del dispositivo antes de que aparezca el aviso del servicio en segundo plano.

Los administradores también pueden iniciar o detener este servicio:

1. En Windows 7, haga clic en **Inicio**, en **Panel de control** y luego en **Sistema y seguridad**.

   o

   En Windows Vista®, haga clic en **Inicio**, en **Panel de control** y luego en **Sistema y mantenimiento**.

   o

   En Windows XP, haga clic en **Inicio**, en **Panel de control** y luego en **Rendimiento y mantenimiento**.

2. Haga clic en **Herramientas administrativas** y luego en **Servicios**.
3. Seleccione el servicio **Bloqueo/auditoría de dispositivo de HP ProtectTools**.
4. Para iniciar el servicio, haga clic en **Inicio**.

   o

   Para detener el servicio si se está ejecutando, haga clic en **Detener**.

Si detiene el servicio Bloqueo/auditoría de dispositivo, no se detendrá el bloqueo del dispositivo. Hay dos componentes que exigen el bloqueo del dispositivo:

- El servicio Bloqueo de dispositivos/auditoría
- El controlador DAMDrv.sys

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

Para determinar si el servicio en segundo plano se está ejecutando, abra una ventana de solicitud de comando y luego escriba `sc query flcdlock`.

Para determinar si el controlador del dispositivo se está ejecutando, abra una ventana de solicitud de comando y luego escriba `sc query damdrv`.

Configuración de clases de dispositivo

Los Administradores pueden ver y modificar las listas de usuarios y grupos a los que se les permite o niega la autorización para acceder a clases de dispositivos o dispositivos específicos.

La vista **Configuración de 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 haberse instalado en el sistema antes.
  - La protección se aplica generalmente a una clase de dispositivo. Un usuario o grupo seleccionado será capaz de acceder a cualquier dispositivo que corresponda a esa clase de dispositivo.
  - La protección también se puede aplicar a dispositivos específicos.
- **Lista de usuarios**: muestra a todos los usuarios y grupos a los que se les ha permitido o negado el acceso a la clase de dispositivo o al dispositivo específico seleccionado.
  - La entrada en la Lista de usuario puede hacerse para un usuario específico o para un grupo al que pertenezca el usuario.
  - Si la entrada de un usuario o grupo de la Lista de usuarios no está disponible, la configuración ha sido heredada de la clase de dispositivo de la Lista de dispositivos o de la carpeta Clases.
  - Algunas clases de dispositivo, como el DVD y el CD-ROM, pueden controlarse aún más al permitir o denegar el acceso por separado para las operaciones de lectura y de escritura.

    En el caso de los otros dispositivos y clases, los derechos de acceso para lectura y escritura pueden heredarse. Por ejemplo, el acceso de lectura puede heredarse de una clase más alta, pero el acceso de escritura puede denegársele específicamente a un usuario o grupo.

    NOTA: Si la casilla de verificación de **Lectura** está en blanco, la entrada de control de acceso no tiene efecto en el acceso de lectura al dispositivo, pero el acceso de lectura no está negado.

    NOTA: El grupo Administradores no puede agregarse a la Lista de usuarios. En vez de ello, utilice el grupo Administradores de dispositivos.

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

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

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

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

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

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

    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 otorgar el acceso o el acceso de lectura+escritura apenas para un dispositivo que esté debajo de este dispositivo en la jerarquía de los dispositivos.

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

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

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

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

Negación del acceso a un usuario o grupo

Para evitar que un usuario o un grupo acceda a un dispositivo o a una clase de dispositivos:

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 dispositivo**
   - **Todos los dispositivos**
   - **Dispositivo individual**
3. En **Usuario/Grupos**, haga clic en el usuario o el grupo al que se le va a denegar el acceso y luego haga clic en **Denegar**.
4. Haga clic en **Aplicar**.

NOTA: Cuando las configuraciones para denegar o permitir estén definidas en el mismo nivel del dispositivo para un usuario, la negación del acceso prevalecerá sobre la autorización del mismo.

Autorización del acceso a un usuario o un grupo

Para otorgarle la autorización a un usuario o a un grupo para que acceda a un dispositivo o a una clase de dispositivos:

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 uno de los siguientes:
   - **Clase de dispositivo**
   - **Todos los dispositivos**
   - **Dispositivo individual**
3. Haga clic en **Agregar**.

   Se abrirá el cuadro de diálogo Seleccionar usuarios o grupos.

4. Haga clic en **Avanzado** y luego en **Encontrar ahora** para buscar los usuarios o grupos que va a agregar.
5. Haga clic en el usuario o en el grupo que se va a agregar a la lista de usuarios y grupos disponibles y luego haga clic en **Aceptar**.
6. Haga clic en **Aceptar** de nuevo.
7. Haga clic en **Permitir** para otorgarle a este usuario el acceso.
8. Haga clic en **Aplicar**.

Autorización del acceso a una clase de dispositivos para un usuario o un grupo

Para permitirle a un usuario acceder a una clase de dispositivos y a la vez denegarle el acceso a todos los otros miembros del grupo de ese usuario:

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 dispositivo**
   - **Todos los dispositivos**
   - **Dispositivo individual**
3. En **Usuario/Grupos**, seleccione el grupo al que se le va a denegar el acceso y entonces haga clic en **Denegar**.
4. Navegue a la carpeta que está debajo de la de la clase requerida y agregue al usuario específico.
5. Haga clic en **Permitir** para otorgarle a este usuario el acceso.
6. Haga clic en **Aplicar**.

Autorización del acceso a un dispositivo específico para un usuario o un grupo

Los Administradores pueden permitir el acceso a un dispositivo específico y a la vez denegarles el acceso a todos los otros miembros del grupo de ese usuario para todos 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 dispositivo que desea configurar y luego navegue a la carpeta que aparece debajo.
3. En **Usuario/Grupos**, haga clic en **Permitir** al lado del grupo al que se le va a otorgar el acceso.
4. Haga clic en **Denegar** al lado del grupo al que se le va a negar el acceso.
5. Navegue al dispositivo específico al que se va a autorizar el acceso al usuario en la lista de dispositivos.
6. Haga clic en **Agregar**.

   Se abrirá el cuadro de diálogo Seleccionar usuarios o grupos.

7. Haga clic en **Avanzado** y luego en **Encontrar ahora** para buscar los usuarios o grupos que va a agregar.
8. Haga clic en el usuario al que se le va a permitir el acceso y luego haga clic en **Aceptar**.
9. Haga clic en **Permitir** para otorgarle a este usuario el acceso.
10. Haga clic en **Aplicar**.

Eliminación de la configuración de un usuario o un grupo

A fin de eliminar la autorización a un usuario o a un grupo para acceder a un dispositivo o a una 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 dispositivo**
   - **Todos los dispositivos**
   - **Dispositivo individual**
3. En **Usuario/Grupos**, haga clic en el usuario o grupo que desea eliminar y luego haga clic en **Eliminar**.
4. Haga clic en **Aplicar**.

Restauración de la configuración

⚠ **PRECAUCIÓN:** La restauración de la configuración descarta todos los cambios que se le hayan hecho a la configuración del dispositivo y la devuelve a los valores predefinidos de fábrica.

Para restaurar la configuración a los valores de fábrica:

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 **Restablecer**.
3. Haga clic en **Sí** en la solicitud de confirmación.
4. Haga clic en **Aplicar**.

Configuración JITA

La Configuración JITA permite que el administrador vea y modifique las listas de usuarios y grupos a los que se les permite acceder a los dispositivos utilizando la autenticación Just-in-time (JITA).

Los usuarios activados con JITA podrán acceder a algunos dispositivos para los cuales se han restringido las políticas creadas en la vista **Configuración de clases de dispositivo** o **Configuración sencilla**.

- **Escenario**: se configura una política de Configuración sencilla para denegarles el acceso a la unidad de DVD/CD-ROM a todos los que no sean administradores de dispositivos.
- **Resultado**: un usuario activado con JITA que intente acceder a la unidad de DVD/CD-ROM recibe el mismo mensaje de “acceso denegado” que un usuario que no tiene JITA activada.

Luego aparece un mensaje en un globo que pregunta si el usuario desea obtener acceso a JITA. Si se hace clic en el globo, se abre el cuadro de diálogo Autenticar usuario. Cuando el usuario introduce correctamente las credenciales, se otorga acceso a la unidad de DVD/CD-ROM.

El período de JITA puede autorizarse para una cantidad establecida de minutos o 0 minutos. Un período de JITA de 0 minutos no caducará. Los usuarios tendrán acceso al dispositivo desde el momento en que se autentiquen hasta el momento en que apaguen el sistema.

El período de JITA también puede extenderse, si está configurado para hacerlo. En este escenario, 1 minuto antes de que el período de JITA esté a punto de expirar, los usuarios pueden hacer clic en el mensaje para ampliar su acceso sin tener que volver a autenticarse.

Si se otorga al usuario un período de JITA limitado o ilimitado, tan pronto como el usuario apague el sistema u otro usuario inicie sesión, el período de JITA expirará. La próxima vez que el usuario inicie sesión e intente acceder a un dispositivo activado con JITA, aparecerá un mensaje para introducir las credenciales.

JITA se encuentra disponible para las siguientes clases de dispositivos:

- Unidades de DVD/CD-ROM
- Medios extraíbles

Creación de una JITA para un usuario o un grupo

Los Administradores pueden permitir que los usuarios o grupos accedan a los dispositivos utilizando la autenticación Just-in-time.

1. En el panel izquierdo de la Consola administrativa de HP ProtectTools, haga clic en **Device Access Manager** y luego en **Configuración de JITA**.
2. En el menú desplegable del dispositivo, seleccione **Medios extraíbles** o **Unidades de DVD/CD-ROM**.
3. Haga clic en **+** para agregar a un usuario o grupo a la configuración JITA.
4. Seleccione la casilla de verificación **Activado**.
5. Fije el período de JITA en el tiempo necesario.
6. Haga clic en **Aplicar**.

El usuario debe salir y luego volver a iniciar sesión para que se aplique la nueva configuración JITA.

Creación de una JITA extensible a un usuario o un grupo

Los Administradores pueden permitir que un usuario o grupo acceda a dispositivos utilizando la autenticación Just-in-time que el usuario puede extender antes de que expire.

1. En el panel izquierdo de la Consola administrativa de HP ProtectTools, haga clic en **Device Access Manager** y luego en **Configuración de JITA**.
2. En el menú desplegable del dispositivo, seleccione **Medios extraíbles** o **Unidades de DVD/CD-ROM**.
3. Haga clic en **+** para agregar a un usuario o grupo a la configuración JITA.
4. Seleccione la casilla de verificación **Activado**.

5. Fije el período de JITA en el tiempo necesario.
6. Seleccione la casilla de verificación **Extensible**.
7. Haga clic en **Aplicar**.

El usuario debe salir y luego volver a iniciar sesión para que se aplique la nueva configuración JITA.

Desactivación de una JITA para un usuario o un grupo

Los Administradores pueden desactivar el acceso de un usuario o grupo a los dispositivos utilizando la autenticación Just-in-time.

1. En el panel izquierdo de la Consola administrativa de HP ProtectTools, haga clic en **Device Access Manager** y luego en **Configuración de JITA**.
2. En el menú desplegable del dispositivo, seleccione **Medios extraíbles** o **Unidades de DVD/CD-ROM**.
3. Seleccione el usuario o grupo cuya JITA desea desactivar.
4. Desmarque la casilla de verificación **Activado**.
5. Haga clic en **Aplicar**.

Cuando el usuario inicia sesión e intenta acceder al dispositivo, se niega el acceso.

Configuración avanzada

La Configuración avanzada ofrece las siguientes funciones:

- Gestión del grupo Administradores de dispositivos
- Administración de las letras de la unidad a las que Device Access Manager nunca niega el acceso.

El grupo Administradores de dispositivos se utiliza para excluir a los usuarios de confianza (en términos de acceso al dispositivo) de las restricciones impuestas por una política de Device Access Manager. Los usuarios de confianza generalmente incluyen a los administradores del sistema. Consulte Grupo Administradores de dispositivos en la página 97 para obtener más información.

La vista de **Configuración avanzada** también permite que el administrador configure una lista de las letras de unidades para las cuales Device Access Manager no restringirá el acceso a ningún usuario.

NOTA: Los servicios en segundo plano de Device Access Manager deben estar ejecutándose cuando se configure la lista de las letras de las unidades.

Para iniciar estos servicios:

1. Aplique una política de Configuración sencilla, como denegar el acceso a los medios extraíbles a todos los que no sean administradores de dispositivos.

   o

   Abra una ventana de solicitud de mensaje con privilegios de Administrador y luego escriba:

   ```
   sc start flcdlock
   ```

   Presione intro.

2. Cuando se inician los servicios, puede editarse la lista de las unidades. Introduzca las letras de la unidad de los dispositivos que no desee que controle Device Access Manager.

   Las letras de la unidad se muestran para las unidades de disco duro o particiones.

NOTA: Ya sea que la unidad del sistema (por lo general C) esté o no en esta lista, el acceso a esta nunca se le denegará a ningún usuario.

Grupo Administradores de dispositivos

Cuando Device Access Manager está instalado, se crea un grupo Administradores de dispositivos.

El grupo Administradores de dispositivos se utiliza para excluir a los usuarios de confianza (en términos de acceso al dispositivo) de las restricciones impuestas por una política de Device Access Manager. Los usuarios de confianza generalmente incluyen a los administradores del sistema.

NOTA: El hecho de agregar a un usuario al grupo Administradores de dispositivos no le permite automáticamente al usuario acceder a los dispositivos. En la vista **Configuración de clases de dispositivo**, si el grupo Usuarios no tiene acceso a un dispositivo, debe otorgarse acceso al grupo Administradores de dispositivos con el fin de que los miembros del grupo tengan acceso al dispositivo. Sin embargo, la vista **Configuración sencilla** puede utilizarse para denegar el acceso a las clases de dispositivos para todos los usuarios que no sean miembros del grupo Administradores de dispositivos.

Para agregar usuarios al grupo Administradores de dispositivos:

1. En la vista **Configuración avanzada**, haga clic en **+**.
2. Escriba el nombre del usuario de confianza.
3. Haga clic en **Aceptar**.
4. Haga clic en **Aplicar**.

Los métodos alternativos para administrar la pertenencia a este grupo incluyen:

- En Windows 7 Professional o Windows Vista, se pueden agregar usuarios a este grupo utilizando el componente estándar de Microsoft Management Console (MMC) “Usuarios y grupos locales”.
- En el caso de las versiones domésticas de Windows 7, Windows Vista o Windows XP, desde una cuenta con privilegios de administrador, escriba lo siguiente en una ventana de solicitud de comando:

  ```
  net localgroup “Administradores de dispositivos” username /add
  ```

  En este comando, “username” es el nombre de usuario que desea agregar a este grupo.

Compatibilidad con eSATA

Para que Device Access Manager controle los dispositivos eSATA, debe configurarse lo siguiente:

1. La unidad debe estar conectada cuando se inicia el sistema.
2. Utilizando la vista **Configuración avanzada**, asegúrese de que la letra del dispositivo eSATA no esté en la lista de las unidades para las cuales Device Access Manager no denegará el acceso. Si la letra de la unidad eSATA aparece en la lista, elimine la letra de la unidad y luego haga clic en **Aplicar**.
3. El dispositivo puede controlarse utilizando la clase de dispositivo de Medios extraíbles, utilizando ya sea la vista **Configuración sencilla** o la vista **Configuración de clases de dispositivo**.

Clases de dispositivos no administrados

HP ProtectTools Device Access Manager no administra las siguientes clases de dispositivos:

- Dispositivos de entrada/salida
  - Biométrica
  - Mouse
  - Teclado
  - Impresora
  - Impresoras Plug and Play (PnP)
  - Actualización de impresora
  - Dispositivos infrarrojos de interfaz humana
  - Lector de smart card

- Múltiples puertos en serie
- Unidad de disco
- Controlador de disquete (FDC)
- Controlador de disco duro (HDC)
- Clase de dispositivo de interfaz humana (HID)

- Alimentación eléctrica
  - Batería
  - Soporte de administración de energía avanzada (APM)
- Varios
  - PC
  - Decodificador
  - Pantalla
  - Procesador
  - Sistema
  - Desconocido
  - Volumen
  - Instantánea de volumen
  - Dispositivos de seguridad
  - Acelerador de seguridad
  - Controlador de pantalla unificado Intel®
  - Controlador de medios
  - Alterador de medios
  - Multifunción
  - Legacard
  - Cliente de red
  - Servicio de red
  - Transporte de red
  - Adaptador del SCSI

9 Recuperación en caso de robo

Computrace for HP ProtectTools (se adquiere por separado) le permite monitorizar, administrar y rastrear su equipo de forma remota.

Una vez activado, Computrace for HP ProtectTools se configura desde el Centro de Clientes de Absolute Software. Desde el Centro de Clientes, el administrador puede configurar Computrace for HP ProtectTools para monitorizar o administrar el equipo. Si el sistema se extravía o sustrae, el Centro de Clientes puede ayudar a las autoridades locales a localizar y recuperar el equipo. Si está configurado, Computrace puede continuar funcionando incluso en caso de que se borre o se sustituya la unidad de disco duro.

Para activar Computrace for HP ProtectTools:

1. Conéctese a Internet.
2. Haga clic en **Inicio**, en **Todos los programas**, en **HP** y luego en **HP ProtectTools Security Manager**.
3. En el panel izquierdo de Security Manager, haga clic en **Recuperación en caso de robo**.
4. A fin de iniciar el Asistente de activación de Computrace, haga clic en **Activar ahora**.
5. Introduzca su información de contacto y la información de pago de su tarjeta de crédito o introduzca una clave de producto adquirida por anticipado.

El Asistente de activación procesa la transacción de forma segura y configura su cuenta de usuario en el sitio web del Centro de Clientes de Absolute Software. Después de que se completa el proceso, usted recibe un correo electrónico de confirmación que incluye la información de su cuenta del Centro de Clientes.

Si ya ejecutó anteriormente el Asistente de activación de Computrace y su cuenta de usuario del Centro de Clientes ya existe, puede adquirir licencias adicionales comunicándose con su representante de cuenta de HP.

Para iniciar sesión en el Centro de Clientes:

1. Vaya a https://cc.absolute.com/.
2. En los campos **Nombre de usuario** y **Contraseña**, ingrese las credenciales que recibió en el correo electrónico de confirmación y a continuación haga clic en **Iniciar sesión**.

Por medio del uso del Centro de Clientes, usted puede:

- Monitorizar sus equipos.
- Proteger sus datos remotos.
- Informar el robo de un equipo protegido por Computrace.

▲ Haga clic en **Sepa más** para obtener más información sobre Computrace for HP ProtectTools.

10 Embedded Security for HP ProtectTools (sólo en algunos modelos)

NOTA: El chip embedded security Trusted Platform Module (TPM) debe estar instalado en el equipo para utilizar Embedded Security for HP ProtectTools.

Embedded Security for HP ProtectTools protege contra el acceso no autorizado a los datos o a credenciales del usuario. Este módulo de software proporciona los siguientes recursos de seguridad:

- Encriptación optimizada de archivos y carpetas de sistema de archivos de encriptación (EFS) de Microsoft®
- Creación de una unidad personal segura (PSD) para proteger los datos del usuario
- Funciones de administración de datos, como copias de seguridad y restauración de jerarquía de claves
- Soporte para aplicaciones de otros fabricantes (como Microsoft Outlook e Internet Explorer) para operaciones de certificados digitales protegidos al utilizar el software Embedded Security.

El chip TPM de seguridad incorporado mejora y activa otros recursos de seguridad de HP ProtectTools Security Manager. Por ejemplo, Credential Manager for HP ProtectTools puede utilizar el chip incorporado como factor de autenticación cuando el usuario inicia sesión en Windows.

Procedimientos de configuración

⚠ **PRECAUCIÓN:** Para reducir el riesgo de seguridad, se recomienda enfáticamente que su administrador de TI inicialice de inmediato el chip de seguridad incorporado. Si no se inicializa correctamente el chip de seguridad incorporado, puede suceder que un usuario no autorizado, un gusano o un virus se apropien del equipo y obtengan el control de las tareas del propietario, como la manipulación del archivo de recuperación de emergencia y la configuración de los parámetros de acceso del usuario.

Siga los pasos que aparecen en las secciones a continuación para activar e inicializar el chip de seguridad incorporado.

Activación del chip de seguridad incorporado en la utilidad de configuración del equipo

El chip de seguridad incorporado debe estar activado en el Asistente de inicialización rápida o en la utilidad de configuración del equipo.

Para activar el chip de seguridad incorporado en la utilidad de configuración del equipo:

1. Abra la utilidad de configuración iniciando o reiniciando el equipo y luego presione f10 mientras aparece el mensaje “F10 = ROM Based Setup” en el ángulo inferior izquierdo de la pantalla.
2. Si no definió una contraseña de administrador, utilice las teclas de flecha para seleccionar **Security** (Seguridad), **Setup password** (Contraseña de arranque) y entonces presione intro.
3. Ingrese la contraseña en las casillas **Contraseña nueva** y **Verificar nueva contraseña** y, a continuación, presione f10.
4. En el menú **Seguridad**, utilice las teclas de flecha para seleccionar **TPM Embedded Security** y, a continuación, presione intro.
5. En **Embedded Security**, si el dispositivo está oculto, seleccione **Disponible**.
6. Seleccione **Embedded security device state** (Estado del dispositivo de seguridad incorporado) y luego cambie la configuración a **Enable** (Activar).
7. Presione f10 para aceptar los cambios en la configuración de Embedded Security.
8. A fin de guardar sus preferencias y salir de la utilidad de configuración del equipo, utilice las teclas de flecha para seleccionar **File** (Archivo), seleccione **Save Changes and Exit** (Guardar cambios y salir) y luego siga las instrucciones que aparecen en pantalla.

Inicialización del chip de seguridad incorporado

En el proceso de inicialización para Embedded Security, usted podrá realizar las siguientes tareas:

- Definir una contraseña de propietario para el chip embedded security que protege el acceso a todas las funciones de propietario del chip embedded security.
- Configurar el archivo de recuperación de emergencia, que es un área de almacenamiento protegida que permite la re-encriptación de las claves de usuario básico para todos los usuarios.

Para inicializar el chip embedded security:

1. Haga clic con el botón derecho del mouse en el icono de **HP ProtectTools Security Manager** del área de notificación, en el extremo derecho de la barra de tareas, y luego seleccione **Inicialización de Embedded Security**.

   Se abrirá el asistente para la inicialización de HP ProtectTools Embedded Security.

2. Siga las instrucciones que aparecen en pantalla.

Configuración de la cuenta básica del usuario

La configuración de una cuenta de usuario básico en Embedded Security permite las siguientes tareas:

- Producir una clave de usuario básico que protege la información encriptada y define una contraseña para proteger la clave de usuario básico.
- Configurar una unidad personal segura (PSD) para almacenar archivos y carpetas encriptados.

PRECAUCIÓN: Proteja la contraseña de la clave de usuario básico. La información encriptada no se puede acceder ni recuperar sin esta contraseña.

Para configurar una cuenta de usuario básico y activar los recursos de seguridad del usuario:

1. Si el Asistente de inicialización del usuario de Embedded Security no está abierto, haga clic en **Inicio**, en **Todos los programas**, en **HP** y luego en **HP ProtectTools Security Manager**.
2. En el panel izquierdo, haga clic en **Embedded Security**, y luego haga clic en **Valores de configuración del usuario**.
3. En el panel derecho, en **Funciones de Embedded Security**, haga clic en **Configurar**.

   Aparecerá el asistente para la inicialización de usuario de Embedded Security.
4. Siga las instrucciones que aparecen en pantalla.

NOTA: Para utilizar correo electrónico seguro, primero debe configurar el cliente de correo electrónico para usar un certificado digital que se crea con Embedded Security. Si no hay un certificado digital disponible, debe obtener uno de la autoridad de certificación. Para obtener instrucciones sobre la configuración del correo electrónico y la obtención de un certificado digital, consulte la ayuda en el software cliente de correo electrónico.

Tareas generales

Después de que la cuenta de usuario básico haya sido configurada, es posible realizar las siguientes tareas:

- Encriptación de archivos y carpetas
- Envío y recepción de correo electrónico encriptado

Uso de la unidad segura personal

Después de haber configurado la unidad segura personal, se le solicitará escribir la contraseña de clave de usuario básico en el próximo inicio de sesión. Si se ingresa correctamente la contraseña de clave de usuario básico, podrá acceder a la PSD directamente desde el Explorador de Windows.

Encriptación de archivos y carpetas

Al trabajar con archivos encriptados, tenga en cuenta las siguientes reglas:

- Sólo se pueden encriptar archivos y carpetas en particiones NTFS. No se pueden encriptar archivos y carpetas en particiones FAT.
- Los archivos de sistema y los archivos comprimidos no pueden ser encriptados y los archivos encriptados no pueden ser comprimidos.
- Las carpetas temporales deben encriptarse porque son potencialmente interesantes para los piratas informáticos (hacker).
- Cuando se encripta un archivo o carpeta por primera vez, se configura automáticamente una política de recuperación. Esta política garantiza que si pierde sus certificados de encriptación y claves privadas pueda utilizar un agente de recuperación para desencriptar la información.

Para encriptar archivos y carpetas:

1. Haga clic con el botón derecho sobre el archivo o la carpeta que desea encriptar.
2. Haga clic en **Encriptar**.
3. Haga clic en una de las siguientes opciones:
    - **Aplicar cambios sólo a esta carpeta.**
    - **Aplicar cambios a esta carpeta, a las subcarpetas y a los archivos.**
4. Haga clic en **Aceptar**.

Envío y recepción de correo electrónico encriptado

Embedded Security le permite enviar y recibir correo electrónico encriptado, pero los procedimientos varían según el programa que utiliza para acceder a su correo electrónico. Para obtener más información, consulte la ayuda del software Embedded Security y la ayuda de su programa de correo electrónico.

Cambio de la contraseña de clave básica del usuario

Para cambiar la contraseña de clave básica del usuario:

1. Haga clic en **Inicio**, en **Todos los programas**, en **HP** y luego en **HP ProtectTools Security Manager**.
2. En el panel izquierdo, haga clic en **Embedded Security**, y luego haga clic en **Valores de configuración del usuario**.
3. En el panel derecho, en **Contraseña básica del usuario**, haga clic en **Cambiar**.
4. Ingrese la antigua contraseña y luego defina y confirme la nueva contraseña.
5. Haga clic en **Aceptar**.

Tareas avanzadas

Los administradores puede efectuar las siguientes tareas en Embedded Security:

- Copias de seguridad y restauración de las credenciales de Embedded Security, configuración de Embedded Security y unidades seguras personales
- Cambio de la contraseña del propietario
- Restablecimiento de una contraseña de usuario
- Migración segura de credenciales de seguridad de un usuario desde una plataforma de origen a una plataforma de destino

Creación y restauración de copias de seguridad

El recurso de copia de seguridad de Embedded Security crea un archivo que contiene información de certificación a ser restaurada en caso de emergencia.

Creación de un archivo de copia de seguridad

Para crear un archivo de copia de seguridad:

1. Haga clic en **Inicio**, en **Todos los programas**, en **HP** y después en **Consola administrativa de HP ProtectTools**.
2. En el panel izquierdo, haga clic en **Embedded Security**, y luego haga clic en **Copia de seguridad**.
3. En el panel derecho, haga clic en **Configurar**. Se abrirá el Asistente de copia de seguridad de HP Embedded Security for HP ProtectTools.
4. Siga las instrucciones que aparecen en pantalla.

Restauración de datos de certificación desde el archivo de copia de seguridad

Para restaurar los datos desde el archivo de copia de seguridad:

1. Haga clic en **Inicio**, en **Todos los programas**, en **HP** y después en **Consola administrativa de HP ProtectTools**.
2. En el panel izquierdo, haga clic en **Embedded Security**, y luego haga clic en **Copia de seguridad**.
3. En el panel derecho, haga clic en **Restaurar todo**. Se abrirá el Asistente de copia de seguridad de HP Embedded Security for HP ProtectTools.
4. Siga las instrucciones que aparecen en pantalla.

Cambio de la contraseña de propietario

Los administradores pueden cambiar la contraseña del propietario:

1. Haga clic en **Inicio**, en **Todos los programas**, en **HP**, y después en **Consola administrativa de HP ProtectTools**.
2. En el panel izquierdo, haga clic en **Embedded Security**, y luego haga clic en **Avanzado**.
3. En el panel derecho, en **Contraseña de propietario**, haga clic en **Cambiar**.
4. Ingrese la antigua contraseña de propietario y luego defina y confirme la nueva.
5. Haga clic en **Aceptar**.

Redefinición de una contraseña de usuario

Un administrador puede ayudar a un usuario a reconfigurar una contraseña olvidada. Para obtener información adicional, consulte la ayuda del software.

Migración de claves con el asistente de migración

La migración es una tarea avanzada de administrador que permite la administración, restauración y transferencia de claves y certificados.

Para obtener información sobre migración, consulte la ayuda del software Embedded Security.

11 Excepciones de la contraseña localizada

A nivel de seguridad de preinicio y a nivel de HP Drive Encryption, el soporte de localización de la contraseña es limitado, como se describe en las secciones siguientes.

Los IME de Windows no son compatibles a nivel de seguridad de preinicio o a nivel de HP Drive Encryption

En Windows, el usuario puede elegir un IME (editor de método de entrada) para ingresar caracteres y símbolos complejos, por ejemplo los caracteres japoneses o chinos, utilizando un teclado occidental estándar.

Los IME no son compatibles a nivel de seguridad de preinicio o de HP Drive Encryption. No puede ingresarse una contraseña de Windows con un IME en la pantalla de inicio de sesión de Seguridad de preinicio o de HP Drive Encryption y al hacerlo puede originar una situación de bloqueo. En algunos casos, Microsoft® Windows no muestra el IME cuando el usuario ingresa la contraseña.

Por ejemplo, para algunas instalaciones japonesas de Windows XP, el IME predeterminado se denomina Microsoft IME Standard 2002 for Japanese, que en realidad se traduce a la disposición del teclado E0010411. Sin embargo, esto es un IME, no una disposición del teclado. (El esquema de codificación de la disposición del teclado está reservado por Microsoft para los IME, que extienden el concepto de la disposición de un teclado). Debido a que esto no es una disposición del teclado que puede representarse en el entorno de tecleo para el mensaje de Seguridad de preinicio del BIOS o el mensaje de la contraseña de HP Drive Encryption, cualquier contraseña tecleada con este IME es rechazada por HP ProtectTools. Microsoft IME Standard 2002 for Japanese también es diferente del “Nombre común” en Microsoft Windows Vista®. Windows asigna algunos IME a la disposición de un teclado. En dichos casos, el IME es compatible con HP ProtectTools, debido a que se utiliza la definición de la disposición del teclado subyacente (el código hexadecimal).

La solución es cambiar a una de las siguientes disposiciones del teclado compatibles que se traduce en la disposición del teclado 00000411:

- Microsoft IME for Japanese
- La disposición del teclado japonés
- Office 2007 IME for Japanese: si Microsoft o un tercero utiliza el término IME o el editor de método de entrada, el método de entrada puede no ser efectivamente un IME. Esto puede causar confusión, pero el software lee la representación del código hexadecimal. De este modo, si un IME se asigna a la disposición de un teclado compatible, entonces HP ProtectTools puede admitir la configuración.

⚠ **¡ADVERTENCIA!** Cuando se implemente HP ProtectTools, se rechazarán las contraseñas ingresadas con un IME de Windows.

Cambios de la contraseña que utilizan la disposición del teclado que también es compatible

Si la contraseña se fija inicialmente con una disposición del teclado, como Inglés (EE.UU.) (409) y luego el usuario cambia la contraseña con una disposición del teclado diferente que también es compatible, como Latinoamericano (080A), el cambio de contraseña funcionará en HP Drive Encryption, pero no funcionará en el BIOS si el usuario utiliza caracteres que existen en este último pero no en el primero (por ejemplo, ē).

NOTA: Los administradores pueden resolver este problema al utilizar el recurso HP ProtectTools Manage Users para eliminar el usuario de HP ProtectTools, seleccionando la disposición del teclado deseada en el sistema operativo y luego ejecutando de nuevo el Asistente de configuración de Security Manager para el mismo usuario. El BIOS guarda la disposición del teclado deseada y las contraseñas que pueden teclearse con esta disposición del teclado se configurarán adecuadamente en el BIOS.

Otro problema posible es el uso de diferentes disposiciones del teclado que pueden producir todos los mismos caracteres. Por ejemplo, tanto la disposición del teclado Internacional (EE.UU.) (20409) como la disposición del teclado Latinoamericano (080A) pueden producir el carácter é, aunque podrían requerirse distintas secuencias de teclas. Si una contraseña se configura inicialmente con la disposición del teclado Latinoamericano, entonces se configura la disposición del teclado Latinoamericano en el BIOS, incluso si la contraseña se cambia posteriormente con la disposición del teclado Internacional (EE.UU.).

Manejo de teclas especiales

- Chino, eslovaco, francés canadiense y checo

  Cuando un usuario selecciona una de las disposiciones del teclado anteriores y luego ingresa una contraseña (por ejemplo, abcdef), debe ingresarse la misma contraseña mientras se presiona la tecla mayús para las minúsculas y la tecla mayús y la tecla bloq mayús para las mayúsculas en la Seguridad de preinicio del BIOS y HP Drive Encryption. Las contraseñas numéricas deben ingresarse con el teclado numérico.

- Coreano

  Cuando un usuario selecciona una disposición del teclado coreano compatible y luego ingresa una contraseña, debe ingresarse la misma contraseña mientras se presiona la tecla alt a la derecha para las minúsculas y la tecla alt a la derecha y la tecla bloq mayús para las mayúsculas en la Seguridad de preinicio del BIOS y HP Drive Encryption.

- Los caracteres no admitidos se enumeran en la siguiente tabla:

Idioma	Windows	BIOS	Drive Encryption
Árabe	Las teclas ﻯ ,ﻰ, y ﻯ generan dos caracteres.	Las teclas ﻯ ,ﻰ, y ﻯ generan un caracter.	Las teclas ﻯ ,ﻰ, y ﻯ generan un caracter.
Francés canadiense	ç, è, à, y é con bloq mayús son Ç, È, À y É en Windows.	ç, è, à, y é con bloq mayús son ç, è, à, y é en la Seguridad de preinicio del BIOS.	ç, è, à, y é con bloq mayús son ç, è, à, y é en HP Drive Encryption.
Español	40a no es compatible. Sin embargo, funciona porque el software lo convierte en c0a. Sin embargo, debido a diferencias sutiles entre las disposiciones del teclado, se recomienda que los usuarios hispanoparlantes cambien la disposición de su teclado Windows a 1040a (variación español) o 080a (Latinoamericano).	n/a	n/a
EE.UU. (internacional)	◦ Las teclas ¡, ¤, ‘, ’, ¥, y × en la fila superior son rechazadas. ◦ Las teclas å, ®, y Þ en la segunda fila son rechazadas. ◦ Las teclas á, ð, y ø en la tercera fila son rechazadas. ◦ Las tecla æ en la fila inferior es rechazada.	n/a	n/a

Idioma	Windows	BIOS	Drive Encryption
Checo	◦ La tecla ğ es rechazada. ◦ La tecla į es rechazada. ◦ La tecla ų es rechazada. ◦ Las teclas ė, ı y ż son rechazadas. ◦ Las teclas ģ, ķ, ļ, ņ y ţ son rechazadas.	n/a	n/a
Eslovaco	La tecla ż es rechazada.	◦ Las teclas š, ś y ş son rechazadas cuando se teclean, pero son aceptadas cuando se ingresan con el teclado del software. ◦ Las tecla muerta ţ genera dos caracteres.	n/a
Húngaro	La tecla ż es rechazada.	Las tecla ţ genera dos caracteres.	n/a

Idioma	Windows	BIOS	Drive Encryption
Esloveno	La tecla żŻ es rechazada en Windows y la tecla alt genera una tecla muerta en el BIOS.	Las teclas ú, Ú, ů, Ů, ş, Ş, ś, Ś, š y Š son rechazadas en el BIOS.	n/a
Japonés	Para Windows XP únicamente, la disposición del teclado japonés estándar, 411, es totalmente compatible. Un IME, comúnmente representado en Windows XP como Microsoft Standard IME 2002, normalmente no sería compatible. Sin embargo, las pruebas empíricas han demostrado que este IME es un casi duplicado de la disposición del teclado 411 cuando se teclean caracteres simples. Por lo tanto, el software cambia este IME a la disposición del teclado 411 cuando asegura el BIOS y HP Drive Encryption con contraseñas japonesas localizadas. Cuando está disponible, el IME de Microsoft Office 2007 es una mejor opción. A pesar del nombre del IME, es en realidad la disposición del teclado 411, que es compatible.	n/a	n/a

Qué hacer cuando una contraseña es rechazada

Las contraseñas pueden ser rechazadas por los siguientes motivos:

- Un usuario utiliza un IME que no es compatible. Este es un problema común con los idiomas de doble byte (coreano, japonés, chino). Para resolver este problema:

  1. Haga clic en **Inicio**, en **Panel de control** y luego en **Opciones regionales y de idioma**.
  2. Seleccione la ficha **Idiomas**.
  3. Haga clic en el botón **Detalles**.
  4. En la ficha **Configuración** , haga clic en el botón **Agregar** para agregar a un teclado compatible (agregar teclados de EE.UU. en Idioma de entrada chino).
  5. Configure el teclado compatible para la entrada predeterminada.
  6. Reinicie HP ProtectTools y luego vuelva a ingresar la contraseña.

- Un usuario utiliza un caracter que no es compatible. Para resolver este problema:

  1. Cambie la contraseña de Windows para que utilice sólo caracteres admitidos. Los caracteres no admitidos se enumeran en Manejo de teclas especiales en la página 114.
  2. Vuelva a ejecutar el Asistente de configuración de Security Manager y luego ingrese la nueva contraseña de Windows.

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
Consulte *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
Un área de almacenamiento protegida que permite realizar la reencriptación de las claves básicas del usuario de una clave de propietario de una plataforma a otra.

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

Autenticación
El proceso de verificación de si un usuario está autorizado a realizar una determinada tarea, como acceder a un equipo, modificar la configuración de un programa específico o visualizar datos seguros.

Autenticación de encendido
Un recurso de seguridad que requiere alguna forma de autenticación, como una smart card, un chip de seguridad o una contraseña, cuando se enciende el equipo.

Autoridad de certificación (CA)
Un servicio que emite los certificados necesarios para ejecutar 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 aparece en la barra de herramientas de las aplicaciones de Microsoft Office. Al hacer clic en el botón, se le permite firmar, encriptar o quitar la encriptación en un documento de Microsoft Office.

Certificado de 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.

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.

Chip de seguridad incorporado de Módulo de plataforma segura (TPM)
Término genérico para el chip de Embedded Security de HP ProtectTools. Un TPM autentica un equipo, en lugar de un usuario, al guardar información específica del sistema host, como claves de encriptación, certificados digitales y contraseñas. Un TPM minimiza el riesgo de que la información del equipo se vea comprometida por un robo físico o un ataque de un hacker externo.

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
La práctica de encriptar y desencriptar datos para que puedan ser decodificados sólo por personas específicas.

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
El medio con el cual un usuario comprueba la elegibilidad para una tarea específica en el proceso de autenticación.

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

Cuenta de usuario de Windows
El perfil de una persona autorizada a iniciar sesión en una red o un equipo individual.

Descodificación
Un procedimiento utilizado en criptografía para convertir datos encriptados en texto sin formato.

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

Dominio
Un grupo de equipos que forman parte de una red y comparten una base de datos de directorio común. Los dominios tienen un nombre único y cada uno tiene una serie de normas y procedimientos 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
Un recurso de seguridad que vincula la unidad de disco duro a un usuario y requiere que el usuario introduzca correctamente la contraseña de DriveLock cuando se inicia 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
Un procedimiento, como el uso de un algoritmo, empleado en criptografía para convertir texto común en texto encriptado a fin de evitar que destinatarios no autorizados lean esos datos. Existen muchos tipos de encriptación de datos y estos son la base de la seguridad de la red. Los tipos comunes incluyen 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
Una 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, un grupo de credenciales y configuraciones que se maneja como una cuenta o perfil para un usuario en particular.

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.

JITA
Autenticación Just-in-time.

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 de seguridad
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
Un modo de transferencia de datos entre un equipo y dispositivos de almacenamiento masivo, como unidades de disco duro y 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 de Windows y su contraseña o el PIN de smart card. En la mayoría de los casos, al introducir correctamente la información en la pantalla de inicio de sesión de Drive Encryption se les permite acceder directamente a Windows sin tener que volver a iniciar sesión 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

El estándar de Infraestructura de clave pública que define las interfaces para crear, utilizar y administrar 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)
Un proveedor o biblioteca de algoritmos criptográficos que pueden utilizarse en una interfaz bien definida para realizar funciones criptográficas específicas.

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

Registro único
Un recurso que guarda información de autenticación y le permite utilizar Security Manager para acceder a Internet y a aplicaciones de Windows que requieren autenticación por contraseña.

Reinicio
El proceso de reiniciar el 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.

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

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

Sello 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
Es el servicio en segundo plano de bloqueo/auditoría de dispositivo de HP ProtectTools, que debe estar en ejecución para que se apliquen las políticas de control de acceso al dispositivo. Puede verse desde dentro de la aplicación Servicios, en la opción Herramientas administrativas del Panel de control. Si no está en ejecución, HP ProtectTools Security Manager intenta iniciarlo cuando se aplican las políticas de control de acceso al dispositivo.

Sistema de archivos de encriptación (EFS)
Un sistema que encripta todos los archivos y subcarpetas dentro de la carpeta seleccionada.

Smart card
Un pequeño dispositivo de hardware, de tamaño y forma similares a los de una tarjeta de crédito, que guarda información que identifica al propietario. Se utiliza para autenticar al propietario en un equipo.

Tarjeta de ID
Un de escritorio de Windows que sirve para identificar visualmente su escritorio con su nombre de usuario e imagen elegida. Haga clic en la tarjeta de identificación para abrir la Consola administrativa de HP ProtectTools.

Token
Consulte *método de inicio de sesión de seguridad*.

Token USB
Un dispositivo de seguridad que guarda información que identifica a un usuario. Al igual que una smart card o lector biométrico, se utiliza para autenticar al propietario en un equipo.

Token virtual
Un recurso de seguridad que funciona de manera similar a una smart card y a un lector de tarjeta. El token se guarda en la unidad de disco duro del equipo o en el registro de Windows. Cuando inicia 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.

Índice

CH

D

E