HP ProtectTools

Pasos iniciales

Primera edición: agosto 2012

Número de referencia del documento: 702113-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 Security Manager (para administradores)	• Se necesitan derechos de administrador de Microsoft Windows® para acceder. • 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.
Consola de usuario de 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.

El módulo de software HP ProtectTools puede estar preinstalado, precargado o disponible para descargar desde el sitio Web de HP. Para obtener más información, visite http://www.hp.com.

NOTA: Las instrucciones en esta guía están escritas bajo el supuesto de que ya instaló los módulos de software HP ProtectTools correspondientes.

Recursos de HP ProtectTools

En la siguiente tabla se detallan los recursos clave de los módulos HP ProtectTools.

Módulo	Recursos clave
Consola administrativa de HP ProtectTools Security Manager	Los administradores pueden realizar las siguientes funciones: • Usar el Asistente de configuración de Security Manager para establecer y configurar los niveles de seguridad y los métodos de inicio de sesión de seguridad. • Configurar opciones ocultas de los usuarios. • Activar Drive Encryption y configurar el acceso de los usuarios. • Configurar políticas de Device Access Manager y acceso de usuarios. • Usar herramientas de administrador para agregar y eliminar usuarios de HP ProtectTools y ver su estado de usuarios.

Módulo	Recursos clave
Consola de usuario de HP ProtectTools Security Manager	Los usuarios generales pueden realizar las siguientes funciones: • Ver configuración para el estado de la encriptación y Device Access Manager. • Activar Computrace for HP ProtectTools. • Configurar preferencias y opciones de Copias de seguridad y restauración.
Administrador de credenciales	Los usuarios generales pueden realizar las siguientes funciones: • Cambiar los nombres de usuario y contraseñas. • Configurar y cambiar credenciales de usuario, como una contraseña de Windows, una huella digital, imágenes de rostro, smart card, tarjeta de proximidad o tarjeta sin contactos.
Administrador de contraseñas	Los usuarios generales pueden realizar las siguientes funciones: • Organizar y configurar nombres de usuario y contraseñas. • Crear contraseñas más seguras para brindar una mayor seguridad de cuenta. Password Manager completa y envía la información automáticamente. • Simplificar el proceso de inicio de sesión con la característica Inicio de sesión único, la cual recuerda y aplica automáticamente credenciales de usuario.
Drive Encryption for HP ProtectTools (solo 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. • Ofrece la opción de activar unidades de autoencriptación (solo en algunos modelos).
Device Access Manager for HP ProtectTools (solo 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 de comunicación para usuarios o grupos de usuarios específicos.
Recuperación en caso de robo (Computrace for HP ProtectTools, se adquiere por separado)	• Requiere la adquisición por separado de suscripciones de rastreo y localización para su activación. • 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.

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.

Administrador de contraseñas

Password Manager almacena nombres de usuarios y contraseñas, y puede utilizarse para:

- 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 a través de Internet. También visita con frecuencia varios sitios web populares que requieren información de inicio de sesión. Como se preocupa, en gran medida, por la seguridad, no utiliza la misma contraseña en cada cuenta. La agente de compra ha decidido utilizar Password Manager para asociar enlaces web a diferentes nombres de usuario y contraseñas. Cuando se dirige a un sitio web para iniciar una sesión, el Administrador de contraseñas le presenta las credenciales automáticamente. También puede configurar Password Manager para que le muestre los nombres de usuario y contraseñas si así lo desea.

También es posible utilizar Password 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 muy trabajador 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 ellas tiene información de inicio de sesión distinta. 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 Password Manager. Una vez finalizada esa tarea, el contador implementa Password Manager para que los empleados puedan trabajar en las cuentas web sin conocer, en ningún momento, cuáles son las credenciales de inicio de sesión que están utilizando.

Drive Encryption for HP ProtectTools (solo en algunos modelos)

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 solo 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 de unidad de autoencriptación.

Drive Encryption for HP ProtectTools no permite el acceso a los datos encriptados incluso cuando se retira la unidad, ya que ambos se encuentran vinculados a la placa del sistema original.

Ejemplo 2: Un administrador hospitalario desea asegurarse de que solo 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 solo el personal autorizado puede iniciar el equipo o dominio con su nombre de usuario y contraseña personales.

Device Access Manager for HP ProtectTools (solo en algunos modelos)

Device Access Manager for HP ProtectTools permite que un administrador restrinja y controle el acceso al hardware. 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 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.

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.

Computrace for HP ProtectTools (anteriormente LoJack Pro) (se adquiere por separado)

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

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.

Logro de objetivos de seguridad clave

Los módulos HP ProtectTools pueden trabajar en conjunto para proporcionar soluciones para diversos problemas de seguridad, incluidos los siguientes objetivos de seguridad clave:

- Proteger contra robo dirigido
- Restringir acceso a datos confidenciales
- Prevenir el acceso no autorizado de ubicaciones internas o externas
- Crear políticas de contraseñas seguras

Proteger contra robo dirigido

Un ejemplo de robo dirigido sería el robo de un equipo que contiene datos confidenciales e información de clientes en un punto de revisión de seguridad de un aeropuerto. Los siguientes recursos ayudan a la protección contra el robo dirigido:

- El recurso de autenticación de preinicio, si está activado, ayuda a evitar el acceso al sistema operativo.
    - Security Manager for HP ProtectTools: consulte HP ProtectTools Security Manager en la página 26.
    - Drive Encryption for HP ProtectTools: consulte Drive Encryption for HP ProtectTools (solo en algunos modelos) en la página 43.
- La encriptación ayuda a asegurar que se pueda acceder a los datos incluso si el disco duro se extrae y se instala en un sistema sin protección.
- Computrace puede rastrear la ubicación de un equipo tras su robo.
    - Computrace for HP ProtectTools: consulte Recuperación en caso de robo (solo en algunos modelos) en la página 64.

Restringir acceso a 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 gerentes de TI restrinjan el acceso a los dispositivos de comunicación para que la información confidencial no pueda copiarse desde la unidad de disco duro. Consulte Configuración de clases de dispositivo en la página 55.

Prevenir el acceso no autorizado de 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, cuando está activado, ayuda a evitar el acceso al sistema operativo:
  - Security Manager for HP ProtectTools: consulte HP ProtectTools Security Manager en la página 26.
  - Drive Encryption for HP ProtectTools: consulte Drive Encryption for HP ProtectTools (solo en algunos modelos) en la página 43.
- Security Manager ayuda a asegurar que un usuario no autorizado no pueda obtener contraseñas ni acceso a aplicaciones protegidas por contraseña. Consulte HP ProtectTools Security Manager en la página 26.
- 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. Consulte Device Access Manager for HP ProtectTools (solo en algunos modelos) en la página 53.

Crear políticas de contraseñas seguras

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. Consulte HP ProtectTools Security Manager en la página 26.

Elementos de seguridad adicional

Asignación de roles de seguridad

Al administrar la seguridad del equipo (sobre todo para grandes organizaciones), una práctica importante es dividir responsabilidades y derechos entre diversos tipos de administradores y usuarios.

NOTA: En una organización pequeña o para uso individual, es posible que todos estos roles los cumpla la misma persona.

En el caso de HP ProtectTools, los deberes y privilegios de seguridad se pueden dividir en los siguientes roles:

- 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.

  NOTA: Muchos de los recursos en HP ProtectTools los puede personalizar el funcionario de seguridad en colaboración con HP. Para obtener más información, visite 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 recomienda a los administradores que sigan las "mejores prácticas" a la hora de restringir los privilegios de usuario final y el acceso de usuario.

A los usuarios sin autorización no se les deben conceder privilegios administrativos.

Administración de contraseñas de HP ProtectTools

La mayoría de los recursos de HP ProtectTools Security Manager están asegurados con contraseñas. En la siguiente tabla se enumeran las contraseñas más usadas comúnmente, el módulo de software en que se configura la contraseña y la función de esta.

Las contraseñas configuradas y usadas solo por administradores de TI también se indican en esta tabla. Todas las demás contraseñas pueden ser establecidas por usuarios o administradores regulares.

Contraseña de HP ProtectTools	Configurar en el siguiente módulo	Función
Contraseña de inicio de sesión de Windows	Panel de control de Windows o HP ProtectTools Security Manager	Se puede usar para inicio de sesión manual y autenticación a fin de acceder a diversos 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 copias de seguridad y recuperación de Security Manager.
PIN de smart card	Administrador de credenciales	Puede utilizarse como autenticación multifactor. Puede utilizarse como autenticación de Windows. Autentica a los usuarios de Drive Encryption, si se selecciona smart card.

Creación de una contraseña segura

Al crear contraseñas, primero debe seguir cualquier especificación establecida por el programa. En general, sin embargo, considere las siguientes pautas para ayudarlo a crear contraseñas seguras y reducir así las posibilidades de que su contraseña se vea amenazada:

- Use contraseñas con más de 6 caracteres, de preferencia más de 8.
- Mezcle minúsculas y mayúsculas a lo largo de la contraseña.
- Siempre que sea posible, mezcle caracteres alfanuméricos e incluya caracteres especiales y signos de puntuación.
- Sustituya las letras de una palabra clave por caracteres especiales o números. Por ejemplo, puede usar el número 1 para las letras I o L.
- Combine palabras de 2 o más idiomas.
- Divida una palabra o frase intercalando números o caracteres especiales, por ejemplo: "Mar2-2Avilla45".
- No use una contraseña que aparecería en un 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 solo un par de caracteres de aumento.
- Si escribe una contraseña, no la almacene en un lugar comúnmente visible muy cerca del equipo.
- No guarde la contraseña en un archivo, como correo electrónico, en el equipo.
- No comparta cuentas ni diga a nadie a su contraseña.

Copia de seguridad de credenciales y configuración

Puede crear credenciales de las siguientes maneras:

- Use Drive Encryption for HP ProtectTools para seleccionar y crear copias de seguridad de credenciales de HP ProtectTools.
- Use la herramienta de Copias de seguridad y recuperación de HP ProtectTools Security Manager como una ubicación central desde la cual puede crear copias de seguridad y restaurar credenciales de seguridad desde alguno de los módulos HP ProtectTools.

2 Pasos iniciales

Para configurar los parámetros de HP ProtectTools, utilice el asistente de configuración bien de HP Client Security o de HP ProtectTools Security Manager.

Una vez completado el asistente de configuración de HP Client Security, el estado de la aplicación se mostrará en el panel de control de HP Client Security.

Asistente de configuración de HP Client Security

NOTA: La administración de HP ProtectTools requiere privilegios administrativos.

El asistente de configuración de HP Client Security lo guía a través de la configuración de los recursos de Security Manager que se utilizan con más frecuencia. Si no completó el asistente de configuración de HP Client Security anteriormente, puede iniciarlo de una de estas formas:

▲ En la pantalla de inicio, haga clic o toque la aplicación **HP Client Security**.

– o –

En el escritorio de Windows, haga clic o toque el dispositivo **HP ProtectTools**.

Las páginas se mostrarán en el siguiente orden:

1. **Contraseña de Windows**: escriba su contraseña de Windows.

   De esta forma protegerá su cuenta de Windows mediante una autenticación más segura.

2. **SpareKey**: para registrar la opción SpareKey, seleccione tres preguntas de seguridad.

3. **Registrar huellas digitales**: si tiene instalado un lector de huellas digitales y el controlador asociado, puede registrar huellas digitales. Debe seleccionar y registrar 2 huellas digitales como mínimo.

4. **Drive Encryption**: si tiene instalado Drive Encryption for HP ProtectTools, puede activar la encriptación de la unidad principal:

   - Encriptación de software para un disco duro tradicional;
   - Encriptación de hardware si se detecta una unidad de autoencriptación.

   Antes de activar la encriptación debe guardar una clave de encriptación en una o varias de las siguientes ubicaciones:

   NOTA: Si cancela el asistente en este momento, no podrá activar la autenticación de Windows y Drive Encryption.

   - **Medios extraíbles**, tales como una unidad flash USB con formato FAT 32.
     - Esta opción se selecciona de forma predeterminada si se detecta un único dispositivo extraíble antes de que se muestre la página de Drive Encryption.
     - Si se detectan dos o más dispositivos extraíbles, seleccione una de las unidades que se muestren.
   - **SkyDrive**: esta opción está disponible cuando se detecta una conexión a Internet.

Se requiere Windows® Live ID. Escriba su ID y contraseña o bien regístrese para conseguir una.

5. La página Finalizar le notificará que el proceso se ha realizado con éxito y le pedirá que reinicie el sistema para activar Drive Encryption.

Asistente de configuración de HP ProtectTools Security Manager

NOTA: La administración de HP ProtectTools requiere privilegios administrativos.

El asistente de configuración de HP ProtectTools Security Manager lo guía a través de la configuración de los recursos de Security Manager. Además de los parámetros que muestra el asistente, los administradores pueden configurar distintos recursos de seguridad adicionales mediante la Consola administrativa. Esta configuración se aplica al equipo y a todos los usuarios que comparten el equipo.

Para iniciar el asistente de configuración de HP ProtectTools Security Manager:

▲ Haga clic en **Asistente de configuración** en el panel izquierdo de la Consola administrativa y siga las instrucciones que aparezcan en pantalla hasta completar la configuración.

Los administradores pueden iniciar la Consola administrativa desde la Consola de usuario de HP ProtectTools Security Manager. Para obtener más información, consulte Consola administrativa de HP ProtectTools Security Manager en la página 15.

Security Manager y sus aplicaciones están disponibles para todos los usuarios que compartan este equipo.

Panel de control de HP Client Security

Para abrir HP Client Security si completó el asistente de configuración de HP Client Security con anterioridad:

▲ En la pantalla de inicio, escriba `hp`y, a continuación, seleccione **HP Client Security**.

El panel de control mostrará una visión general de los recursos y el estado relacionado de cada aplicación.

▲ Haga clic o toque la fila de una aplicación para que se muestre más información sobre la misma:

- El botón **Configurar ahora** indica que la aplicación en cuestión aún no se ha configurado. Haga clic o toque el botón para abrir la página de la aplicación y configurarla.
- El botón **Configuración** indica que el estado de la aplicación es correcto. Haga clic o toque el botón para acceder a los parámetros de configuración de la aplicación.
- La **Consola de usuario** se inicia para una configuración de usuario.
- La **Consola administrativa** se inicia para una configuración que requiera privilegios administrativos.
- El **panel de control del estado** permanece abierto tras iniciar la Consola de usuario o Consola administrativa. El estado se actualiza una vez configurados los parámetros y cerrada la consola.

3 Guía de instalación rápida para pequeñas empresas

Este capítulo está diseñado para demostrar los pasos básicos para activar las opciones más comunes y útiles dentro de HP ProtectTools para pequeñas empresas. Existen numerosas herramientas y opciones disponibles en este software que le permitirán ajustar sus preferencias y configurar su control de acceso. Esta Guía de instalación fácil se centrará en lograr que cada módulo se ejecute con el mínimo esfuerzo y tiempo. Para obtener información adicional, simplemente seleccione el módulo de su interés y haga clic en **?** o en botón Ayuda en la esquina superior derecha. Este botón proporcionará información de manera automática para ayudarlo con la ventana actualmente desplegada.

Pasos iniciales

1. En el escritorio de Windows, haga doble clic en el icono de **HP ProtectTools** en el área de notificación situada en el extremo derecho de la barra de tareas para abrir HP ProtectTools Security Manager.
2. Introduzca su contraseña de Windows o cree una contraseña.
3. Complete el asistente de configuración.

NOTA: HP ProtectTools Security Manager está configurado, de forma predeterminada, con una política de autenticación robusta.

Esta configuración está diseñada para evitar el acceso no autorizado mientras se está conectado a Windows y debe usarse cuando se requiere alta seguridad o si los usuarios estás lejos de sus sistemas con frecuencia durante el día. Si desea cambiar esta configuración, haga clic en la ficha Política de sesión y realice sus selecciones.

Para que HP ProtectTools Security Manager sólo requiera autenticación una única vez durante el inicio de sesión de Windows, siga este procedimiento.

1. En el escritorio de Windows, haga doble clic en el icono de **HP ProtectTools** en el área de notificación situada en el extremo derecho de la barra de tareas para abrir HP ProtectTools Security Manager.
2. En el panel izquierdo, haga clic en **Administración** y, a continuación, en **Consola administrativa**.
3. En el panel izquierdo, en **Sistema**, seleccione **Autenticación** del grupo **Seguridad**.
4. Haga clic en la ficha **Política de sesión** y, a continuación, seleccione los requisitos de combinación de inicio de sesión. Para revertir las selecciones, haga clic en **Restaurar valores predeterminados**.
5. Haga clic en el botón **Aplicar** luego de finalizar.

Administrador de contraseñas

¡Contraseñas! Todos tenemos unas cuantas, sobre todo cuando accedemos regularmente a sitios web o utilizamos aplicaciones que requieren iniciar una sesión. Los usuarios estándar suelen utilizar la misma contraseña para todas las aplicaciones y sitios web, y si se vuelven creativos, en seguida se olvidan de qué contraseña corresponde a qué aplicación.

Password Manager puede recordarle sus contraseñas de forma automática o bien ofrecerle la posibilidad de elegir qué sitios recordar y cuáles no. Una vez inicie la sesión en su equipo, Password Manager le proporcionará sus contraseñas o credenciales para las aplicaciones o sitios web incluidos.

Cuando accede a alguna aplicación o sitio Web que requiere credenciales, Password Manager reconocerá automáticamente el sitio y preguntará si desea que el software recuerde su información. Si desea excluir ciertos sitios, puede declinar la solicitud.

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

1. Como ejemplo, diríjase a una de las aplicaciones o sitios web incluidos y haga clic en el icono del Administrador de contraseñas en el ángulo superior izquierdo de la página web para añadir la autenticación de la web.
2. Ponga nombre al vínculo (opcional) e ingrese un nombre de usuario y contraseña en Password Manager.

NOTA: Las áreas que Password Manager usará ahora y para visitas posteriores se resaltan.

3. Luego de finalizar, haga clic en el botón **Aceptar**.
4. Password Manager también puede guardar su nombre de usuario y contraseñas para usos compartidos de redes o unidades de red distribuidas.

Visualización y administración de autenticaciones guardadas en Password Manager

Password Manager le permite ver, administrar, crear copias de seguridad e iniciar sus autenticaciones desde una ubicación central. Password Manager también admite el inicio de sitios guardado desde Windows.

Para abrir Password Manager, use uno de los siguientes dos métodos:

- Use la combinación de teclado de ctrl+clave de logotipo de Windows+h para abrir Password Manager y haga clic en **Abrir** para iniciar y autenticar el acceso directo guardado.

  – o –

- Seleccione la ficha **Administrar** en Password Manager para abrir HP ProtectTools Security Manager y editar las credenciales.

La opción **Editar** de Password Manager le permite ver y modificar el nombre, el nombre de inicio de sesión e incluso mostrar las contraseñas.

HP ProtectTools for Small Business permite realizar una copia de seguridad de todas las credenciales y configuraciones así como copiarlas en otro equipo.

Device Access Manager for HP ProtectTools

Device Access Manager se puede usar para restringir el uso de diversos dispositivos de almacenamiento interno y externo para que sus datos permanezcan protegidos en el disco duro y no se arranquen por la puerta de su empresa. Un ejemplo sería permitir que un usuario tenga acceso a sus datos pero bloquearlo para que no los copie en un CD, reproductor de música personal o dispositivo de memoria USB. A continuación, una manera sencilla de configurar esto.

1. En el escritorio de Windows, haga doble clic en el icono de **HP ProtectTools** en el área de notificación situada en el extremo derecho de la barra de tareas para abrir la Consola de usuario de HP ProtectTools Security Manager.
2. En el panel izquierdo de HP ProtectTools Security Manager, haga clic en **Administración** y, a continuación, en **Consola administrativa**.
3. Haga clic en **Device Access Manager** y, a continuación, en **Configuración de clases de dispositivo**.
4. El próximo paso es seleccionar quién seguirá teniendo acceso mientras todos los demás se bloquean.
5. Seleccione los dispositivos de hardware que desea restringir y haga clic en el botón **Aplicar** para finalizar el proceso.
6. Seleccione **Agregar**, haga clic en **Avanzadas** y, a continuación, en **Encontrar ahora**.
7. Seleccione el usuario deseado y, a continuación, haga clic en **Aceptar > Aceptar > Aplicar**.

   Su elección se mostrará en el cuadro de texto **Usuario/Grupos**.
8. Seleccione la **clase de dispositivo** que utilizará el usuario, seleccione **Permitir** o **Negar** y, a continuación, haga clic en **Aplicar**.

Drive Encryption for HP ProtectTools

Drive Encryption for HP ProtectTools se usa para proteger sus datos mediante la encriptación de toda la unidad de disco duro. Los datos contenidos en el disco duro permanecerán protegidos si roban el PC alguna vez y si extraen el disco duro del equipo original y lo colocan en otro diferente.

Una ventaja adicional en cuestión de seguridad es que Drive Encryption requiere que se autentique adecuadamente mediante su nombre de usuario y contraseña antes de que se inicie el sistema operativo. Este procedimiento se denomina autenticación de preinicio.

Para hacerle las cosas más fáciles, varios módulos de software sincronizan contraseñas automáticamente, que incluyen cuentas de usuario de Windows, dominios, Drive Encryption for HP ProtectTools, Password Manager y HP ProtectTools Security Manager.

Aplique los siguientes pasos para activar Drive Encryption for HP ProtectTools:

1. En el escritorio de Windows, haga doble clic en el icono de **HP ProtectTools** en el área de notificación situada en el extremo derecho de la barra de tareas para abrir HP ProtectTools Security Manager.
2. En el panel izquierdo, haga clic en **Administración** y, a continuación, en **Consola administrativa**.
3. En el panel izquierdo, haga clic en **Asistente de configuración**.
4. Seleccione **Siguiente** en la pantalla de bienvenida.

5. Ingrese su contraseña de Windows para iniciar el asistente de activación y luego haga clic en **Siguiente**.
6. Omita SpareKey si no lo desea.
7. Marque la casilla **Drive Encryption** y luego haga clic en **Siguiente**.
8. Marque la unidad que desea encriptar y luego haga clic en **Siguiente**.
9. La ventana de configuración de Drive Encryption requiere una unidad flash USB o algún otro dispositivo externo donde almacenar la clave de recuperación de la encriptación. Mantenga esta clave de recuperación en un lugar seguro, ya que con ella se pueden recuperar los datos o acceder a la unidad en caso de que la contraseña de preinicio se pierda o falle.
10. Haga clic en **Siguiente**, complete el proceso y haga clic en **Finalizar**. Extraiga la unidad flash USB y reinicie el equipo cuando esté listo.
11. Cuando el sistema se inicie, Drive Encryption solicitará su contraseña de Windows. Ingrese la contraseña y luego haga clic en **Aceptar**.

NOTA: Mientras la unidad se encripta, puede que el equipo funcione con mayor lentitud. Una vez encriptada completamente, su rendimiento volverá a la normalidad. Cuando se accede a los datos de la unidad, éstos se encriptan o desencriptan según indique el administrador.

La autenticación de Drive Encryption "se vinculará" al inicio de sesión de Windows a través del escritorio de Windows por lo que no necesitará volver a introducir la contraseña.

4 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.

La Consola de usuario de Security Manager cuenta con aplicaciones adicionales para ayudar a la recuperación del equipo en caso de robo o de que éste se extravíe (sólo en algunos modelos).

Mediante la Consola administrativa, 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

Pasos iniciales

Para configurar los parámetros de HP ProtectTools, utilice el asistente de configuración bien de HP Client Security o de HP ProtectTools Security Manager.

Una vez completado el asistente de configuración de HP Client Security, el estado de la aplicación se mostrará en el panel de control de HP Client Security.

Asistente de configuración de HP Client Security

NOTA: La administración de HP ProtectTools requiere privilegios administrativos.

El asistente de configuración de HP Client Security lo guía a través de la configuración de los recursos de Security Manager que se utilizan con más frecuencia. Si no completó el asistente de configuración de HP Client Security anteriormente, puede iniciarlo de una de estas formas:

▲ En la pantalla de inicio, haga clic o toque la aplicación **HP Client Security**.

– o –

En el escritorio de Windows, haga clic o toque el dispositivo **HP ProtectTools**.

Las páginas se mostrarán en el siguiente orden:

1. **Contraseña de Windows**: escriba su contraseña de Windows.

   De esta forma protegerá su cuenta de Windows mediante una autenticación más segura.

2. **SpareKey**: para registrar la opción SpareKey, seleccione tres preguntas de seguridad.

3. **Registrar huellas digitales**: si tiene instalado un lector de huellas digitales y el controlador asociado, puede registrar huellas digitales. Debe seleccionar y registrar 2 huellas digitales como mínimo.

4. **Drive Encryption**: si tiene instalado Drive Encryption for HP ProtectTools, puede activar la encriptación de la unidad principal:

   - Encriptación de software para un disco duro tradicional;
   - Encriptación de hardware si se detecta una unidad de autoencriptación.

   Antes de activar la encriptación debe guardar una clave de encriptación en una o varias de las siguientes ubicaciones:

   NOTA: Si cancela el asistente en este momento, no podrá activar la autenticación de Windows y Drive Encryption.

   - **Medios extraíbles**, tales como una unidad flash USB con formato FAT 32.
     - Esta opción se selecciona de forma predeterminada si se detecta un único dispositivo extraíble antes de que se muestre la página de Drive Encryption.
     - Si se detectan dos o más dispositivos extraíbles, seleccione una de las unidades que se muestren.
   - **SkyDrive**: esta opción está disponible cuando se detecta una conexión a Internet.

     Se requiere Windows® Live ID. Escriba su ID y contraseña o bien regístrese para conseguir una.

5. La página Finalizar le notificará que el proceso se ha realizado con éxito y le pedirá que reinicie el sistema para activar Drive Encryption.

Asistente de configuración de HP ProtectTools Security Manager

NOTA: La administración de HP ProtectTools requiere privilegios administrativos.

El asistente de configuración de HP ProtectTools Security Manager lo guía a través de la configuración de los recursos de Security Manager. Además de los parámetros que muestra el asistente, los administradores pueden configurar distintos recursos de seguridad adicionales mediante la Consola administrativa. Esta configuración se aplica al equipo y a todos los usuarios que comparten el equipo.

Para iniciar el asistente de configuración de HP ProtectTools Security Manager:

▲ Haga clic en **Asistente de configuración** en el panel izquierdo de la Consola administrativa y siga las instrucciones que aparezcan en pantalla hasta completar la configuración.

Los administradores pueden iniciar la Consola administrativa desde la Consola de usuario de HP ProtectTools Security Manager. Para obtener más información, consulte Consola administrativa de HP ProtectTools Security Manager en la página 15.

Security Manager y sus aplicaciones están disponibles para todos los usuarios que compartan este equipo.

Panel de control de HP Client Security

Para abrir HP Client Security si completó el asistente de configuración de HP Client Security con anterioridad:

▲ En la pantalla de inicio, escriba `hp`y, a continuación, seleccione **HP Client Security**.

El panel de control mostrará una visión general de los recursos y el estado relacionado de cada aplicación.

▲ Haga clic o toque la fila de una aplicación para que se muestre más información sobre la misma:

- El botón **Configurar ahora** indica que la aplicación en cuestión aún no se ha configurado. Haga clic o toque el botón para abrir la página de la aplicación y configurarla.
- El botón **Configuración** indica que el estado de la aplicación es correcto. Haga clic o toque el botón para acceder a los parámetros de configuración de la aplicación.
- La **Consola de usuario** se inicia para una configuración de usuario.
- La **Consola administrativa** se inicia para una configuración que requiera privilegios administrativos.
- El **panel de control del estado** permanece abierto tras iniciar la Consola de usuario o Consola administrativa. El estado se actualiza una vez configurados los parámetros y cerrada la consola.

Apertura de la Consola administrativa de HP ProtectTools

Utilice la Consola administrativa de HP ProtectTools para tareas administrativas como el establecimiento de políticas del sistema o la configuración del software. A la Consola administrativa se accede a través de HP ProtectTools Security Manager:

1. En el escritorio de Windows, haga doble clic en el icono de **HP ProtectTools** en el área de notificación, en el extremo derecho de la barra de tareas.

   – o –

   En el **Panel de control**, seleccione **Sistema y seguridad** y, a continuación, **HP ProtectTools Security Manager**.

2. En el panel izquierdo de la Consola de usuario de Security Manager, haga clic en **Administración** y, a continuación, 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.

1. En el escritorio de Windows, haga doble clic en el icono de **HP ProtectTools** en el área de notificación, en el extremo derecho de la barra de tareas.

   – o –

   En el **Panel de control**, seleccione **Sistema y seguridad** y, a continuación, **HP ProtectTools Security Manager**.

2. En el panel izquierdo de la Consola de usuario de Security Manager, haga clic en **Administración** y, a continuación, en **Consola administrativa**.

La Consola administrativa muestra las siguientes selecciones en el panel izquierdo de la página de inicio:

- **Sistema**: le permite configurar los siguientes recursos de seguridad y la autenticación para usuarios y dispositivos.
  - **Seguridad**
  - **Usuarios**
  - **Credenciales**
- **Aplicaciones**: le permite configurar los parámetros para HP ProtectTools Security Manager y las aplicaciones de Security Manager.
- **Datos**: le permite configurar los parámetros de Drive Encryption (sólo en algunos modelos).
- **Equipo**: le permite configurar los parámetros de Device Access Manager.
- **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 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**: le permite administrar los recursos, la autenticación y la configuración que establece cómo interactuarán los usuarios con este equipo.
- **Usuarios**: permite configurar, administrar y registrar los usuarios de este equipo.
- **Credenciales**: permite administrar la configuración de los dispositivos de seguridad incorporados o conectados al equipo y configurar sus parámetros.

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

Para definir las políticas que rigen las credenciales necesarias para autenticar a un usuario cuando inicia 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**, seleccione una categoría de usuario, por ejemplo Administradores o Usuarios convencionales.
3. Haga clic en la credencial de autenticación para que se muestre el diálogo de edición.
4. Para requerir una combinación de dos credenciales de autenticación, haga clic en la flecha hacia abajo para seleccionar cada credencial, luego haga clic en **Aceptar**.
5. Para eliminar una credencial, haga clic en **X**, o haga clic en la credencial y luego haga clic en **Eliminar**.
6. Haga clic en **Sí** en el diálogo de configuración.
7. Para confirmar si los usuarios pueden iniciar sesión, haga clic en **Verificar que HP ProtectTools puede iniciar sesión**.
8. Para regresar la configuración original, haga clic en **Restaurar valores predeterminados**.
9. Haga clic en **Aplicar**.

Política de sesión

Para definir las políticas que estipulan las credenciales necesarias para realizar la autenticación 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**, seleccione una categoría de usuario, por ejemplo Administradores o Usuarios convencionales.
3. Haga clic en la credencial de autenticación para que se muestre el diálogo de edición.
4. Para requerir una combinación de dos credenciales de autenticación, haga clic en la flecha hacia abajo para seleccionar cada credencial, luego haga clic en **Aceptar**.
5. Para eliminar una credencial, haga clic en **X**, o haga clic en la credencial y luego haga clic en **Eliminar**.
6. Haga clic en **Sí** en el diálogo de configuración.
7. Para confirmar si los usuarios pueden iniciar sesión, haga clic en **Verificar que HP ProtectTools puede iniciar sesión**.

8. Para regresar la configuración original, haga clic en **Restaurar valores predeterminados**.
9. Haga clic en **Aplicar**.

Configuración

Para permitir que los usuarios de este equipo omitan el inicio de sesión en Windows si ya se realizó la autenticación a nivel del BIOS o a nivel de Drive Encryption:

1. En el panel izquierdo de la Consola administrativa, haga clic en **Seguridad** y luego en **Configuración**.
2. **Permitir inicio de sesión en One Step**: marque la casilla de verificación para activar el inicio de sesión en One Step o desmárquela para desactivarla.
3. 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 a través de Security Manager. Además, se verifica si registraron o no las credenciales adecuadas que les permitan cumplir con dichas políticas.

Para administrar usuarios, seleccione las siguientes configuraciones:

- Para agregar usuarios 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**.
- Para ver las políticas para un usuario específico, seleccione el usuario y luego vea las políticas en la ventana inferior.

Credenciales

En la aplicación Credenciales, puede configurar los parámetros disponibles 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 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.
2. Para permitir la recuperación de SpareKey para el inicio de sesión de Windows, seleccione la casilla de verificación.
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 del lector de huellas digitales cuando escanee sus huellas.

  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.

- **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 tarda un poco más en responder, pero la configuración requiere menos energía.
  - **Energía total**: el lector de huellas digitales está siempre preparado para su uso, aunque esta configuración consume más energía.

Rostro

Si el equipo tiene una cámara web instalada o conectada y el programa Face Recognition está instalado, los administradores pueden establecer el nivel de seguridad de Face Recognition para encontrar un término medio entre la facilidad de uso y la dificultad para violar la seguridad del equipo.

1. Haga clic en **Credenciales** y, a continuación, haga clic en **Rostro**.
2. 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 adversas, haga clic en la barra para mover el control deslizante a la posición **Practicidad**.
   - **Equilibrio**: para ofrecer un término medio entre seguridad y facilidad de uso, si tiene información confidencial o su equipo se encuentra en un área donde pueden producirse intentos de inicio de sesión sin autorización, haga clic en la barra para mover el control deslizante a la posición **Equilibrio**.
   - **Precisión**: para dificultar que algún usuario logre acceder si las escenas de registro o las condiciones de iluminación en ese momento no son adecuadas y que sea, así, menos probable que se produzca una falsa aceptación, haga clic en la barra para mover el control deslizante a la posición **Precisión**.

3. Para regresar la configuración a los valores originales, haga clic en **Restaurar valores predeterminados**.
4. Haga clic en **Aplicar**.

Smart card

Los administradores deben inicializar la smart card antes de que esta pueda utilizarse para la autenticación. La mayoría de las tarjetas inteligentes estándar CSP y PKCS11 son compatibles con Windows.

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 middleware de Smart card debe estar instalado.

1. Obtenga e instale el middleware para la smart card que se usa (como ActivClient 6.x para una smart card ActivIdentity).
2. Inserte la smart card en el lector.
3. Inicializar la smart card (formato).
   a. Abra la herramienta de inicialización de smart card, si bien ésta puede mostrarse cuando inserte la smart card en el lector.
   b. Siga las instrucciones que aparecen en pantalla para configurar un PIN.
   c. Anote el código de desbloqueo para referencia futura.
4. Cree y guarde un par de claves y certificado.
   a. Abra la **Consola administrativa de HP ProtectTools**.
   b. Haga clic en **Credenciales**, haga clic en **Smart Card** y luego haga clic en la ficha **Administración**.
   c. Asegúrese de que **Inicializar la smart card** esté seleccionado.
   d. Introduzca su PIN, haga clic en **Aplicar** y luego siga las instrucciones que aparecen en pantalla.

      Después de que se haya inicializado correctamente la smart card, usted debe 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. Haga clic en **Asistente de configuración**.
2. En la pantalla **Bienvenido**, haga clic en **Siguiente**.
3. Escriba su contraseña de Windows y haga clic en **Siguiente**.
4. En la página **SpareKey**, haga clic en **Omitir la configuración de SpareKey** (a menos que desee actualizar la información de SpareKey) y luego haga clic en **Siguiente**.
5. En la página **Active los recursos de seguridad**, haga clic en **Siguiente**.

6. En la página **Elija sus credenciales**, asegúrese de que la casilla de verificación **Smart card** esté seleccionada y, a continuación, haga clic en **Siguiente**.
7. En la página **Smart card**, escriba su PIN y luego haga clic en **Siguiente**.
8. Haga clic en **Finalizar**.

Los usuarios también pueden registrar una smart card en la Consola de usuario de Security Manager. Para obtener más información, consulte la ayuda del software HP ProtectTools Security Manager. Basta hacer clic en el icono de **?** azul en la parte superior derecha de la página de Smart card.

Configuración de la smart card

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

- **Configuración**: marque la casilla de verificación **Bloquear el equipo al extraer la smart card** para configurar el equipo de forma que se bloquee automáticamente cuando se extraiga una smart card y, a continuación, haga clic en **Aplicar**.

NOTA: El equipo se bloquea solo 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 las opciones apropiadas de las siguientes:
  - **Inicializar la smart card**: prepara una smart card para su uso 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: Los recursos que no son compatibles con su smart card o el middleware asociado no estarán disponibles.

▲ Haga clic en **Aplicar**.

Tarjeta sin contactos

Una tarjeta sin contactos es una pequeña tarjeta de plástico que contiene un chip de computación. Si hay un lector de tarjetas sin contactos conectado al equipo, si se instaló el controlador asociado del fabricante y si se seleccionó una tarjeta sin contactos como una credencial de autenticación, puede usar la tarjeta sin contactos para autenticación. Los siguientes tipos de tarjetas sin contactos son compatibles con HP ProtectTools:

- Tarjetas de memoria HID iCLASS sin contactos
- Tarjetas de memoria MiFare Classic 1k, 4k y mini sin contactos

▲ Para configurar la tarjeta sin contactos, colóquela muy cerca del lector, siga las instrucciones que aparecen en la pantalla y luego haga clic en **Aplicar**.

Tarjeta de proximidad

Una tarjeta de proximidad es una pequeña tarjeta de plástico que contiene un chip de computación. Si hay un lector de tarjetas de proximidad conectado al equipo, se instaló el controlador asociado del fabricante y se seleccionó una tarjeta de proximidad como una credencial de autenticación, podrá usar la tarjeta de proximidad junto con otras credenciales para mayor seguridad.

▲ Para configurar la tarjeta sin contactos, colóquela cerca del lector y luego haga clic en **Aplicar**.

Bluetooth

Si el equipo dispone de funcionalidad Bluetooth® se seleccionó Bluetooth como credencial de autenticación y hay un teléfono Bluetooth emparejado con el equipo, puede usar el teléfono Bluetooth en conjunto con otras credenciales para mayor seguridad. Especifique la configuración de Bluetooth:

▲ Para permitir la autenticación silenciosa, seleccione la casilla de verificación y luego haga clic en **Aplicar**.

PIN

Si se seleccionó PIN como credencial de autenticación, puede usar un PIN en conjunto con otras credenciales para mayor seguridad. Especifique la configuración PIN:

1. Haga clic en la flecha hacia arriba o abajo para seleccionar la longitud mínima del PIN.

   El número máximo de dígitos permitidos es 8.

2. Haga clic en **Aplicar**.

Aplicaciones

La página Configuración en Aplicaciones en el panel izquierdo de la Consola administrativa contiene dos fichas que le permiten personalizar el comportamiento de dos fichas que le permiten personalizar el comportamiento de las aplicaciones de HP ProtectTools Security Manager.

▲ En el panel izquierdo de la Consola administrativa, en **Aplicaciones**, haga clic en **Configuración**.

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.

1. Seleccione la casilla de verificación que está al lado de una configuración específica para activarla o desmarque esta casilla para desactivarla.
2. Haga clic en **Aplicar**.

Ficha Aplicaciones

Los administradores pueden activar o desactivar las siguientes operaciones:

- **Estado**: marque la casilla de verificación para activar todas las aplicaciones o desmárquela para desactivar todas las aplicaciones.
- **Password Manager**: activa Password Manager para todos los usuarios del equipo.

1. Seleccione la casilla de verificación que está al lado de una configuración específica para activarla o desmarque esta casilla para desactivarla.
2. Haga clic en **Aplicar**.

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

Datos

La sección de Datos del panel izquierdo de la Consola administrativa le permite configurar los parámetros de la siguiente aplicación:

- **Drive Encryption**: le permite establecer la configuración y mostrar el estado de la unidad. Para obtener más información, consulte la ayuda del software Drive Encryption. Basta hacer clic en el icono de **?** azul en la parte superior derecha de la página de Drive Encryption.

Equipo

La sección de Equipo del panel izquierdo de la Consola administrativa le permite configurar la configuración para la aplicación Device Access Manager:

- Configuración sencilla
- Configuración de clases de dispositivo
- Configuración de la autenticación just in time (JITA)
- Configuración avanzada

Para obtener más información, consulte la ayuda del software Device Access Manager haciendo clic en el icono de **?** azul en la parte superior derecha de la página Device Access Manager.

5 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:

▲ En el escritorio de Windows, haga doble clic en el icono de **HP ProtectTools** en el área de notificación, en el extremo derecho de la barra de tareas.

– o –

En el **Panel de control**, seleccione **Sistema y seguridad** y, a continuación, **HP ProtectTools Security Manager**.

Uso de la Consola de usuario de Security Manager

La Consola de usuario de Security Manager es el punto central para acceder fácilmente a los recursos, las aplicaciones y la configuración de Security Manager. La Consola de usuario muestra los siguientes componentes:

- **Tarjeta de identificación**: muestra el nombre del usuario de Windows y un icono que identifica la cuenta del usuario que inició la sesión.
- **Aplicaciones de seguridad**: muestra un menú expansible con enlaces para la configuración de las siguientes categorías de seguridad:
  - **Inicio**: le permite administrar contraseñas, configurar sus credenciales de autenticación o verificar el estado de las aplicaciones de seguridad.
  - **Recuperación en caso de robo**: Computrace for HP ProtectTools (se adquiere por separado).
- **Mis inicios de sesión**: le permite administrar sus credenciales de autenticación con Password Manager y Credential Manager.

- **Mis datos**: le permite administrar la seguridad de sus datos con Drive Encryption.

NOTA: Este componente no aparecerá si la aplicación no está instalada.

- **Mi equipo**: le permite administrar la seguridad de su equipo con Device Access Manager.

NOTA: Este componente no aparecerá si la aplicación no está instalada.

- **Administración**: permite a los administradores acceder a la **Consola administrativa** para administrar la seguridad y los usuarios.
- **Avanzadas**: muestra comandos para acceder a recursos adicionales, que incluyen:
  - **Preferencias**: le permite personalizar la configuración 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 de Security Manager. Este icono se encuentra en la parte superior derecha del marco de la ventana, al lado de los iconos para minimizar y maximizar.

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 forma en la que aparece su nombre. De forma predeterminada, se muestra su nombre completo de usuario de Windows y la imagen seleccionada durante la configuración de Windows.

Para cambiar el nombre que se muestra:

1. Abra la Consola de usuario de Security Manager. Para obtener más información, consulte Apertura de Security Manager en la página 26.
2. Haga clic en la tarjeta de identificación en el ángulo superior izquierdo de la Consola de usuario.
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**.

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, huella digital, rostro, smart card, tarjeta de proximidad, tarjeta sin contactos, teléfono Bluetooth o PIN.
- **Credential Manager**: permite cambiar fácilmente su contraseña de Windows, registrar sus huellas digitales y registrar su rostro, así como configurar una smart card, una tarjeta sin contactos, una tarjeta de proximidad, un teléfono Bluetooth o un PIN.

Los administradores pueden acceder a información sobre aplicaciones de seguridad adicional al hacer clic en **Administración** y luego en **Administración central**, en el ángulo inferior izquierdo del panel de control.

Administrador de contraseñas

Iniciar sesión en Windows, sitios web y aplicaciones es más fácil y seguro con Password Manager. Puede utilizarlo para crear contraseñas más fuertes que no tiene que anotar o recordar, y luego iniciar sesión fácil y rápidamente con una huella digital, su rostro, smart card, tarjeta de proximidad, tarjeta sin contactos, PIN o su contraseña de Windows.

El Administrador de contraseñas ofrece las siguientes opciones:

Ficha Administrar

- Agregar, editar o eliminar inicios de sesión.
- Utilice 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.
- Configure de un vistazo si cualquiera de sus contraseñas está en riesgo de seguridad.

Ficha Solidez de la contraseña

- Verifique la solidez de las contraseñas individuales usadas para sitios Web y aplicaciones, así como también, la solidez de contraseña general.
- La solidez de la contraseña se ilustra con indicadores rojos, amarillos o verdes.

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 del **Password Manager** para mostrar un menú de contexto donde puede elegir entre las siguientes opciones:

- Agregar [algúndominio.com] al Password Manager
- Abrir el Administrador de contraseñas
- Configuración del icono
- Ayuda

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] al Administrador de contraseñas**: le permite agregar un inicio de sesión para la pantalla de inicio de la sesión en curso.
- **Abrir Administrador de contraseñas**: inicia Password Manager.
- **Configuraciones del icono**: le permite especificar las condiciones en las que aparece el icono del **Administrador de contraseñas**.
- **Ayuda**: muestra la ayuda de 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:

- **Complete los datos de inicio de sesión**: muestra la página Verifique su identidad. Si la autenticación se realiza con éxito, sus datos de inicio de sesión se introducirán en los campos de inicio de sesión automáticamente y la página se enviará a continuación (si se especificó su envío cuando se creó el inicio de sesión o se editó por última vez).
- **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 al Administrador de contraseñas.
- **Abrir Administrador de contraseñas**: inicia Password Manager.
- **Ayuda**: muestra la ayuda de 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, el Administrador de contraseñas 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 **Enlaces rápidos de Password Manager** 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 al Administrador de contraseñas**.
3. Escriba sus datos de inicio de sesión. Los campos de inicio de sesión en la pantalla y sus campos correspondientes en el cuadro de diálogo están identificados con un borde naranja en negrita. También puede mostrar este cuadro de diálogo haciendo clic en **Agregar inicio de sesión** desde la ficha **Password Manager**, mediante las teclas de acceso rápido ctrl+tecla del logotipo de Windows+h, o pasar el dedo por el lector de huellas digitales.
   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. Haga clic en **Aceptar** para seleccionar el método de autenticación que desea utilizar (huellas digitales, rostro, smart card, tarjeta de proximidad, tarjeta sin contactos, teléfono

Bluetooth, PIN o contraseña) 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.

e. Si el Administrador de contraseñas 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.
- 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 del **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 están identificados con un borde naranja en negrita.

   También puede mostrar este cuadro de diálogo haciendo clic en **Editar para el inicio de sesión deseado** en la ficha **Administrador de contraseñas**.
3. Edite su información de inicio de sesión.
   - Para 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 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 Enlaces rápidos del Password Manager

Password Manager ofrece una forma rápida y fácil de abrir los sitios Web y los programas para los que creó inicios de sesión. Haga doble clic en el inicio de sesión de un programa o sitio Web del menú **Enlaces rápidos de Password Manager** o en la ficha **Administrar** de Password Manager para abrir la pantalla de inicio de sesión y complete sus datos de inicio de sesión.

Cuando crea un inicio de sesión, éste se agrega automáticamente al menú de **Vínculos rápidos** de Password Manager.

Para mostrar el menú **Vínculos rápidos**:

1. Presione la combinación de teclas de acceso rápido del **Administrador de contraseñas** (ctrl+tecla del logotipo de Windows+h es la configuración de fábrica). Para cambiar la combinación de teclas de acceso rápido en la Consola de usuario de Security Manager, haga doble clic en **Administrador de contraseñas** y, a continuación, en **Configuración**.
2. Escanee su huella digital (en equipos con un lector de huellas digitales incorporado o conectado) o ingrese 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 la Consola de usuario de Security Manager, haga clic en **Administrador de contraseñas**.
2. Haga clic en la ficha **Administrar** y luego haga clic en **Agregar categoría**.
3. Introduzca un nombre para la categoría.
4. Haga clic en **Aceptar**.

Para agregar un inicio de sesión a una categoría:

1. Coloque el puntero del mouse sobre el inicio de sesión deseado.
2. Mantenga presionado el botón izquierdo del mouse.
3. Arrastre el inicio de sesión a la lista de categorías. Las categorías se 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 solo se copian a la categoría seleccionada. Puede agregar el mismo inicio de sesión a más de una categoría y puede mostrar todos los inicios de sesión haciendo clic en **Todos**.

Administración de sus inicios de sesión

El Administrador de contraseñas hace que sea fácil administrar 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 la Consola de usuario de Security Manager, haga clic en **Administrador de contraseñas** y, a continuación, en la ficha **Administrar**.

- **Agregar inicio de sesión**: haga clic en **Agregar inicio de sesión** y siga las instrucciones que aparezcan en pantalla.
- **Sus inicios de sesión**: haga clic en un inicio de sesión existente, seleccione una de las siguientes opciones y siga las instrucciones que aparezcan en pantalla:
  - **Abrir**: abre un sitio web o programa para el que existe un inicio de sesión.
  - **Agregar**: agrega un inicio de sesión. Para obtener más información, consulte Adición de inicios de sesión en la página 29.
  - **Editar**: edita un inicio de sesión. Para obtener más información, consulte Edición de inicios de sesión en la página 30.
  - **Eliminar**: elimina un sitio web o programa del que existe un inicio de sesión.
- **Agregar categoría**: haga clic en **Agregar categoría** y siga las instrucciones que aparezcan en pantalla. Para obtener más información, consulte Organización de inicios de sesión en categorías en la página 31.

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

1. Abra la pantalla de inicio de sesión para el sitio Web o programa.
2. Haga clic en el icono del **Administrador de contraseñas** para mostrar su menú de 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.

En la ficha **Seguridad de contraseña**, indicadores de estado rojos, amarillos o verdes ilustran la solidez de las contraseñas individuales usadas para sitios web y aplicaciones, así como también, la solidez de contraseña general.

Configuración del icono del Administrador de contraseñas

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, el Administrador de contraseñas le pide que agregue un inicio de sesión para la pantalla mostrando el icono del **Administrador de contraseñas** con un signo más.

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

   - **Solicitud para agregar inicios de sesión para las pantallas de inicio de sesión**: haga clic en esta opción para que el Administrador de contraseñas le pida que agregue un inicio de sesión cuando una pantalla de inicio de sesión muestre que aún no existe una configuración de inicio.
   - **Excluir esta pantalla**: marque la casilla de verificación para que el Administrador de contraseñas no le vuelva a pedir que agregue un inicio de sesión para esta pantalla de inicio de sesión.

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

     ◦ Abra la Consola de usuario de Security Manager mientras se muestra el inicio de sesión del sitio web o la página del programa previamente excluidos y, a continuación, haga clic en **Administrador de contraseñas**.

     ◦ 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 al Administrador de contraseñas.

     ◦ Siga las instrucciones que aparecen en pantalla. Para obtener más información, consulte Adición de inicios de sesión en la página 29.

     ◦ El icono de aparece cada vez que se abre este inicio de sesión del sitio Web o pantalla del programa.

     No solicitar agregar inicios de sesión en la pantalla de inicio de sesión: seleccione el botón de radio.

2. Para acceder a los parámetros de configuración adicionales del Administrador de contraseñas, haga clic en **Administrador de contraseñas** y, a continuación, en **Configuración** en la Consola de usuario de Security Manager.

Configuración

Puede especificar la configuración para personalizar el Password Manager:

1. **Solicitud para agregar inicios de sesión para las pantallas de inicio de sesión**: el icono del **Administrador de contraseñas** con un signo más aparece cada vez que se detecta una pantalla de inicio de sesión de un sitio web o programa, lo que indica que puede agregar un inicio de sesión para esta pantalla en el menú **Inicios de sesión**. A fin de desactivar esta función, desmarque la casilla de verificación junto a **Solicitud para agregar inicios de sesión para las pantallas de inicio de sesión**.
2. **Abrir Administrador de contraseñas con ctrl+win+h**: la tecla de acceso rápido predeterminada que abre el menú de **Enlaces rápidos del Administrador de contraseñas** 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.

Administrador de credenciales

Las credenciales de Security Manager le sirven para verificar su identidad. El administrador de este equipo puede configurar qué credenciales se pueden utilizar para probar su identidad cuando inicie 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 **Administrador de credenciales** en **Mis inicios de sesión** y pueden incluir lo siguiente:

- Contraseña
- SpareKey
- Huellas digitales
- Rostro
- Smart Card
- Tarjeta sin contactos
- Tarjeta de proximidad
- Bluetooth
- PIN

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 la Consola de usuario de Security Manager, haga clic en **Administrador de credenciales** y, a continuación, 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 pedirá que configure su SpareKey personal durante la configuración inicial realizada con el asistente de configuración de HP ProtectTools Security Manager.

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 **Crear**.

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

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

Registro de sus huellas digitales

Si el administrador seleccionó Huellas digitales en la pantalla **Elija sus credenciales** y su equipo tiene un lector de huellas digitales incorporado o conectado, el asistente de configuración de HP ProtectTools Security Manager lo guiará en el proceso de configurar o "registrar" sus huellas digitales. También puede registrar sus huellas digitales en la página de Huellas digitales de **Credential Manager**, en la Consola de usuario de Security Manager.

1. En la página de Huellas digitales del asistente, se muestra un diagrama de dos manos. Los dedos que ya están registrados aparecen resaltados. Haga clic en un dedo del diagrama.

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

2. Se le solicita que pase el dedo por el lector de huellas digitales hasta que su huella digital se haya registrado correctamente. Cuando un dedo está registrado aparece con el contorno resaltado.
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 asistente, la información de la huella digital no se guarda hasta que usted haga clic en **Siguiente**. Si deja el equipo inactivo durante un tiempo o cierra el programa, los cambios que haya realizado **no** se guardan.

Registro de escenas para inicio de sesión mediante reconocimiento de rostros

Si opta por el inicio de sesión mediante reconocimiento de rostros y su equipo tiene una cámara web incorporada o conectada, el asistente de configuración de HP ProtectTools Security Manager le pedirá que registre escenas. También puede registrar escenas en la página de Inicio de sesión mediante reconocimiento de rostros de **Administrador de credenciales**, en la Consola de usuario 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 configuración de HP ProtectTools Security Manager:

1. En la página de inicio de sesión mediante reconocimiento de rostros, haga clic en **Avanzada** y luego configure las opciones adicionales. Para obtener más información, consulte Configuración de usuario avanzada en la página 37.
2. Haga clic en **Aceptar**.
3. Haga clic en **Inicio** o si ha registrado escenas previamente, haga clic en **Registrar una nueva escena**.
4. Durante el registro de escenas puede ver una demostración si hace clic en **Reproducir vídeo**.

   Si éste es el registro inicial, un diálogo aparecerá preguntando si desea ver una demostración en video. Haga clic en **Sí** o **No**.
5. Si hay poca luz, el software puede aumentar el brillo de la pantalla automáticamente o también puede hacer clic en el icono **Lamparita** para cambiar la iluminación de fondo.
6. Haga clic en el icono de la **Cámara** y luego siga las instrucciones que aparecen en la pantalla para registrar su escena.

NOTA: Asegúrese de mirar su imagen, girando la cabeza como corresponda, mientras se capturan las escenas.

7. Haga clic en **Siguiente**.

También puede registrar escenas desde la Consola de usuario de Security Manager:

1. Abra la Consola de usuario de Security Manager. Para obtener más información, consulte Apertura de Security Manager en la página 26.
2. En **Mis inicios de sesión**, haga clic en **Administrador de credenciales** y luego en **Rostro**.
3. Haga clic en **Avanzadas** para configurar las opciones adicionales. Para obtener más información, consulte Configuración de usuario avanzada en la página 37.
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 se le solicita que ingrese su contraseña de Windows, escríbala y haga clic en **Siguiente**.
7. Durante el registro de escenas puede ver una demostración si hace clic en **Reproducir vídeo**.

   Si éste es el registro inicial, un diálogo aparecerá preguntando si desea ver una demostración en video. Haga clic en **Sí** o **No**.
8. Si hay poca luz, el software puede aumentar el brillo de la pantalla automáticamente o también puede hacer clic en el icono **Lamparita** para cambiar la iluminación de fondo.
9. Haga clic en el icono de la **Cámara** y luego siga las instrucciones que aparecen en la pantalla para registrar su escena.

NOTA: Asegúrese de mirar su imagen, girando la cabeza como corresponda, 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 registro de rostros.

Autenticación

Después de que haya registrado una o más escenas, podrá utilizar su rostro para la autenticación cuando inicie sesión en el equipo o cuando comience una nueva sesión de Windows.

1. Cuando se abre la pantalla de autenticación y la cámara detecta su rostro, tiene 5 segundos para iniciar el proceso de inicio de sesión. Si su rostro se autentica exitosamente, puede acceder al equipo.
2. Si el inicio de sesión mediante reconocimiento de rostros ha expirado, Face Recognition hace una pausa. Haga clic en el icono **Cámara** para reanudar el proceso de autenticación.

NOTA: Si la iluminación es insuficiente y no puede iniciar sesión con Face Recognition, puede ingresar su contraseña de Windows para iniciar sesión en el equipo.

3. Una vez que haya iniciado sesión en el equipo, si Face Recognition le solicita que agregue escenas adicionales para mejorar su capacidad de iniciar sesión durante inicios de sesión futuros, haga clic en **Sí**.

Modo oscuro

Si la iluminación es demasiado oscura durante el proceso de inicio de sesión mediante reconocimiento de rostros, el color del fondo de la pantalla de inicio de sesión mediante reconocimiento de rostros cambia automáticamente a una pantalla en blanco para proporcionar mejor iluminación al rostro.

Para cambiar manualmente el color de fondo de la pantalla de inicio de sesión mediante reconocimiento de rostros, haga clic en el icono **Lamparita**.

Aprendizaje

Si el inicio de sesión mediante reconocimiento de rostros falla, pero usted logra introducir su contraseña con éxito, se le puede solicitar que guarde una serie de imágenes para aumentar las posibilidades de un inicio de sesión mediante reconocimiento de rostros exitoso en el futuro.

Eliminación de una escena

Para eliminar una escena registrada actualmente:

1. Abra la Consola de usuario de Security Manager. Para obtener más información, consulte Apertura de Security Manager en la página 26.
2. En **Mis inicios de sesión**, haga clic en **Credential Manager** y luego haga clic en **Rostro**.
3. Haga clic en la escena que se eliminará y luego haga clic en el icono **Papelera de reciclaje**.
4. Haga clic en **Aceptar** en el diálogo de confirmación.

Configuración de usuario avanzada

1. Abra la Consola de usuario de Security Manager. Para obtener más información, consulte Apertura de Security Manager en la página 26.
2. En **Mis inicios de sesión**, haga clic en **Administrador de credenciales** y luego en **Rostro**.

3. Haga clic en **Avanzada** para configurar las siguientes opciones:

   Ficha **Otras configuraciones**: seleccione la casilla 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 logra introducir su contraseña correctamente, se le podría solicitar que guarde varias imágenes capturadas para aumentar las posibilidades de iniciar la sesión, correctamente en el futuro, mediante el reconocimiento de rostros.
   - **Solicitar registrar una escena nueva cuando falla el inicio de sesión**: si el inicio de sesión mediante reconocimiento de rostros falla, pero logra introducir su contraseña con éxito, se le podría solicitar que registre una nueva escena para aumentar las posibilidades de iniciar la sesión, correctamente en el futuro, mediante el reconocimiento de rostros.

4. Para regresar la configuración a los valores originales, haga clic en **Restaurar valores predeterminados**.
5. Haga clic en **Aceptar**.

Configuración de una smart card

Si hay un lector de smart card incorporado o conectado al equipo, el administrador ha activado una smart card como credencial de autenticación y realizó los pasos descritos en la ayuda del software Consola administrativa de HP ProtectTools, el asistente de configuración de HP ProtectTools Security Manager le pedirá que inserte y configure una smart card. También puede configurar su smart card en la página de Smart card del **Administrador de credenciales**, en la Consola de usuario de Security Manager.

NOTA: Un administrador debe inicializar la smart card antes de que pueda usarse.

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 administración de PIN que HP ProtectTools utilizará en su algoritmo de seguridad.

Los administradores pueden inicializar la smart card mediante el uso del software del fabricante o la Consola administrativa de HP ProtectTools. Para obtener más información, consulte la ayuda del software Consola administrativa de HP ProtectTools.

Registro de la smart card

Después de la inicialización de la smart card, los usuarios pueden registrarla en Security Manager:

1. Abra la Consola de usuario de Security Manager. Para obtener más información, consulte Apertura de Security Manager en la página 26.
2. Haga clic en **Credential Manager** y luego en **Smart card**.
3. Asegúrese de que **Configurar** esté seleccionado.
4. Escriba su contraseña de Windows y su PIN y, a continuación, haga clic en **Guardar**.

Los administradores también pueden registrar la smart card en la Consola administrativa de HP ProtectTools. Para obtener más información, consulte la ayuda de software de la Consola administrativa de HP ProtectTools.

Modificación del PIN de la smart card

Para cambiar el PIN de su smart card:

1. Inserte una smart card que ya se haya formateado e inicializado previamente.
2. Seleccione **Cambiar PIN de la smart card**.
3. Escriba su PIN antiguo y luego escriba y confirme un nuevo PIN.

Tarjeta sin contactos

Una tarjeta sin contactos es una pequeña tarjeta de plástico que contiene un chip de computación. Si hay un lector de tarjetas sin contactos conectado al equipo, si el administrador instaló el controlador asociado del fabricante y el administrador activó una tarjeta sin contactos como una credencial sin contactos como credencial de autenticación, puede usar una tarjeta sin contactos como credencial de autenticación. Los siguientes tipos de tarjetas sin contactos son compatibles con HP ProtectTools:

- Tarjetas de memoria HID iCLASS sin contactos
- Tarjetas de memoria MiFare Classic 1k, 4k y mini sin contactos

▲ Para configurar la tarjeta sin contactos, colóquela muy cerca del lector, siga las instrucciones que aparecen en la pantalla y luego haga clic en **Aplicar**.

Tarjeta de proximidad

Una tarjeta de proximidad es una pequeña tarjeta de plástico que contiene un chip de computación. Si hay un lector de tarjetas de proximidad conectado al equipo, si el administrador instaló el controlador asociado del fabricante y si el administrador activó una tarjeta de proximidad como una credencial de autenticación, puede usar una tarjeta de proximidad en conjunto con otras credenciales para mayor seguridad.

▲ Para configurar su tarjeta de proximidad, colóquela muy cerca del lector, siga las instrucciones que aparezcan en pantalla y, a continuación, haga clic en **Aplicar**.

Bluetooth

Si el administrador activó Bluetooth como credencial de autenticación, puede configurar un teléfono Bluetooth en conjunto con otras credenciales para mayor seguridad.

NOTA: Solo se admiten dispositivos de teléfonos Bluetooth.

1. Asegúrese de que la funcionalidad Bluetooth esté activada en el equipo y que el teléfono Bluetooth esté activado en modo de detección. Para conectar el teléfono, se le puede solicitar que escriba un código generado automáticamente en el dispositivo Bluetooth. Según los valores de la configuración del dispositivo Bluetooth, es posible que se requiera una comparación de los códigos de emparejamiento entre el equipo y el teléfono.
2. Para registrar el teléfono, selecciónelo y luego haga clic en **Registrar**.
3. Haga clic en **Aceptar** en el diálogo de confirmación.

PIN

Si el administrador activó un PIN como credencial de autenticación, puede configurar un PIN en conjunto con otras credenciales para mayor seguridad.

▲ Para configurar un nuevo PIN, introduzca el PIN y, a continuación, vuelva a introducirlo para confirmarlo.

Administración

Los administradores pueden acceder a la Consola administrativa y Administración central al hacer clic en **Administración** y seleccionar, a continuación, **Consola administrativa** en el panel inferior izquierdo de la Consola de usuario de HP ProtectTools Security Manager.

Para obtener más información, consulte la ayuda del software Consola administrativa de HP ProtectTools.

Opciones avanzadas

Puede acceder a las siguientes opciones al hacer clic en **Avanzadas** en el panel inferior izquierdo de la Consola de usuario:

- **Preferencias**: le permite personalizar la configuración de Security Manager.
- **Copia de seguridad y restauración**: le permite realizar copias de seguridad y restaurar sus datos de Security Manager.
- **Acerca de**: muestra información sobre la versión de Security Manager.

Configuración de sus preferencias

Puede personalizar configuraciones para HP ProtectTools Security Manager. En la Consola de usuario de Security Manager, haga clic en **Avanzadas** y, a continuación, 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 solo 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 responderá con un sonido cuando pase 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 la configuración de Sonido de Windows o desactivar la respuesta de sonido desmarcando esta opción.

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

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

    Para mostrar solo los escaneos de buena calidad, 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 qual también se denomina importación y exportación.

NOTA: Con este recurso sólo se harán copias de seguridad de la información de Password Manager y Face Recognition. Drive Encryption cuenta con un sistema de copias de seguridad independiente. No se crean copias de seguridad de la información de Device Access Manager y autenticación de huellas digitales.

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 la Consola de usuario de Security Manager. Para obtener más información, consulte Apertura de Security Manager en la página 26.
2. En el panel izquierdo de la Consola de usuario, haga clic en **Avanzadas** y, a continuación, en **Copias 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 la Consola de usuario de Security Manager. Para obtener más información, consulte Apertura de Security Manager en la página 26.
2. En el panel izquierdo de la Consola de usuario, haga clic en **Avanzadas** y, a continuación, en **Copias 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**.

6 Drive Encryption for HP ProtectTools (solo en algunos modelos)

Drive Encryption for HP ProtectTools brinda una completa protección de datos mediante la encriptación de los datos de su equipo. Cuando Drive Encryption esté 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® .

HP ProtectTools Security Manager (Consola administrativa, asistente de configuración avanzada y asistente de configuración de HP Client Security) 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 o particiones para su encriptación. Para obtener más información, consulte la ayuda del software HP ProtectTools Security Manager.

Es posible realizar las siguientes tareas con Drive Encryption:

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

NOTA: Solo las unidades de disco duro SATA internas y eSATA externas pueden encriptarse.

- Creación de las claves de copia de seguridad
- Recuperación de acceso a un equipo encriptado mediante claves de copia de seguridad y HP SpareKey
- Activación de la autenticación de preinicio de Drive Encryption mediante el uso de una contraseña, una huella digital registrada o el PIN de las smart cards seleccionadas

Apertura de Drive Encryption

Los administradores pueden acceder a Drive Encryption al abrir la Consola de usuario de HP ProtectTools Security Manager.

1. En el escritorio de Windows, haga doble clic en el icono de **HP ProtectTools** en el área de notificación, en el extremo derecho de la barra de tareas.

   – o –

   En el **Panel de control**, seleccione **Sistema y seguridad** y, a continuación, **HP ProtectTools Security Manager**.

2. En el panel izquierdo de la Consola de usuario de HP ProtectTools Security Manager, seleccione **Administración** y, a continuación, **Consola administrativa**.

3. En el panel izquierdo de la Consola administrativa de HP ProtectTools, seleccione **Drive Encryption**.

Tareas generales

Activación de Drive Encryption para unidades de disco duro estándares

Las unidades de disco duro estándares se encriptan mediante la encriptación de software Siga estos pasos para activar Drive Encryption:

1. Abra la **Consola administrativa de HP ProtectTools**. Para obtener más información, consulte Apertura de la Consola administrativa de HP ProtectTools en la página 17.

2. En el panel izquierdo, haga clic en **Asistente de configuración**.

3. Seleccione la casilla de verificación **Drive Encryption** y entonces haga clic en **Siguiente**.

4. Para hacer una copia de seguridad de la clave de encriptación, conecte un dispositivo externo para grabar la clave. Esta clave debe utilizarse para acceder a los datos si los demás métodos fallan.

5. En **Hacer copia de seguridad de claves de Drive Encryption**, seleccione la casilla de verificación del dispositivo de almacenamiento donde se guardará la clave de encriptación.

6. Haga clic en **Siguiente**.

NOTA: Se le solicita que reinicie el equipo ahora. Después del reinicio, se muestra la pantalla de arranque previo de Drive Encryption, que requiere autenticación antes del inicio de Windows.

Se ha activado Drive Encryption. La encriptación de las particiones de unidad seleccionadas puede tardar varias horas, según el número y tamaño de las particiones.

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 cumplan con la especificación de OPAL de Trusted Computing Group relacionada a 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:

NOTA: La encriptación de hardware está disponible solo si TODAS las unidades del equipo son unidades de autoencriptación que cumplen las especificaciones de OPAL de Trusted Computing Group para administración de unidades de autoencriptación. En este caso, la opción **Usar la encriptación de la unidad por hardware** está disponible y se puede usar encriptación de hardware o software.

Si hay una combinación de unidades de autoencriptación y unidades de disco duro estándares, entonces la opción **Usar encriptación de la unidad por hardware** no se encuentra disponible y solo se puede usar encriptación de software. Para obtener más información, consulte Activación de Drive Encryption para unidades de disco duro estándares en la página 44.

- Utilice el asistente de configuración de HP ProtectTools Security Manager para activar Drive Encryption.

– o –

Encriptación de software

1. Abra la **Consola administrativa de HP ProtectTools**. Para obtener más información, consulte Apertura de la Consola administrativa de HP ProtectTools en la página 17.
2. En el panel izquierdo, haga clic en **Asistente de configuración**.
3. Seleccione la casilla de verificación **Drive Encryption** y entonces haga clic en **Siguiente**.

   NOTA: Si la opción **Usar encriptación de la unidad por hardware** está disponible en la parte inferior de la pantalla, desmarque la casilla de verificación.
4. En **Unidades que se encriptarán**, seleccione la casilla de verificación de la unidad de disco duro que desea encriptar y, a continuación, haga clic en **Siguiente**.
5. Para hacer una copia de seguridad de la clave de encriptación, inserte el dispositivo de almacenamiento en la ranura adecuada.
6. En **Hacer copia de seguridad de claves de Drive Encryption**, seleccione la casilla de verificación del dispositivo de almacenamiento donde se guardará la clave de encriptación.
7. Haga clic en **Aplicar**.

   NOTA: El equipo se reiniciará.

   Se ha activado Drive Encryption. La encriptación de la unidad puede tardar algunas horas, dependiendo de su tamaño.

Encriptación de hardware

1. Abra la **Consola administrativa de HP ProtectTools**. Para obtener más información, consulte Apertura de la Consola administrativa de HP ProtectTools en la página 17.
2. En el panel izquierdo, haga clic en **Asistente de configuración**.
3. Seleccione la casilla de verificación **Drive Encryption** y entonces haga clic en **Siguiente**.
4. Si la casilla de verificación **Usar encriptación de unidad de hardware** está disponible en la parte inferior de la pantalla, asegúrese de que está seleccionada.

   Si la casilla de verificación está desmarcada o si no está disponible, se aplica encriptación de software. Para obtener más información, consulte Activación de Drive Encryption para unidades de disco duro estándares en la página 44.

5. En **Unidades que se encriptarán**, seleccione la casilla de verificación de la unidad de disco duro que desea encriptar y, a continuación, haga clic en **Siguiente**.

NOTA: Si solo 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, también se seleccionará automáticamente disco 0 y se pondrá de color gris, pero la opción para seleccionar otras unidades de disco duro para encriptación de hardware queda disponible.

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

6. Para hacer una copia de seguridad de la clave de encriptación, inserte el dispositivo de almacenamiento en la ranura adecuada.
7. En **Hacer copia de seguridad de 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: Se le solicita que reinicie el equipo ahora. Se mostrará el arranque previo de Drive Encryption, que requiere autenticación antes del inicio de Windows.

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.

1. Abra la **Consola administrativa de HP ProtectTools**. Para obtener más información, consulte Apertura de la Consola administrativa de HP ProtectTools en la página 17.
2. En el panel izquierdo, haga clic en **Asistente de configuración**.
3. Desmarque la casilla de verificación **Drive Encryption** y, a continuación, haga clic en **Siguiente**.

Se inicia la desactivación de Drive Encryption.

NOTA: Si se utilizó encriptación de software, se iniciará la desencriptación. Puede tardar varias horas, según el tamaño de las particiones de unidades de disco duro encriptadas. Cuando la desencriptación haya terminado, se desactivará Drive Encryption.

Si se utilizó encriptación de hardware, la unidad se desencriptará instantáneamente y luego de unos minutos se desactivará Drive Encryption.

Una vez que Drive Encryption está desactivado, se le solicitará que apague el equipo, si cuenta con hardware encriptado, o reinicie el equipo si cuenta con software encriptado.

Inicio de sesión después de la activación de Drive Encryption

Cuando encienda su equipo una vez que haya activado Drive Encryption y registrado su cuenta de usuario, deberá iniciar sesión en la pantalla de inicio de sesión de Drive Encryption:

NOTA: Al salir de la suspensión o del modo de espera, no se muestra la autenticación de arranque previo de Drive Encryption para la encriptación de software o hardware. La encriptación de hardware proporciona la opción **Desactivar el modo de suspensión para obtener seguridad adicional**, lo cual evita la suspensión o el modo de espera cuando está activada.

Al salir de la hibernación, se muestra la autenticación de arranque previo de Drive Encryption para la encriptación de software o hardware.

NOTA: Si el administrador de Windows ha activado la seguridad de prearranque en el BIOS en HP ProtectTools Security Manager y el inicio de sesión en One-Step está activado de forma predeterminada, puede iniciar sesión en el equipo inmediatamente después de la autenticación previa al arranque del BIOS, sin necesidad de volver a autenticarse en la pantalla de inicio de sesión de Drive Encryption.

Inicio de sesión de un usuario:

▲ En la página **Inicio de sesión**, escriba su contraseña de Windows, el PIN de smart card o SpareKey, o bien realice el reconocimiento de rostros o deslice un dedo cuya huella digital esté registrada.

Inicio de sesión de usuarios múltiples:

1. En la página **Seleccionar usuario para inicio de sesión**, seleccione el usuario para inicio de sesión en la lista desplegable y, a continuación, haga clic en **Siguiente**.
2. En la página **Inicio de sesión**, introduzca 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 compatibles

- ActivIdentity Oberthur Cosmopol IC 64k V5.2
- Gemalto Cyberflex Access 64k V2c
- ActivIdentity Activkey SIM (Gemalto Cyberflex Access 64k V2c)

NOTA: Si la clave de recuperación se usa para iniciar sesión en la pantalla de inicio de sesión de Drive Encryption, se requieren credenciales adicionales en el inicio de sesión de Windows para acceder a las cuentas de usuario de acceso.

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

Se recomienda encarecidamente que utilice el asistente de configuración de HP ProtectTools Security Manager para proteger sus datos mediante la encriptación de su unidad de disco duro. Después de la activación se puede encriptar cualquier unidad de disco duro o partición agregada al seguir estos pasos:

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

NOTA: Esto también se aplica al caso en que hay una combinación de unidades en la cual están presentes una o más unidades de autoencriptación y una o más unidades estándares.

– o –

▲ Para las unidades encriptadas de hardware, seleccione las unidades adicionales para encriptar.

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, desactivado o se activó la encriptación de hardware) y ver el estado de encriptación de todas las unidades de disco duro del equipo.

NOTA: Solo se puede seleccionar o anular la selección de unidades de disco duro adicionales para encriptación de hardware en la página Configuración de Drive Encryption.

- 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 se encuentra en uno de los siguientes estados:

Encriptación de software

- No encriptado
- Encriptado
- Encriptando
- Desencriptando

Encriptación de hardware

- Encriptada
- No encriptadas (para unidades adicionales)

Uso de seguridad mejorada con TPM (solo en algunos modelos)

Si el Módulo de plataforma segura (TPM) está activado y se ha seleccionado la seguridad mejorada de Drive Encryption con la funcionalidad TPM, la contraseña de Drive Encryption estará protegida por el chip de seguridad TPM. Si se extrae la unidad de disco duro y se instala en otro equipo, se niega el acceso a la unidad.

PRECAUCIÓN: La propiedad de TPM no se puede compartir con TPM.msc de Windows.

NOTA: Debido a que la contraseña está protegida por el chip de seguridad TPM, si la unidad de disco duro se traslada a otro equipo, no será posible acceder a los datos a menos que se migre la configuración de TPM a ese equipo.

NOTA: La opción TPM debe estar activada en la configuración del BIOS.

Encriptación o desencriptación de particiones de unidades individuales (solo encriptación de software)

Los administradores pueden usar la página Configuración de Drive Encryption para encriptar una o más unidades de disco duro en el equipo o desencriptar cualquier partición de unidad que ya está encriptada.

1. Abra la **Consola administrativa de HP ProtectTools**. Para obtener más información, consulte Apertura de la Consola administrativa de HP ProtectTools en la página 17.
2. En el panel izquierdo, haga clic en el icono **+** que está a la izquierda de **Drive Encryption** para que se muestren las opciones disponibles.
3. Haga clic en **Configuración**.
4. En **Estado de la unidad**, seleccione o desmarque la casilla de verificación junto a cada unidad que desee encriptar o desencriptar y luego haga clic en **Aplicar**.

NOTA: Cuando una partición se encripta o desencripta, una barra de progreso muestra el porcentaje de partición encriptada y el tiempo restante para completar el proceso.

NOTA: No se admiten particiones dinámicas. Si una partición se muestra como disponible, pero no puede encriptarse al ser seleccionada, la partición es dinámica. Una partición dinámica es consecuencia de la reducción de una partición realizada a fin de crear una nueva partición en Administración de discos.

Cuando se va a convertir una partición en una partición dinámica, se muestra una advertencia.

Copias de seguridad y recuperación (tarea de administrador)

Cuando se activa Drive Encryption, los administradores pueden usar la página de Copia de seguridad de la 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 la clave 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 al equipo. El lugar de almacenamiento también debe ser seguro, debido a que el dispositivo de almacenamiento permite el acceso a Windows.

NOTA: Para guardar la clave de encriptación, debe usar un dispositivo de almacenamiento USB con formato FAT32 o FAT16. Una memoria USB, una tarjeta de memoria Secure Digital (SD) o MultiMediaCard (MMC) pueden utilizarse para copias de seguridad.

1. Abra la **Consola administrativa de HP ProtectTools**. Para obtener más información, consulte Apertura de la Consola administrativa de HP ProtectTools en la página 17.
2. En el panel izquierdo, haga clic en el icono **+** que está a la izquierda de **Drive Encryption** para que se muestren las opciones disponibles.
3. Haga clic en **Copia de seguridad de claves de encriptación**.

4. Inserte el dispositivo de almacenamiento que se utilizará para realizar la copia de seguridad de la clave de encriptación.

NOTA: Para guardar la clave de encriptación, debe usar un dispositivo de almacenamiento USB con formato FAT32. Una memoria USB, una tarjeta de memoria Secure Digital (SD) o MultiMediaCard (MMC) pueden utilizarse para copias de seguridad. En algunos casos podría utilizarse SkyDrive.

5. En **Unidad**, seleccione la casilla de verificación del dispositivo donde desea almacenar la 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 **Aceptar**. La clave de encriptación se guarda en el dispositivo de almacenamiento que seleccionó.

Recuperación de acceso a un equipo activado mediante claves de copia de seguridad

Los administradores pueden realizar una recuperación mediante la clave de Drive Encryption con copia de seguridad en un dispositivo de almacenamiento extraíble en la activación o al seleccionar la opción **Copias de seguridad de claves de Drive Encryption** en Security Manager.

1. Inserte el dispositivo de almacenamiento extraíble que contiene la copia de seguridad de su clave.
2. Encienda el equipo.
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. Ingrese la ruta de archivo o el nombre que contiene su clave de copia de seguridad y luego haga clic en **Recuperar**.

   – o –

   Haga clic en **Examinar** para buscar el archivo de copia de seguridad requerido, haga clic en **Aceptar** y luego haga clic en **Recuperar**.
6. Cuando se abra el cuadro de diálogo de confirmación, haga clic en **Aceptar**.

   Se mostrará la pantalla de inicio de sesión de Windows.

NOTA: Si la clave de recuperación se usa para iniciar sesión en la pantalla de inicio de sesión de Drive Encryption, se requieren credenciales adicionales en el inicio de sesión de Windows para acceder a las cuentas de usuario de acceso. Se recomienda enfáticamente que reinicie su contraseña después de realizar una recuperación.

Realización de una recuperación de HP SpareKey

La recuperación de SpareKey en el preinicio de Drive Encryption requiere que responda preguntas de seguridad correctamente antes de poder acceder al equipo. Para obtener más información sobre la configuración de Recuperación de SpareKey, consulte la ayuda de software de Security Manager.

Para realizar una recuperación de HP SpareKey si olvida su contraseña:

1. Encienda el equipo.
2. Cuando se muestre la página Drive Encryption for HP ProtectTools, navegue a la página de inicio de sesión de usuario.
3. Haga clic en **SpareKey**.

NOTA: Si el SpareKey no se ha inicializado en Security Manager, el botón **SpareKey** no está disponible.

4. Escriba las respuestas correctas a las preguntas mostradas y luego haga clic en **Inicio de sesión**.

   Se mostrará la pantalla de inicio de sesión de Windows.

NOTA: Si SpareKey se usa para iniciar sesión en la pantalla de inicio de sesión de Drive Encryption, se requerirán credenciales adicionales en el inicio de sesión de Windows para acceder a las cuentas de usuario. Se recomienda enfáticamente que reinicie su contraseña después de realizar una recuperación.

Visualización del 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 mediante la Consola administrativa de HP ProtectTools.

1. Abra la **Consola de usuario de HP ProtectTools**. Para obtener más información, consulte Apertura de Security Manager en la página 26.
2. En **Mis datos**, haga clic en **Drive Encryption**.

   En caso de encriptación de software o hardware, se muestra el estado de encriptación de unidad como una de las siguientes opciones:

   - Activado
   - Desactivado

   En caso de encriptación de software, se muestra el estado de encriptación de unidad como una de las siguientes opciones para cada unidad de disco duro o partición de disco duro:

   - No encriptado
   - Encriptado
   - Encriptando
   - Desencriptando

   En caso de encriptación de hardware, se muestra el estado de encriptación de unidad como una de las siguientes opciones

   - No encriptado
   - 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.

7 Device Access Manager for HP ProtectTools (solo 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 62.

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. Iniciar **HP ProtectTools Security Manager** desde el **panel de control de HP Client Security**.

   – o –

   En el escritorio de Windows, haga doble clic en el icono de **HP ProtectTools** en el área de notificación, en el extremo derecho de la barra de tareas.

   – o –

   En el **Panel de control**, seleccione **Sistema y seguridad** y, a continuación, **HP ProtectTools Security Manager**.
3. En el panel izquierdo de la Consola de usuario de HP ProtectTools Security Manager, haga clic en **Administración** y, a continuación, seleccione **Consola administrativa**.
4. En el panel izquierdo de la Consola administrativa, haga clic en **Device Access Manager**.

Los usuarios estándares pueden ver la política de HP ProtectTools Device Access Manager mediante 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 deniega el acceso a clases de dispositivos, según la pertenencia al grupo Administradores de dispositivos.
- **Configuración de clases de dispositivo**: permite o deniega el acceso a tipos de dispositivos o dispositivos específicos para grupos o usuarios específicos.
- **Configuración JITA**: configura la autenticación Just In Time (JITA), de forma que permita 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 permitir o denegar 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

NOTA: Si se usan dispositivos Bluetooth como credenciales de seguridad, no se debe restringir el acceso de dispositivos Bluetooth en la política de Device Access Manager.

- Todos los módem
- 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 del dispositivo, siga estos pasos:

1. En el panel izquierdo de la Consola administrativa de HP ProtectTools, haga clic en **Device Access Manager**, y, a continuación, 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 de Auditoría/Bloqueo del 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.

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

Al iniciar el servicio, se inicia el controlador del dispositivo. Si se detiene el servicio, sin embargo, no se detiene el controlador.

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

Para determinar si el controlador del dispositivo se está ejecutando, abra una ventana de solicitud de comando y 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 anteriormente.
  - 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 denegado 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 deniega el acceso de escritura a un dispositivo o clase de dispositivos:

Al mismo usuario, al mismo grupo, o a un miembro del mismo grupo se le puede 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 a 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 a 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 deniega 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 a 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 deniega el acceso de lectura+escritura a un dispositivo o clase de dispositivos:

Al mismo usuario, al mismo grupo, o a un miembro del mismo grupo se le puede 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, a continuación, 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, a continuación, 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 abre 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, a continuación, 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, a continuación, 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 abre 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, a continuación, 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.

NOTA: La página de configuraciones avanzadas no se ha reiniciado.

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, a continuación, 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 de 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 denegar 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, aparece el diálogo de 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, a continuación, 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, a continuación, 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. Vea Grupo Administradores de dispositivos en la página 61 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 todos los que no sean Administradores de dispositivos a los medios extraíbles.

   – 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**.

Compatibilidad con dispositivos 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 disco flexible (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

8 Recuperación en caso de robo (solo en algunos modelos)

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. Abra la Consola de usuario de Security Manager. Para obtener más información, consulte Apertura de Security Manager en la página 26.
3. En el panel izquierdo de Security Manager, haga clic en **Recuperación en caso de robo**.
4. Para iniciar el Asistente de configuración de Computrace, haga clic en **Comenzar**.
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.

9 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.

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. A través del **Panel de control**, agregue una distribución del teclado compatible (agregue el teclado de inglés/teclado EE.UU. al elegir chino como idioma de entrada).
  2. Configure el teclado compatible para la entrada predeterminada.
  3. 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. Para obtener más información sobre los caracteres no admitidos, consulte la ayuda del software Consola administrativa de HP ProtectTools.
  2. Vuelva a ejecutar el asistente de configuración de HP ProtectTools Security Manager y, a continuación, introduzca la nueva contraseña de Windows.

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.

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.

Idioma	Windows	BIOS	Drive Encryption
Francés canadiense	ç, è, à y é escritos con bloq mayús son Ç, È, À y É en Windows.	ç, è, à y é escritos con bloq mayús son ç, è, à y é en la seguridad de prearranque del BIOS.	ç, è, à y é escritos 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 × de la fila superior se rechazarán. ◦ Las teclas å, ® y Þ de la segunda fila se rechazarán. ◦ Las teclas á, ð y ø de la tercera fila se rechazarán. ◦ La tecla æ de la fila inferior se rechazará.	n/a	n/a
Checo	◦ La tecla ğ se rechazará. ◦ La tecla į se rechazará. ◦ La tecla ų se rechazará. ◦ Las teclas ė, ı y ż se rechazarán. ◦ Las teclas ģ, ķ, ļ, ņ y ţ se rechazarán.	n/a	n/a
Eslovaco	La tecla ż se rechazará.	◦ Si se introduce š, ś o ş presionando las teclas del teclado físico, se rechazarán. No obstante, sí se aceptan al introducirlas mediante el teclado del software. ◦ La tecla inactiva ţ genera dos caracteres.	n/a
Húngaro	La tecla ż se rechazará.	La tecla ţ genera dos caracteres.	n/a

Idioma	Windows	BIOS	Drive Encryption
Esloveno	La tecla żŻ se rechaza en Windows y la tecla alt genera una tecla inactiva en el BIOS.	ú, Ú, ů, Ů, ş, Ş, ś, Ś, š y Š se rechazan en el BIOS.	n/a
Japonés	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

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. Solo 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.

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.

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.

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

Consola administrativa
Una ubicación central donde los administradores puede administrar y acceder a los recursos y la configuración de HP ProtectTools.

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 solo 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.

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

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.

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

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.

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 imagen de un usuario registrado que se utiliza para la autenticación.

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

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 consta de un nombre de usuario y una contraseña (y posiblemente otra información seleccionada) que puede utilizarse para iniciar sesión en sitios Web u otros programas.

JITA
Autenticación Just-in-time.

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

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.

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.

Recuperación de HP SpareKey
La capacidad para acceder a su equipo al contestar preguntas de seguridad correctamente.

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.

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

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

Servicio en segundo plano
Es el servicio en segundo plano de Auditoría/Bloqueo del 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 se estuviera ejecutando, HP ProtectTools Security Manager intentará iniciarlo cuando se apliquen 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 gadget de escritorio de Windows que sirve para identificar visualmente su escritorio con su nombre de usuario e imagen elegida.

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. Solo pueden inscribirse (con aprobación del administrador) e iniciar sesión.

Índice