HP Client Security

Pasos iniciales

© Copyright 2013 Hewlett-Packard Development Company, L.P.

Bluetooth es una marca comercial de su propietario utilizada por Hewlett-Packard Company bajo licencia. Intel es una marca comercial de Intel Corporation en los Estados Unidos y en otros países y es utilizada bajo licencia. Microsoft y Windows son marcas comerciales registradas de Microsoft Corporation en los Estados Unidos.

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

Primera edición: agosto de 2013

Número de referencia del documento: 735339-E51

Tabla de contenido

1 Introducción a HP Client Security Manager

HP Client Security le permite proteger sus datos, su dispositivo y su identidad, aumentando así la seguridad de su equipo.

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

Los módulos del software HP Client Security pueden estar preinstalados, precargados o pueden descargarse del sitio web de HP. Para obtener más información, consulte http://www.hp.com.

NOTA: Las instrucciones incluidas en esta guía asumen que usted ya ha instalado los módulos correspondientes del software HP Client Security.

Recursos de HP Client Security

La siguiente tabla detalla los recursos claves de los módulos de HP Client Security.

Módulo	Recursos clave
HP Client Security Manager	Los administradores pueden realizar las siguientes funciones: • Proteger su equipo antes de que se inicie Windows® • Proteger su cuenta de Windows mediante una autenticación sólida • Administrar sus datos de inicio de inicio de sesión y sus contraseñas para sitios web y aplicaciones • Cambiar fácilmente la contraseña del sistema operativo Windows • Utilizar huellas digitales para mayor seguridad y comodidad • Configurar una smart card, tarjeta sin contactos o tarjeta de proximidad para autenticación • Utilizar su teléfono Bluetooth como método de identificación • Establecer un PIN para ampliar sus opciones de autenticación • Configurar las políticas de inicio de sesión y sesión • Realizar copias de seguridad y restaurar los datos de sus programas • Agregar más aplicaciones, como por ejemplo HP Drive Encryption, HP File Sanitizer, HP Trust Circles, HP Device Access Manager y HP Computrace Los usuarios generales pueden realizar las siguientes funciones: • Visualizar la configuración de Encryption Status y Device Access Manager. • Activar Computrace. • Configurar Preferencias y opciones de Copias de seguridad y recuperación.

Módulo	Recursos clave
Administrador de contraseñas	Los usuarios generales pueden realizar las siguientes funciones: • Organizar y configurar nombres de usuario y contraseñas. • Crear contraseñas más seguras para mejorar la seguridad de las cuentas de correo electrónico y web. 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. • Marcar una cuenta como amenazada, de modo que se le avisará en relación con otra cuenta(s) con credenciales similares. • Importar datos de inicio de sesión desde un explorador compatible.
HP Drive Encryption (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).
HP Device Access Manager	• 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.
HP Trust Circles	• Proporciona seguridad para archivos y documentos. • Encripta los archivos que se colocan en las carpetas especificadas por el usuario y los protege dentro de un círculo de confianza. • Permite que los archivos sean utilizados y compartidos solo por los miembros en el círculo de confianza.
Recuperación en caso de robo (Computrace, 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 de los productos de HP Client Security y ejemplos de usos comunes

La mayoría de los productos de HP Client Security incorporan tanto la autenticación del usuario (generalmente una contraseña) como una copia de seguridad administrativa para tener acceso en

caso de que las contraseñas se pierdan, no estén disponibles o se olviden, o si en cualquier momento la seguridad de la empresa exige el acceso.

NOTA: Algunos de los productos de HP Client Security están diseñados para restringir el acceso a datos. Los datos deben encriptarse cuando los mismos son tan importantes que el usuario preferiría perder la información a que se acceda a la misma sin autorización. Es recomendable hacer 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.
- Marca una cuenta como amenazada, de modo que se le avisará en relación con otra cuenta(s) con credenciales similares.
- Importa datos de inicio de sesión desde un explorador compatible.

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 empleado que trabaja mucho ha sido ascendido y ahora administrará toda la contabilidad del departamento. 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 empleado decide organizar todos los vínculos web, los nombres de usuario de las empresas y las contraseñas en Password Manager. Una vez finalizada esa tarea, el empleado 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.

HP Drive Encryption (solo en algunos modelos)

HP Drive Encryption se usa para restringir el acceso a los datos que se encuentran almacenados en toda la unidad de disco duro del equipo o en una unidad secundaria. Drive Encryption también puede administrar unidades auto encriptables.

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.

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.

HP Device Access Manager (solo en algunos modelos)

HP Device Access Manager permite a un administrador restringir y administrar el acceso al hardware. Device Access Manager puede usarse para bloquear el acceso no autorizado a las unidades flash USB donde podrían copiarse datos. También puede restringir el acceso a las unidades de CD/DVD, al control de dispositivos USB, conexiones de red, etc. Un ejemplo posible es una situación en la que proveedores externos necesitan acceder a los equipos de la empresa pero no deberían poder copiar los datos a una unidad USB.

Ejemplo 1: El gerente de una empresa de suministros médicos trabaja frecuentemente con expedientes médicos personales junto con la información de su compañía. Los empleados necesitan acceder a estos datos, y sin embargo, es de extrema importancia que los datos no se extraigan del equipo mediante una unidad USB o cualquier otro medio de almacenamiento externo. La red es segura, pero los equipos tienen grabadoras de CD y puertos USB que podrían permitir que los datos se copien o roben. El gerente usa Device Access Manager para desactivar los puertos USB y las grabadoras de CD para que no se las pueda utilizar. Si bien los puertos USB estarán bloqueados, el mouse y el teclado continuarán 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 (se adquiere por separado)

Computrace (se adquiere por separado) es un servicio que puede localizar la ubicación de un equipo robado si el usuario accede a Internet. Computrace también puede ayudar a administrar y localizar equipos de manera remota, así como supervisar el uso y las aplicaciones de equipos.

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 de HP Client Security pueden trabajar juntos para ofrecer soluciones para una variedad de problema de seguridad, incluidos los siguientes objetivos de seguridad claves:

- 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.
  - HP Client Security—Consulte HP Client Security en la página 13.
  - HP Drive Encryption: consulte HP Drive Encryption (solo en algunos modelos) en la página 31.
- 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: consulte Recuperación en caso de robo (solo en algunos modelos) en la página 56.

Restringir acceso a datos confidenciales

Imagine que un auditor contratado está trabajando en su empresa y que se le permitió el acceso a los equipos para poder revisar delicados datos financieros. Pero usted no quiere que el auditor pueda imprimir los archivos o guardarlos en un dispositivo grabable, como por ejemplo un CD. El siguiente recurso ayuda a restringir el acceso a los datos:

- HP Device Access Manager les permite a los gerentes de TI restringir el acceso a dispositivos de comunicación de forma que la información delicada no se pueda copiar desde el disco duro. Consulte Vista del sistema en la página 45.

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 investigación y desarrollo, y también para la información privada, como los registros de pacientes o los registros financieros personales. Los siguientes recursos ayudan a evitar el acceso no autorizado:

- El recurso de autenticación de preinicio, si está activado, ayuda a evitar el acceso al sistema operativo. (consulte HP Drive Encryption (solo en algunos modelos) en la página 31.
- HP Client Security ayuda a garantizar que un usuario no autorizado no pueda obtener contraseñas o acceso a aplicaciones protegidas por contraseña. Consulte HP Client Security en la página 13.
- HP Device Access Manager les permite a los gerentes de TI restringir el acceso a dispositivos grabables de forma que la información delicada no se pueda copiar desde el disco duro. Consulte HP Device Access Manager (solo en algunos modelos) en la página 44.

Crear políticas de contraseñas seguras

Si entra en vigor 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, Password Manager proporciona un repositorio protegido para las contraseñas y la comodidad de un inicio de sesión único. Consulte Password Manager en la página 19.

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 HP Client Security, las tareas y privilegios de seguridad pueden dividirse en los siguientes roles:

- Oficial de seguridad: define el nivel de seguridad para la empresa o red y determina los recursos de seguridad a desplegar, como por ejemplo Drive Encryption.

  NOTA: El oficial de seguridad puede personalizar muchos de los recursos de HP Client Security en cooperación con HP. Para obtener más información, consulte http://www.hp.com.

- Administrador de TI: aplica y administra los recursos de seguridad definidos por el oficial de seguridad. También puede activar y desactivar algunos recursos. Por ejemplo, si el oficial de seguridad ha decidido implementar Smart Cards, el administrador de TI puede activar los modos de contraseña y 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 establecer el PIN de la Smart Card y usar la tarjeta como método de autenticación.

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

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

Administración de contraseñas de HP Client Security

La mayoría de los recursos de HP Client Security están protegidos por contraseñas. La siguiente tabla enumera las contraseñas comúnmente utilizadas, el módulo de software donde se configura la contraseña, y la función de la contraseña.

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 Client Security	Configurar en el siguiente módulo	Función
Contraseña de inicio de sesión de Windows	Panel de control de Windows o HP Client Security	Puede utilizarse para el inicio de sesión manual y para la autenticación con el fin de acceder a distintos recursos de HP Client Security.

Contraseña de HP Client Security	Configurar en el siguiente módulo	Función
Contraseña de Copias de seguridad y recuperación de HP Client Security	HP Client Security, 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 con números o caracteres especiales en el medio, por ejemplo, “Mary2-2Cat45.”
- 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 configuraciones

Puede utilizar la herramienta de Copias de seguridad y recuperación de HP Client Security como una ubicación central desde la cual realizar copias de seguridad y restaurar credenciales de seguridad desde algunos módulos instalados de HP Client Security.

2 Pasos iniciales

Para configurar HP Client Security para el uso con sus credenciales, inicie HP Client Security Manager de una de estas formas: Una vez que el usuario haya completado el asistente, ese usuario no puede iniciarlo de nuevo.

1. En la pantalla de inicio o de aplicaciones, haga clic o pulse en la aplicación **HP Client Security** (Windows 8).

   – o –

   En el escritorio de Windows, haga clic o pulse en el gadget **HP Client Security** (Windows 7).

   – o –

   En el escritorio de Windows, haga doble clic o pulse dos veces en el icono de **HP Client Security** en el área de notificación, en el extremo derecho de la barra de tareas.

   – o –

   En el escritorio de Windows, haga clic o pulse en el icono de **HP Client Security** en el área de notificación y luego seleccione **Abrir HP Client Security**.

2. Se iniciará el asistente de configuración de HP Client Security Setup mostrando la página de bienvenida.

3. Lea la pantalla de bienvenida, verifique su identidad escribiendo su contraseña de Windows y luego haga clic o pulse en **Siguiente**.

   Si aún no ha creado una contraseña de Windows, se le pide que cree una. Se requiere una contraseña de Windows con el fin de proteger su cuenta de Windows del acceso de personas no autorizadas y con el objetivo de utilizar los recursos de HP Client Security.

4. En la página HP SpareKey, seleccione tres preguntas de seguridad. Escriba una respuesta para cada pregunta y haga clic en **Siguiente**. También se permiten preguntas personalizadas. Para obtener más información, consulte HP SpareKey: recuperación de contraseña en la página 15.

5. En la página de huellas digitales, registre al menos el número mínimo de huellas digitales y luego haga clic o pulse en **Siguiente**. Para obtener más información, consulte Huellas digitales en la página 13.

6. En la página Drive Encryption, cree una copia de seguridad de la clave de encriptación y luego haga clic o pulse en **Siguiente**. Para obtener más información, consulte la ayuda del software HP Drive Encryption.

NOTA: Esto se aplica a una situación en la que el usuario es un administrador y el asistente de configuración de HP Client Security no ha sido configurado por un administrador anteriormente.

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

   Esta página proporciona el estado de los recursos y las credenciales.

8. El asistente de configuración de HP Client se asegura de la activación de los recursos autenticación Just In Time y File Sanitizer. Para obtener más información, consulte la ayuda del software HP Device Access Manager y HP File Sanitizer.

NOTA: Esto se aplica a una situación en la que el usuario es un administrador y el asistente de configuración de HP Client Security no ha sido configurado por un administrador anteriormente.

Apertura de HP Client Security

Puede abrir HP Client Security de cualquiera de las siguientes maneras:

NOTA: Debe completarse el asistente de configuración de HP Client Security antes de que se pueda iniciar la aplicación HP Client Security.

- En la pantalla de inicio o de aplicaciones, haga clic o pulse en la aplicación **HP Client Security**.

  – o –

  En el escritorio de Windows, haga clic o pulse en el gadget **HP Client Security** (Windows 7).

  – o –

  En el escritorio de Windows, haga doble clic o pulse dos veces en el icono de **HP Client Security** en el área de notificación, en el extremo derecho de la barra de tareas.

  – o –

  En el escritorio de Windows, haga clic o pulse en el icono de **HP Client Security** en el área de notificación y luego seleccione **Abrir HP Client Security**.

3 Guía de instalación rápida para pequeñas empresas

Este capítulo fue diseñado para demostrar los pasos básicos para activar las opciones más comunes y útiles dentro de HP Client Security for Small Business. Múltiples herramientas y opciones en este software le permiten ajustar sus preferencias y configurar su control de acceso. El objetivo de esta Guía de configuración básica es alcanzar la operatividad de cada módulo con el menor esfuerzo y tiempo de configuración posibles. Para obtener información adicional, seleccione el módulo que le interesa, y luego haga clic en el botón **?** o en el botón Ayuda que se encuentra en la esquina superior derecha. Este botón automáticamente mostrará información para ayudarlo con la ventana que se muestra en el momento.

Pasos iniciales

1. En el escritorio de Windows, abra HP Client Security haciendo doble clic en el icono **HP Client Security** en el área de notificación ubicada en el extremo derecho de la barra de tareas.
2. Introduzca su contraseña de Windows o cree una contraseña.
3. Complete la configuración en HP Client Security Setup.

Si desea que HP Client Security solicite la autenticación solo una vez durante el inicio de sesión de Windows, consulte Recursos de seguridad en la página 28.

Administrador de contraseñas

Cada persona tiene varias contraseñas, especialmente si alguien accede regularmente a sitios web o si utiliza aplicaciones que requieren iniciar sesión. Un usuario normal utiliza la misma contraseña para todas las aplicaciones y sitios web, o bien inventa alternativas creativas y pronto olvida qué contraseña usa con cada 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.

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, utilice la combinación de teclas Ctrl+tecla Windows+h para abrir Password Manager y luego haga clic en **Iniciar sesión** para iniciar y autentificar el acceso directo de teclado guardado.

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

HP Client Security for Small Business permite crear una copia de seguridad de todas las credenciales y configuraciones y/o copiarlas a otro equipo.

HP Device Access Manager

Device Access Manager puede usarse para restringir el uso de varios dispositivos de almacenamiento internos y externos de manera que sus datos permanecerán seguros en la unidad de disco duro y nunca saldrán de las instalaciones de su empresa. Un ejemplo sería permitir a un usuario el acceso a sus datos pero impedir que éstos puedan copiarse a un CD, reproductor de música personal o dispositivo de memoria USB.

1. Abra **Device Access Manager** (consulte Apertura de Device Access Manager en la página 45).

   Se mostrará el acceso para el usuario actual.

2. Para cambiar el acceso de los usuarios, grupos o dispositivos, haga clic o pulse **Cambiar**. Para obtener más información, consulte Vista del sistema en la página 45.

HP Drive Encryption

HP Drive Encryption se usa para proteger sus datos encriptando toda la unidad de disco duro. Los datos almacenados en su unidad de disco duro permanecerán protegidos si alguna vez ocurre el robo del equipo o si se extrae la unidad de disco duro del equipo original y se la coloca en otro equipo.

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 facilitarle las cosas, múltiples módulos de software sincronizan las contraseñas automáticamente, incluidas las cuentas de usuario de Windows, los dominios de autenticación, HP Drive Encryption, Password Manager y HP Client Security.

Para configurar HP Drive Encryption durante la configuración inicial con el asistente de configuración de HP Client Security, consulte Pasos iniciales en la página 8.

4 HP Client Security

La página de inicio de HP Client Security es la ubicación central para el fácil acceso a los recursos, las aplicaciones y las configuraciones de HP Client Security. La página de inicio se divide en tres secciones:

- **DATOS**: permite acceder a las aplicaciones utilizadas para gestionar la seguridad de los datos.
- **DISPOSITIVO**: permite acceder a las aplicaciones utilizadas para gestionar la seguridad de los dispositivos.
- **IDENTIDAD**: permite el registro y la administración de las credenciales de autenticación.

Desplace el cursor sobre una aplicación sobre el mosaico de una aplicación para mostrar una descripción de la aplicación.

HP Client Security puede proporcionar vínculos a las configuraciones del usuario y administrativa en la parte inferior de la página. HP Client Security permite acceder a configuraciones avanzadas y recursos pulsando o haciendo clic en el icono **Engranaje** (configuración).

Recursos, aplicaciones y configuraciones de identidad

Los recursos, aplicaciones y configuraciones de identidad proporcionados por HP Client Security le ayudan a administrar distintos aspectos de su identidad digital. Haga clic o pulse en los siguientes mosaicos de la página de inicio de HP Client Security y luego introduzca su contraseña de Windows:

- **Huellas digitales**: registra y administra su credencial de huellas digitales.
- **SpareKey**: configura y administra su credencial de HP SpareKey, que se puede utilizar para iniciar sesión en su equipo si se han perdido o extraviado otras credenciales. También le permite restablecer la contraseña si la ha olvidado.
- **Contraseña de Windows**: permite acceder fácilmente al cambio de la contraseña de Windows.
- **Dispositivos Bluetooth**: le permite registrar y administrar sus dispositivos Bluetooth.
- **Tarjetas**: le permite registrar y administrar sus smart cards, tarjetas sin contacto y tarjetas de proximidad.
- **PIN**: le permite registrar y administrar su credencial de PIN.
- **RSA SecurID**: le permite registrar y administrar la credencial de RSA SecurID (si se ha configurado adecuadamente).
- **Password Manager**: le permite administrar contraseñas de sus cuentas y aplicaciones de Internet.

Huellas digitales

El asistente de configuración de HP Client Security le orienta a través del proceso de configurar, o "registrar", sus huellas digitales.

También puede registrar o eliminar sus huellas digitales en la página de huellas digitales, a la que puede acceder haciendo clic o pulsando en el icono **Huellas digitales** en la página de inicio de HP Client Security.

1. En la página de huellas digitales, deslice un dedo hasta que se registre correctamente.

   El número de dedos que se debe registrar aparece indicado en la página. Son preferibles los dedos índice o corazón.

2. Para eliminar huellas digitales registradas previamente, haga clic o pulse en **Eliminar**.
3. Para registrar más dedos, haga clic o pulse en **Registrar una huella digital adicional**.
4. Haga clic o pulse en **Guardar** antes de salir de la página.

⚠ **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 por un momento, o cierra el programa, los cambios que efectuó **no** se guardan.

- ▲ Para acceder a la configuración administrativa de huellas digitales, donde los administradores pueden especificar el registro, la precisión y otros ajustes, haga clic o pulse en **Configuración administrativa** (requiere privilegios administrativos).
- ▲ Para acceder a la configuración del usuario de huellas digitales, donde puede especificar los ajustes que rigen la apariencia y el comportamiento de huellas digitales, haga clic o pulse en **Configuración del usuario**.

Configuración administrativa de huellas digitales

Los administradores pueden especificar el registro, la precisión y otros ajustes de un lector de huellas digitales. Se requieren privilegios administrativos.

- ▲ Para acceder a la configuración administrativa de la credencial de huellas digitales, haga clic o pulse en **configuración administrativa** en la página de huellas digitales.

- **Registro de usuario**: elija la cantidad mínima y máxima de huellas digitales que se le permite registrar a un usuario.
- **Reconocimiento**: 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 reconocimiento inferior. 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.

Configuración de usuario de huellas digitales

En la página de configuración de usuario de huellas digitales, puede especificar los ajustes que rigen la apariencia y el comportamiento del reconocimiento.

▲ Para acceder a la configuración de usuario de la credencial de huellas digitales, haga clic o pulse en **Configuración de usuario** en la página de huellas digitales.

- **Activar respuesta de sonido**: de forma predeterminada, HP Client Security 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 la casilla de verificación.
- **Mostrar respuesta de calidad de escaneo**: para mostrar todas las huellas digitales pasadas por el lector, independientemente de la calidad, seleccione la casilla de verificación. Para mostrar sólo las huellas digitales de buena calidad pasadas por el lector, desmarque la casilla de verificación.

HP SpareKey: recuperación de contraseña

La SpareKey le permite acceder a su equipo (en plataformas compatibles) al responder a tres preguntas de seguridad.

HP Client Security le pedirá que configure su HP SpareKey personal durante la configuración inicial realizada con el asistente de configuración de HP Client Security.

Para configurar su HP SpareKey:

1. En la página de HP SpareKey del asistente, seleccione tres preguntas de seguridad y luego introduzca una respuesta para cada pregunta.

   Puede seleccionar una pregunta de una lista predeterminada o escribir su propia pregunta.

2. Haga clic o pulse en **Registrar**.

Para eliminar su HP SpareKey:

▲ Haga clic o pulse en **Eliminar su SpareKey**.

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

Puede seleccionar distintas preguntas o cambiar sus respuestas en la página de SpareKey, a la que se accede desde el mosaico Recuperación de contraseña de la página de inicio de HP Client Security.

Para acceder a la configuración de HP SpareKey, donde un administrador puede especificar ajustes relacionados con la credencial de HP SpareKey, haga clic en **Configuración** (requiere privilegios administrativos).

HP SpareKey Settings

En la página de configuración de HP SpareKey, puede especificar los ajustes que rigen el comportamiento y el uso de la credencial de HP SpareKey.

▲ Para abrir la página de configuración de HP SpareKey, haga clic o pulse en **Configuración** en la página de HP SpareKey (requiere privilegios administrativos).

Los administradores pueden seleccionar los siguientes ajustes:

- Especificar las preguntas que se presentan a cada usuario durante la configuración de HP SpareKey.
- Agregar hasta tres preguntas de seguridad personalizadas a la lista que se presenta a los usuarios.
- Elegir si se permite o no a los usuarios que escriban sus propias preguntas de seguridad.
- Especificar qué entornos de autenticación (autenticación de Windows o de inicio) permiten el uso de HP SpareKey para la recuperación de contraseñas.

Contraseña de Windows

Con HP Client Security 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:

1. En la página de inicio de HP Client Security haga clic o pulse en **Contraseña de Windows**.
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 o pulse en **Cambiar** para cambiar inmediatamente su contraseña actual por la nueva que introdujo.

Dispositivos Bluetooth

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

NOTA: Sólo 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 o pulse en **Registrar**.

Para acceder a la página Configuración de dispositivos Bluetooth en la página 16 en la que un administrador puede especificar la configuración de los dispositivos Bluetooth, haga clic en **Configuración** (requiere privilegios administrativos).

Configuración de dispositivos Bluetooth

Los administradores pueden especificar los siguientes ajustes que rigen el comportamiento y el uso de las credenciales de dispositivos Bluetooth:

Autenticación silenciosa

- **Utilizar automáticamente su dispositivo Bluetooth registrado durante la verificación de su identidad**: seleccione la casilla de verificación para permitir a los usuarios que utilicen la credencial de Bluetooth para la autenticación sin necesidad de que el usuario haga nada, o desmarcar la casilla de verificación para desactivar esta opción.

Proximidad de Bluetooth

- **Bloquear el equipo cuando su dispositivo Bluetooth registrado salga del alcance de su equipo**:seleccione la casilla de verificación para bloquear el equipo cuando un dispositivo Bluetooth que se conectó durante el inicio de sesión salga del alcance, o desmarque la casilla de verificación para desactivar esta opción.

NOTA: El módulo Bluetooth de su equipo debe ser compatible con esta capacidad para aprovechar esta característica.

Tarjetas

HP Client Security puede admitir varios tipos diferentes de tarjetas de identificación, que son pequeñas tarjetas de plástico que contienen un chip informático. Pueden ser smart cards, tarjetas sin contacto y tarjetas de proximidad. Si una de estas tarjetas, y el lector de tarjetas correspondiente, se conecta al equipo, si el administrador instaló el controlador asociado del fabricante y el administrador activó la tarjeta como una credencial de autenticación, puede usar la tarjeta como credencial de autenticación.

En el caso de las smart cards, el fabricante debe proporcionar herramientas para instalar el certificado de seguridad y administración de PIN que HP Client Security utilice en su algoritmo de seguridad. El número y el tipo de caracteres utilizados como PIN son variables. Un administrador debe inicializar la smart card antes de que pueda usarse.

HP Client Security admite los siguientes formatos de smart card:

- CSP
- PKCS11

Los siguientes tipos de tarjetas sin contactos son compatibles con HP Client Security:

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

HP Client Security admite los siguientes tipos de tarjetas de proximidad:

- Tarjetas de proximidad HID

Para registrar una smart card:

1. Inserte la tarjeta en un lector de smart card conectado.
2. Cuando se reconozca la tarjeta, introduzca el PIN de la tarjeta y luego haga clic o pulse en **Registrar**.

Para cambiar el PIN de una smart card:

1. Inserte la tarjeta en un lector de smart card conectado.
2. Cuando se reconozca la tarjeta, introduzca el PIN de la tarjeta y luego haga clic o pulse en **Autenticar**.
3. Haga clic o pulse en **Cambiar PIN** y luego introduzca el nuevo PIN.

Para registrar una tarjeta sin contacto o de proximidad:

1. Coloque la tarjeta sobre el lector adecuado o muy cerca del mismo.
2. Cuando se reconozca la tarjeta, haga clic o pulse en **Registrar**.

Para eliminar una tarjeta registrada:

1. Presente la tarjeta ante el lector.
2. Solo en el caso de las smart cards, introduzca el PIN de la tarjeta asignado y luego haga clic o pulse en **Autenticar**.
3. Haga clic o pulse en **Eliminar**.

Una vez que se registre la tarjeta, los datos de la misma aparecerán en **Tarjetas registradas**. Cuando se elimina una tarjeta, esta se elimina de la lista.

Para acceder a la configuración de tarjetas de proximidad, sin contacto y smart card, donde los administradores pueden especificar los ajustes relacionados con las credenciales de las tarjetas, haga clic o pulse en **Configuración** (se requieren privilegios administrativos).

Configuración de tarjetas de proximidad, sin contacto y smart card

Para acceder a la configuración de una tarjeta, haga clic o pulse en la tarjeta en la lista y luego haga clic o pulse en la flecha que aparece.

Para cambiar el PIN de una smart card:

1. Presente la tarjeta ante el lector
2. Introduzca el PIN de la tarjeta asignado y luego haga clic o pulse en **Continuar**.
3. Introduzca y confirme el nuevo PIN y luego haga clic o pulse en **Continuar**.

Para inicializar el PIN de una smart card:

1. Presente la tarjeta ante el lector
2. Introduzca el PIN de la tarjeta asignado y luego haga clic o pulse en **Continuar**.
3. Introduzca y confirme el nuevo PIN y luego haga clic o pulse en **Continuar**.
4. Haga clic o pulse en **Sí** para confirmar la inicialización.

Para borrar los datos de la tarjeta:

1. Presente la tarjeta ante el lector
2. Introduzca el PIN de la tarjeta asignado (solo para smart cards) y luego haga clic o pulse en **Continuar**.
3. Haga clic o pulse en **Sí** para confirmar la eliminación.

PIN

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

Para establecer un nuevo PIN:

▲ Introduzca el PIN, introdúzcalo de nuevo para confirmarlo y luego haga clic o pulse en **Aplicar**.

Para eliminar un PIN:

▲ Haga clic o pulse en **Eliminar** y luego haga clic o pulse en **Sí** para confirmar.

Para acceder a la configuración de PIN, donde los administradores pueden especificar los ajustes relacionados con las credenciales de PIN, haga clic o pulse en **Configuración** (se requieren privilegios administrativos).

Configuración de PIN

En la página de configuración de PIN, puede especificar el número máximo y mínimo de caracteres de la credencial de PIN.

RSA SecurID

Si el administrador ha activado RSA como credencial de autenticación y se cumplen las siguientes condiciones, puede registrar o eliminar una credencial de RSA SecurID.

NOTA: Se requiere la configuración adecuada.

- El usuario debe haber creado un servidor RSA.
- El token de RSA SecurID asignado al usuario y el equipo deben haberse unido al mismo dominio del servidor RSA.
- El software SecurID está instalado en su equipo.
- Hay una conexión disponible con el servidor RSA configurado correctamente.

Para registrar una credencial de RSA SecurID:

▲ Introduzca su nombre de usuario y contraseña de RSA SecurID (código de token de RSA SecurID o PIN+código de token, en función de su entorno), y luego haga clic o pulse en **Aplicar**.

Tras el registro correcto, aparecerá el mensaje "Su credencial RSA SecurID se ha registrado correctamente" y se activará el botón Eliminar.

Para eliminar una credencial de RSA SecurID:

▲ Haga clic en **Eliminar** y luego seleccione **Sí** en el diálogo emergente que le pregunta “Seguro que desea eliminar su credencial de RSA SecurID?”

Password Manager

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

NOTA: Debido a la estructura cambiante de las pantallas de inicio de sesión en Internet, es posible que Password Manager no sea compatible con todos los sitios web en todo momento.

Password Manager ofrece las siguientes opciones:

Página de Password Manager

- Haga clic o pulse en una cuenta para abrir una página web o aplicación e iniciar sesión.
- Utilice categorías para organizar sus cuentas.

Solidez de la contraseña

- Compruebe de un vistazo si cualquiera de sus contraseñas está en riesgo de seguridad.
- Cuando añada datos de inicio de sesión, compruebe la solidez de las contraseñas individuales utilizadas para sitios web y aplicaciones.
- La solidez de la contraseña se ilustra con indicadores de estado rojos, amarillos o verdes.

El icono de **Password Manager** 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 o pulse 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 sesión actual.
- **Abrir Administrador de contraseñas**: abre el Administrador de contraseñas.
- **Configuraciones del icono**: le permite especificar las condiciones en las que aparece el icono del **Password Manager**.
- **Ayuda**: muestra la ayuda del software de HP Client Security.

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:

- **Rellenar datos de inicio de sesión**: muestra la página **Verificar su identidad**. Si se autentica correctamente, sus datos de inicio de sesión se colocan en los campos de inicio de sesión y luego se envía la página (si se especificó el envío cuando se creó o editó por última vez el inicio de sesión).
- **Editar inicio de sesión**: le permite editar sus datos de inicio de sesión para este sitio web.
- **Agregar inicio de sesión**: le permite agregar una cuenta al Administrador de contraseñas.
- **Abrir Administrador de contraseñas**: abre el Administrador de contraseñas.
- **Ayuda**: muestra la ayuda del software de HP Client Security.

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

Adición de inicios de sesión

Puede agregar fácilmente un inicio de sesión para un sitio web o un programa introduciendo la información de inicio de sesión una vez. En adelante, Password Manager introduce automáticamente la información por usted. Puede utilizar estos inicios de sesión después de navegar hasta el sitio web o programa.

Para agregar un inicio de sesión:

1. Abra la pantalla de inicio de sesión de un sitio web o programa.
2. Haga clic en el icono del **Password Manager** y, a continuación, haga clic o pulse en una de las siguientes opciones, dependiendo de si la pantalla de inicio de sesión es para un sitio web o para un programa:
   - Para un sitio web, haga clic en **Agregar [nombre de dominio] a Password Manager**.
   - Para un programa, haga clic en **Agregar esta pantalla de inicio de sesión a Password Manager**.
3. Escriba sus datos de inicio de sesión. Los campos de inicio de sesión en la pantalla y sus campos correspondientes en el cuadro de diálogo están identificados con un borde naranja en negrita.
   a. Para completar un campo de inicio de sesión con una de las opciones formateadas previamente, haga clic o pulse en las flechas a la derecha del campo.
   b. Para ver la contraseña para este inicio de sesión, haga clic o pulse 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 o pulse en **Aceptar** para seleccionar el método de autenticación que desea utilizar (huellas digitales, 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 de **Password Manager** para notificarle que se creó el inicio de sesión.
   e. Si Password Manager no detecta los campos de inicio de sesión, haga clic en **Más campos**.
      - Seleccione la casilla de verificación para cada campo que se necesita para el inicio de sesión o desmarque la casilla de verificación de los campos que no se requieren para el inicio de sesión.
      - Haga clic o pulse 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:

1. Abra la pantalla de inicio de sesión de un sitio web o programa.
2. Para que se muestre un cuadro de diálogo donde editar su información de inicio de sesión, haga clic o pulse en el icono de **Password Manager** y luego 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 editar información de las cuentas desde la página de Password Manager, haciendo clic o pulsando en el inicio de sesión para mostrar las opciones de edición y luego seleccionando **Editar**.

3. Edite su información de inicio de sesión.

   - Para editar el **Nombre de cuenta**, introduzca un nuevo nombre en el campo.
   - Para agregar o editar un nombre de **Categoría**, introduzca o modifique el nombre en el campo **Categoría**.
   - Para seleccionar un campo de inicio de sesión de **Nombre de usuario** con una de las opciones formateadas previamente, haga clic o pulse en la flecha hacia abajo a la derecha del campo.

     Las opciones formateadas previamente están disponibles solo cuando se está editando el inicio de sesión con el comando Editar en el menú contextual de iconos de Password Manager.
   - Para seleccionar un campo de inicio de sesión de **Contraseña** con una de las opciones formateadas previamente, haga clic o pulse en la flecha hacia abajo a la derecha del campo.

     Las opciones formateadas previamente están disponibles solo cuando se está editando el inicio de sesión con el comando Editar en el menú contextual de iconos de Password Manager.
   - Para agregar campos adicionales de la pantalla a su inicio de sesión, haga clic o pulse en **Más campos**.
   - Para ver la contraseña para este inicio de sesión, haga clic o pulse en el icono **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**.
   - Para marcar que este inicio de sesión tiene una contraseña que ya no es confidencial, seleccione la casilla de verificación **Esta contraseña ya no es confidencial**.

     Después de guardar los cambios, todos las demás inicios de sesión que compartan la misma contraseña también se marcarán como no confidenciales. Después puede visitar cada cuenta afectada y cambiar las contraseñas si es necesario.

4. Haga clic o pulse 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 o pulse dos veces en el inicio de sesión de un programa o sitio web del menú **Enlaces rápidos de Password Manager** o en la página de Password Manager en HP Client Security para abrir la pantalla de inicio de sesión e introduzca 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**:

▲ Presione la combinación de teclas de acceso rápido de **Password Manager** (Ctrl+tecla de Windows+h es la configuración de fábrica). Para cambiar la combinación de teclas de acceso rápido en la página de inicio de HP Client Security, haga clic o pulse en **Password Manager** y luego en **Configuración**.

Organización de inicios de sesión en categorías

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

Para asignar un inicio de sesión a una categoría:

1. En la página de inicio de HP Client Security haga clic o pulse en **Password Manager**.
2. Haga clic o pulse en una cuenta y luego en **Editar**.
3. En el campo **Categoría**, introduzca un nombre de categoría.
4. Haga clic o pulse en **Guardar**.

Para eliminar una cuenta de una categoría:

1. En la página de inicio de HP Client Security haga clic o pulse en **Password Manager**.
2. Haga clic o pulse en una cuenta y luego en **Editar**.
3. En el campo **Categoría**, borre el nombre de categoría.
4. Haga clic o pulse en **Guardar**.

Para renombrar una categoría:

1. En la página de inicio de HP Client Security haga clic o pulse en **Password Manager**.
2. Haga clic o pulse en una cuenta y luego en **Editar**.
3. En el campo **Categoría**, cambie el nombre de categoría.
4. Haga clic o pulse en **Guardar**.

Administración de sus inicios de sesión

Password Manager hace que sea fácil administrar su información de inicio de sesión de acuerdo con nombres de usuario, contraseñas y múltiples cuentas de inicio de sesión, desde una ubicación central.

Sus inicios de sesión se indican en la página de Password Manager.

Para administrar sus inicios de sesión:

1. En la página de inicio de HP Client Security haga clic o pulse en **Password Manager**.
2. Haga clic o pulse en un inicio de sesión existente, seleccione una de las siguientes opciones y siga las instrucciones que aparezcan en pantalla:
   - **Editar**: edite un inicio de sesión. Para obtener más información, consulte Edición de inicios de sesión en la página 21.
   - **Iniciar sesión**: inicia sesión en la cuenta seleccionada.
   - **Eliminar**: elimina el inicio de sesión para la cuenta seleccionada.

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

1. Abra la pantalla de inicio de sesión de un sitio web o programa.
2. Haga clic o pulse en el icono del **Password Manager** para mostrar su menú contextual.
3. Haga clic o pulse 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.

Cuando esté introduciendo una contraseña durante la creación de un inicio de sesión de Password Manager para una cuenta, aparecerá una barra de color debajo de la contraseña para indicar la solidez de la contraseña. Los colores indican los valores siguientes:

- **Rojo**: débil
- **Amarillo**: normal
- **Verde**: sólida

Configuración del icono de Password Manager

Password Manager intenta identificar las pantallas de inicio de sesión para los sitios web y programas. Cuando detecta una pantalla de inicio de sesión para la que usted no creó un inicio de sesión, el Administrador de contraseñas le pide que agregue un inicio de sesión para la pantalla mostrando el icono del **Password Manager** con un signo más.

1. Haga clic o pulse en el icono y luego en **Configuración del icono** para personalizar la forma en la que Password Manager maneja los sitios de inicio de sesión posibles.
   - **Solicitud para agregar inicios de sesión para las pantallas de inicio de sesión**: haga clic en esta opción para que Password Manager le pida que agregue un inicio de sesión cuando una pantalla de inicio de sesión muestre que aún no existe una configuración de inicio.
   - **Excluir esta pantalla**: seleccione la casilla de verificación para que el Administrador de contraseñas no le vuelva a pedir que agregue un inicio de sesión en esta pantalla de inicio de sesión.
   - **No solicitar agregar inicios de sesión en la pantalla de inicio de sesión**: seleccione el botón de radio.
2. A fin de agregar un inicio de sesión para una pantalla que se ha excluido previamente:
   a. Inicie sesión en el sitio web excluido previamente.
   b. Para que Password Manager recuerde la contraseña de este sitio, haga clic o pulse en **Recordar** en el diálogo emergente para guardar la contraseña y crear un inicio de sesión para la pantalla.
3. Para acceder a ajustes adicionales de Password Manager haga clic o pulse en el icono de Password Manager, en **Abrir Password Manager** y luego en **Configuración** en la página de Password Manager.

Importación y exportación de inicios de sesión

En la página de importación y exportación de HP Password Manager, puede importar los inicios de sesión guardados por los navegadores web en su equipo. También puede importar datos de un

archivo de copia de seguridad de HP Client Security y exportar datos a un archivo de copia de seguridad de HP Client Security.

- ▲ Para abrir la página de importación y exportación, haga clic o pulse en **Importar y exportar** en la página de Password Manager.

Para importar contraseñas desde un navegador:

1. Haga clic o pulse en el navegador desde el que desea importar contraseñas (solo se muestran los navegadores instalados).
2. Desmarque la casilla de verificación de las cuentas de las que no desea importar contraseñas.
3. Haga clic o pulse en **Importar**.

La importación o exportación de datos de un archivo de copia de seguridad de HP Client Security puede realizarse a través de los vínculos asociados (en **Otras opciones)** en la página de importación y exportación.

NOTA: Este recurso importa y exporta solo los datos de Password Manager. Si desea información sobre la copia de seguridad y la restauración de datos de HP Client Security adicionales, consulte Copias de seguridad y restauración de sus datos en la página 29.

Para importar datos de un archivo de copia de seguridad de HP Client Security:

1. En la página de importación y exportación de HP Password Manager, haga clic o pulse en **Importar datos de un archivo de copia de seguridad de HP Client Security**.
2. Verifique su identidad.
3. Seleccione el archivo de copia de seguridad creado previamente o introduzca la ruta en el campo correspondiente y luego haga clic en **Examinar**.
4. Introduzca la contraseña utilizada para proteger el archivo y luego haga clic o pulse en **Siguiente**.
5. Haga clic o pulse en **Restaurar**.

Para exportar datos a un archivo de copia de seguridad de HP Client Security:

1. En la página de importación y exportación de HP Password Manager, haga clic o pulse en **Exportar datos a un archivo de copia de seguridad de HP Client Security**.
2. Verifique su identidad y luego haga clic o pulse en **Siguiente**.
3. Introduzca un nombre para el archivo de copia de seguridad. De forma predeterminada, el archivo se guarda en su carpeta de Documentos. Para especificar una ubicación diferente, haga clic o pulse en **Examinar**.
4. Introduzca y confirme una contraseña para proteger el archivo y luego haga clic o pulse en **Guardar**.

Configuración

Puede especificar la configuración para personalizar el Password Manager:

- **Solicitud para agregar inicios de sesión para las pantallas de inicio de sesión**: el icono del **Password Manager** con un signo más aparece cada vez que se detecta una pantalla de inicio de sesión de un sitio web o programa, lo que indica que puede agregar un inicio de sesión para esta pantalla en el menú **Inicios de sesión**.

  A fin de desactivar este recurso, desmarque la casilla de verificación junto a **Solicitud para agregar inicios de sesión en las pantallas de inicio de sesión**.

- **Abrir Password Manager con Ctrl+Win+h**: la tecla de acceso rápido predeterminada que abre el menú de **Vínculos rápidos de Password Manager** es Ctrl+tecla de Windows+h.

  Para cambiar la tecla de acceso rápido, haga clic o pulse 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.

  No se pueden utilizar combinaciones reservadas para Windows o aplicaciones de Windows.

- Para regresar a los valores de las configuraciones predeterminadas, haga clic o pulse en **Restaurar valores predeterminados**.

Configuración avanzada

Los administradores pueden activar o desactivar las siguientes opciones seleccionando el icono **Engranaje** (configuración) en la pantalla de inicio de HP Client Security.

- **Políticas de administrador**: le permite configurar las políticas de inicio de sesión y sesión para administradores.
- **Políticas de usuario estándar**: le permite configurar las políticas de inicio de sesión y sesión para usuarios estándar.
- **Recursos de seguridad**: le permite aumentar la seguridad de su equipo protegiendo su cuenta de Windows mediante autenticación sólida y/o activando la autenticación antes del arranque de Windows.
- **Usuarios**: le permite administrar usuarios y sus credenciales.
- **Mis políticas**: le permite revisar sus políticas de autenticación y el estado de registro.
- **Copia de seguridad y restauración**: le permite realizar copias de seguridad o restaurar datos de HP Client Security.
- **Acerca de HP Client Security**: muestra información de la versión de HP Client Security.

Políticas de administrador

Puede configurar las políticas de inicio de sesión y sesión para administradores de este equipo. Las políticas de inicio de sesión que se establecen aquí rigen las credenciales requeridas para que un administrador local inicie sesión en Windows. Las políticas de sesión que se establecen aquí rigen las credenciales requeridas para que un administrador local verifique la identidad en una sesión de Windows.

De forma predeterminada, todas las políticas nuevas o cambiadas se aplican inmediatamente después de pulsar o hacer clic en **Aplicar**.

Para agregar una nueva política:

1. En la página de inicio de HP Client Security, haga clic o pulse en el icono **Engranaje**.
2. En la página de configuración avanzada, haga clic o pulse en **Políticas de administrador**.
3. Haga clic o pulse en **Agregar nueva política**.
4. Haga clic en las flechas hacia abajo para seleccionar las credenciales principal y secundaria (opcional) para la nueva política y luego haga clic o pulse en **Agregar**.
5. Haga clic en **Aplicar**.

Para retrasar la aplicación de una política nueva o cambiada:

1. Haga clic o pulse en **Aplicar esta política inmediatamente**.
2. Seleccione **Aplicar esta política en la fecha específica**.
3. Introduzca una fecha o utilice el calendario desplegable para seleccionar una fecha en la que debería aplicarse esta política.
4. Si lo desea, seleccione cuándo se recordará a los usuarios la nueva política.
5. Haga clic en **Aplicar**.

Políticas de usuario estándar

Puede configurar las políticas de inicio de sesión y sesión para usuarios estándar de este equipo. Las políticas de inicio de sesión que se establecen aquí rigen las credenciales requeridas para que un usuario estándar inicie sesión en Windows. Las políticas de sesión que se establecen aquí rigen las credenciales requeridas para que un usuario estándar verifique la identidad en una sesión de Windows.

De forma predeterminada, todas las políticas nuevas o cambiadas se aplican inmediatamente después de pulsar o hacer clic en **Aplicar**.

Para agregar una nueva política:

1. En la página de inicio de HP Client Security, haga clic o pulse en el icono **Engranaje**.
2. En la página de configuración avanzada, haga clic o pulse en **Políticas de usuario estándar**.
3. Haga clic o pulse en **Agregar nueva política**.
4. Haga clic en las flechas hacia abajo para seleccionar las credenciales principal y secundaria (opcional) para la nueva política y luego haga clic o pulse en **Agregar**.
5. Haga clic en **Aplicar**.

Para retrasar la aplicación de una política nueva o cambiada:

1. Haga clic o pulse en **Aplicar esta política inmediatamente**.
2. Seleccione **Aplicar esta política en la fecha específica**.
3. Introduzca una fecha o utilice el calendario desplegable para seleccionar una fecha en la que debería aplicarse esta política.
4. Si lo desea, seleccione cuándo se recordará a los usuarios la nueva política.
5. Haga clic en **Aplicar**.

Recursos de seguridad

Puede activar los recursos de seguridad de HP Client Security que sirven de protección contra el acceso no autorizado al equipo.

Para configurar los recursos de seguridad:

1. En la página de inicio de HP Client Security, haga clic o pulse en el icono **Engranaje**.
2. En la página de configuración avanzada, haga clic o pulse en **Recursos de seguridad**.
3. Active los recursos de seguridad seleccionando sus casillas de verificación y luego haga clic o pulse en **Aplicar**. Cuantos más recursos seleccione, más seguro estará su equipo.

   Esta configuración se aplica a todos los usuarios.

   - **Seguridad de inicio de sesión en Windows**: protege sus cuentas de Windows al requerir el uso de credenciales de HP Client Security para su acceso.
   - **Seguridad de preinicio (autenticación de inicio)**: protege su equipo antes del inicio de Windows. Esta opción no está disponible si el BIOS no es compatible.
   - **Permitir el inicio de sesión en un paso**: este ajuste permite omitir el inicio de sesión de Windows si la autenticación se realizó previamente al nivel de autenticación de inicio o Drive Encryption.
4. Haga clic o pulse en **Usuarios** y luego haga clic o pulse en el mosaico del usuario.

Usuarios

Puede supervisar y administrar a los usuarios de HP Client Security de este equipo.

Para agregar otro usuario de Windows a HP Client Security:

1. En la página de inicio de HP Client Security, haga clic o pulse en el icono **Engranaje**.
2. En la página de configuración avanzada, haga clic o pulse en **Usuarios**.
3. Haga clic o pulse en **Agregar otro usuario de Windows a HP Client Security**.
4. Introduzca el nombre del usuario que desee agregar y haga clic o pulse en **Aceptar**.
5. Introduzca la contraseña de Windows del usuario.

   Se mostrará un mosaico del usuario agregado en la página de usuario.

Para eliminar un usuario de Windows de HP Client Security:

1. En la página de inicio de HP Client Security, haga clic o pulse en el icono **Engranaje**.
2. En la página de configuración avanzada, haga clic o pulse en **Usuarios**.
3. Haga clic o pulse en el nombre del usuario que desee eliminar.
4. Haga clic o pulse en **Eliminar usuario** y luego haga clic o pulse en **Sí** para confirmar.

Para mostrar un resumen de las políticas de inicio de sesión y sesión aplicadas a un usuario:

▲ Haga clic o pulse en **Usuarios** y luego haga clic o pulse en el mosaico del usuario.

Mis políticas

Puede mostrar sus políticas de autenticación y el estado de registro. La página Mis políticas también incluye vínculos a las páginas Políticas de administradores y Políticas de usuario estándar.

1. En la página de inicio de HP Client Security, haga clic o pulse en el icono **Engranaje**.
2. En la página de configuración avanzada, haga clic o pulse en **Mis políticas**.

   Se mostrarán las políticas de inicio de sesión y sesión aplicadas al usuario que ha iniciado sesión.

La página Mis políticas también incluye vínculos a Políticas de administrador en la página 26 y Políticas de usuario estándar en la página 27.

Copias de seguridad y restauración de sus datos

Se recomienda efectuar copias de seguridad de sus datos de HP Client Security 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, debería 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: Solo se pueden realizar copias de seguridad de Password Manager con este recurso. 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 Client Security debe estar instalado en cualquier equipo que deba recibir copias de seguridad de datos antes de que los datos puedan restaurarse desde el archivo de copia de seguridad.

Para realizar una copia de seguridad de sus datos:

1. En la página de inicio de HP Client Security, haga clic o pulse en el icono **Engranaje**.
2. En la página de configuración avanzada, haga clic o pulse en **Políticas de administrador**.
3. Haga clic o pulse en **Copia de seguridad y restaurar**.
4. Haga clic o pulse en **Copia de seguridad** y luego verifique su identidad.
5. Seleccione el módulo que desee incluir en la copia de seguridad y luego haga clic o pulse en **Siguiente**.
6. Introduzca un nombre para el archivo de almacenamiento. De forma predeterminada, el archivo se guarda en su carpeta de Documentos. Para especificar una ubicación diferente, haga clic o pulse en **Examinar**.
7. Introduzca y confirme una contraseña para proteger el archivo.
8. Haga clic o pulse en **Guardar**.

Para restaurar sus datos:

1. En la página de inicio de HP Client Security, haga clic o pulse en el icono **Engranaje**.
2. En la página de configuración avanzada, haga clic o pulse en **Políticas de administrador**.
3. Haga clic o pulse en **Copia de seguridad y restaurar**.
4. Seleccione **Restaurar** y luego verifique su identidad.

5. Seleccione el archivo de almacenamiento que se creó anteriormente. Introduzca la ruta en el campo proporcionado. Para especificar una ubicación diferente, haga clic o pulse en **Examinar**.
6. Introduzca la contraseña utilizada para proteger el archivo y luego haga clic o pulse en **Siguiente**.
7. Seleccione los módulos para los cuales desea restaurar los datos.
8. Haga clic o pulse en **Restaurar**.

5 HP Drive Encryption (solo en algunos modelos)

HP Drive Encryption brinda una completa protección de datos mediante la encriptación de los datos de su equipo. Cuando Drive Encryption está activado, debe iniciar sesión en la pantalla de inicio de sesión de Drive Encryption que aparece antes de que se inicie el sistema operativo Windows®.

La pantalla inicial de HP Client Security permite a los administradores de Windows activar Drive Encryption, hacer una copia de seguridad de la clave de encriptación y seleccionar o anular la selección de unidades o particiones para encriptación. Para obtener más información, consulte la ayuda del software HP Client Security.

Es posible realizar las siguientes tareas con Drive Encryption:

- Selección de las configuraciones de Drive Encryption:
  - 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: Sólo 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 abriendo HP Client Security.

1. En la pantalla de Inicio, haga clic o toque la aplicación **HP Client Security** (Windows 8).

   – o –

   En el escritorio de Windows, haga doble clic o pulse dos veces en el icono de **HP Client Security** en el área de notificación, en el extremo derecho de la barra de tareas.

2. Haga clic o pulse en el icono de **Drive Encryption**.

Tareas generales

Activación de Drive Encryption para unidades de disco duro estándares

Las unidades de disco duro estándar se encriptan por medio de software de encriptación. Siga estos pasos para encriptar una unidad o partición de disco:

1. Inicie **Drive Encryption**. Para obtener más información, consulte Apertura de Drive Encryption en la página 31.
2. Seleccione la casilla de verificación de la unidad o partición que desee encriptar y haga clic o pulse en **Copia de seguridad de la clave**.

NOTA: Para mejorar la seguridad, seleccione la casilla de verificación **Desactivar el modo de suspensión para mayor seguridad**. Cuando se desactiva el modo de suspensión, no hay absolutamente ningún riesgo de que las credenciales usadas para desbloquear la unidad se guarden en la memoria.

3. Seleccione una o más de las opciones de copia de seguridad y luego haga clic o pulse en **Copia de seguridad**. Para obtener más información, consulte Copias de seguridad de claves de encriptación en la página 35.
4. Puede continuar trabajando mientras se realiza una copia de seguridad de la clave de encriptación. No reinicie su equipo.

NOTA: Se le solicita que reinicie el equipo. Después del reinicio, se muestra la pantalla de pre-inicio de encriptación de la unidad, 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 Client Security.

Activación de Drive Encryption para unidades de autoencriptación

Las unidades de autoencriptación que cumplen la especificación OPAL de Trusted Computing Group para la administración de unidades de autoencriptación pueden encriptarse mediante el uso de la encriptación por software o por hardware. La encriptación por hardware es mucho más rápida que la encriptación por software. Sin embargo, no puede escoger qué particiones del disco encriptar. Se encripta el disco completo, incluidas las particiones.

Para encriptar particiones específicas, debe usar la encriptación por software. Asegúrese de desmarcar la casilla de verificación **Permitir la encriptación por hardware solo para unidades con autoencriptación (SED)**.

Siga estos pasos a fin de activar Drive Encryption para unidades de autoencriptación:

1. Inicie **Drive Encryption**. Para obtener más información, consulte Apertura de Drive Encryption en la página 31.
2. Seleccione la casilla de verificación de la unidad que desee encriptar y haga clic o pulse en **Copia de seguridad de la clave**.

NOTA: Para mejorar la seguridad, seleccione la casilla de verificación **Desactivar el modo de suspensión para mayor seguridad**. Cuando se desactiva el modo de suspensión, no hay absolutamente ningún riesgo de que las credenciales usadas para desbloquear la unidad se guarden en la memoria.

3. Seleccione una o más de las opciones de copia de seguridad y luego haga clic o pulse en **Copia de seguridad**. Para obtener más información, consulte Copias de seguridad de claves de encriptación en la página 35.

4. Puede continuar trabajando mientras se realiza una copia de seguridad de la clave de encriptación. No reinicie su equipo.

NOTA: En las unidades con autoencriptación, se le pedirá que apague el equipo:

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

Desactivación de Drive Encryption

1. Inicie **Drive Encryption**. Para obtener más información, consulte Apertura de Drive Encryption en la página 31.

2. Desmarque la casilla de verificación de todas las unidades encriptadas y luego haga clic o pulse en **Aplicar**.

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

NOTA: 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 por hardware ofrece la opción **Desactivar el modo de suspensión para mayor seguridad**, que evita la suspensión o el modo en 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 preinicio en el BIOS en HP Client Security y si 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 o el PIN de smart card, ingrese a SpareKey, o bien deslice un dedo con la huella digital 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 luego haga clic o pulse 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

- 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.

Encriptación de unidades de disco duro adicionales

Se recomienda enfáticamente que utilice HP Drive Encryption para proteger sus datos mediante la encriptación de la unidad de disco duro. Después de la activación, se puede encriptar cualquier unidad de disco duro agregada o partición creada al seguir estos pasos:

1. Inicie **Drive Encryption**. Para obtener más información, consulte Apertura de Drive Encryption en la página 31.
2. 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 Drive Encryption para ver y cambiar el estado de encriptación (No encriptado o Encriptado) de todas las unidades de disco duro del equipo.

- 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 encriptado (para unidades adicionales)

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

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

1. Inicie **Drive Encryption**. Para obtener más información, consulte Apertura de Drive Encryption en la página 31.
2. En **Estado de la unidad**, seleccione o anule la selección de la casilla de verificación que está al lado de cada partición de disco duro que desee encriptar o desencriptar y luego haga clic o pulse en **Aplicar**.

NOTA: Cuando una partición se encripta o desencripta, una barra de progreso muestra el porcentaje de partición encriptada.

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.

Administración de discos

- **Sobrenombre**: puede dar nombres a las unidades o particiones para facilitar su identificación.
- **Unidades desconectadas**: Drive Encryption puede hacer un seguimiento de las unidades que se eliminan del equipo. Un disco que se elimina del equipo se traslada automáticamente a la lista Desconectados. Si el disco vuelve al sistema, aparecerá de nuevo en la lista Conectados.
- Si ya no necesita hacer un seguimiento o administrar la unidad desconectada, puede eliminar la unidad desconectada de la lista Desconectados.
- Drive Encryption se mantiene activado hasta que se desmarquen las casillas de verificación de todas las unidades conectadas y la lista Desconectados esté vacía.

Copias de seguridad y recuperación (tarea del 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.

1. Inicie **Drive Encryption**. Para obtener más información, consulte Apertura de Drive Encryption en la página 31.
2. Seleccione la casilla de verificación de una unidad y luego haga clic o pulse en **Copia de seguridad de la clave**.
3. En **Crear clave de recuperación de HP Drive Encryption**, seleccione una o más de las opciones siguientes:
   - **Almacenamiento extraíble**: Seleccione la casilla de verificación y luego seleccione el dispositivo de almacenamiento en el que se guardó la clave de encriptación.
   - **SkyDrive**: seleccione la casilla de verificación. Debe estar conectado a Internet. Inicie sesión en Microsoft SkyDrive y luego haga clic o pulse en **Sí**.

     NOTA: Para utilizar la clave de copia de seguridad de HP Drive Encryption que está almacenada en SkyDrive, debe descargarla de SkyDrive a un dispositivo de almacenamiento extraíble y luego insertar el dispositivo de almacenamiento en este equipo.
   - **TPM** (solo algunos modelos): le permite recuperar sus datos utilizando su contraseña TPM.

     PRECAUCIÓN: Si el TPM se elimina o el equipo está dañado, perderá el acceso a la copia de seguridad. Si se selecciona este método, debe seleccionarse también otro método de copia de seguridad.
4. Haga clic o pulse en **Copia de seguridad**.

   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 **Copia de seguridad de la clave** en Drive Encryption.

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 en HP Drive Encryption, haga clic o pulse en **Recuperación**.
4. Introduzca la ruta de archivo o el nombre que contiene su clave de copia de seguridad y luego haga clic o pulse en **Recuperar**.
5. Cuando se abra el cuadro de diálogo de confirmación, haga clic o pulse 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 HP Client Security.

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

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

NOTA: Si el SpareKey no se ha inicializado en HP Client Security, 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 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.

6 HP File Sanitizer (solo en algunos modelos)

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

File Sanitizer no se puede usar para sanitizar ni purificar los siguientes tipos de unidades.

- Unidades de estado sólido (SSD), como volúmenes RAID que abarcan un dispositivo SSD
- Unidades externas conectadas por USB, Firewire o interfaz eSATA

Si se intenta hacer una operación de trituración o purificación en una unidad SSD, se muestra un mensaje de advertencia y no se realiza la operación.

Eliminación definitiva

La trituración es diferente de una acción de eliminación estándar de Windows®. Cuando tritura un activo con File Sanitizer, los archivos se sobrescriben con datos insignificantes, lo que hace prácticamente imposible recuperar el activo original. Una acción de eliminación simple de Windows puede dejar el archivo (o activo) intacto en la unidad de disco duro o en un estado en el que podrían utilizarse métodos forenses para recuperarlo.

Puede programar una hora de trituración futura o puede activar manualmente la trituración seleccionando el icono de **File Sanitizer** en la pantalla inicial de HP Client Security o utilizando el icono de **File Sanitizer** del escritorio de Windows. Para obtener más información, consulte Configuración de una programación de trituración en la página 40, Trituración haciendo clic con el botón derecho en la página 42 o Inicio manual de una operación de trituración en la página 42.

NOTA: Un archivo .dll se tritura y elimina del sistema sólo si ha sido movido a la Papelera de reciclaje.

Limpieza para liberar espacio

La eliminación de un activo en Windows no elimina completamente el contenido del activo de su unidad de disco duro. Windows sólo elimina la referencia al activo o su ubicación en la unidad de disco duro. El contenido del activo permanece en la unidad de disco duro hasta que otro activo sobrescriba la misma zona en la unidad de disco duro con información nueva.

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

NOTA: El blanqueamiento de espacio libre no ofrece seguridad adicional para los activos triturados.

Puede programar una hora de blanqueamiento de espacio libre futura o puede activar manualmente el blanqueamiento de espacio libre seleccionando el icono de **File Sanitizer** en la pantalla inicial de HP Client Security o utilizando el icono de **File Sanitizer** del escritorio de Windows. Para obtener más información, consulte Configuración de una programación de purificación de espacio libre en la página 41, Inicio manual de blanqueamiento de espacio libre en la página 43 o Uso del icono de File Sanitizer en la página 42.

Apertura de File Sanitizer

1. En la pantalla de Inicio, haga clic o toque la aplicación **HP Client Security** (Windows 8).

   – o –

   En el escritorio de Windows, haga doble clic o pulse dos veces en el icono de **HP Client Security** en el área de notificación, en el extremo derecho de la barra de tareas.

2. En **Datos**, haga doble clic o pulse en **File Sanitizer**.

o

▲ Haga doble clic o pulse dos veces en el icono de **File Sanitizer** en el escritorio de Windows.

– o –

▲ Haga clic con el botón derecho o mantenga pulsado el icono de **File Sanitizer** en el escritorio de Windows, y luego seleccione **Abrir File Sanitizer**.

Procedimientos de configuración

Trituración: File Sanitizer elimina o tritura de forma segura las categorías de activos seleccionadas.

1. En **Trituración**, seleccione la casilla de verificación de cada tipo de archivo que se va a triturar o desmarque la casilla de verificación si no desea triturar esos archivos.
   - **Papelera de reciclaje**: tritura todos los elementos de la papelera de reciclaje.
   - **Archivos temporales del sistema**: tritura todos los archivos que se encuentran en la carpeta temporal del sistema. Las siguientes variables del entorno se buscan en el orden que sigue y la primera ruta encontrada se considera la carpeta del sistema:
     - TMP
     - TEMP
   - **Archivos temporales de Internet**: tritura las copias de páginas web, imágenes y medios guardados por los navegadores web para una visualización más rápida.
   - **Cookies**: tritura todos los archivos almacenados en un equipo por los sitios web para guardar preferencias, como información de inicio de sesión.
2. Para iniciar la trituración, haga clic o pulse en **Triturar**.

Blanqueamiento: escribe datos aleatorios en el espacio libre y evita la recuperación de los archivos eliminados.

▲ Para iniciar el blanqueamiento, haga clic o pulse en **Blanquear**.

Opciones de File Sanitizer: seleccione la casilla de verificación para activar cada una de las siguientes opciones, o desmarque la casilla de verificación para desactivar una opción:

- **Activar icono de escritorio**: muestra el icono de File Sanitizer en el escritorio de Windows.
- **Activar clic con el botón derecho**: le permite hacer clic con el botón derecho o tocar y mantener pulsado un activo y luego seleccionar **HP File Sanitizer – Triturar**.

- **Solicitar contraseña de Windows antes de la trituración manual**: solicita la autenticación con la contraseña de Windows antes de triturar manualmente un elemento.
- **Triturar cookies y archivos temporales de Internet al cerrar el explorador**: tritura todos los activos seleccionados relacionados con Internet, como el historial de sitios visitados, al cerrar un explorador web.

Configuración de una programación de trituración

Puede programar una hora para realizar la trituración automáticamente o también puede triturar activos manualmente en cualquier momento. Para obtener más información, consulte Procedimientos de configuración en la página 39.

1. Abra File Sanitizer y luego haga clic o pulse en **Configuración**.
2. Para programar una hora futura para triturar los activos seleccionados, en **Programa de trituración**, seleccione **Nunca**, **Una vez**, **Diariamente**, **Semanalmente** o **Mensualmente** y luego seleccione un día y una hora:
   a. Haga clic o pulse en la hora, el minuto o el campo AM/PM.
   b. Desplácese hasta que aparezca el valor deseado al mismo nivel que los otros campos.
   c. Haga clic o pulse en el espacio blanco que rodea los campos de la hora.
   d. Repita el proceso con cada campo hasta que se haya seleccionado el programa correcto.
3. Se mostrarán los cuatro tipos de activos siguientes:
   - **Papelera de reciclaje**: tritura todos los elementos de la papelera de reciclaje.
   - **Archivos temporales del sistema**: tritura todos los archivos que se encuentran en la carpeta temporal del sistema. Las siguientes variables del entorno se buscan en el orden que sigue y la primera ruta encontrada se considera la carpeta del sistema:
     - TMP
     - TEMP
   - **Archivos temporales de Internet**: tritura las copias de páginas web, imágenes y medios guardados por los navegadores web para una visualización más rápida.
   - **Cookies**: tritura todos los archivos almacenados en un equipo por los sitios web para guardar preferencias, como información de inicio de sesión.

   Si está marcada, estos activos se triturarán a la hora programada.
4. Para seleccionar activos personalizados adicionales que se triturarán:
   a. En **Lista de trituración programada**, haga clic o pulse en **Agregar carpeta** y luego navegue hasta el archivo o carpeta.
   b. Haga clic o pulse en **Abrir** y luego haga clic o pulse en **Aceptar**.

   Para eliminar un activo de la lista de trituración programada, desmarque la casilla de verificación de ese activo.

Configuración de una programación de purificación de espacio libre

El blanqueamiento de espacio libre no ofrece seguridad adicional para los activos triturados.

1. Abra File Sanitizer y luego haga clic o pulse en **Configuración**.
2. Para programar una hora futura para blanquear su unidad de disco duro, en **Programa de blanqueamiento**, seleccione **Nunca**, **Una vez**, **Diariamente**, **Semanalmente** o **Mensualmente** y luego seleccione un día y una hora:
   a. Haga clic o pulse en la hora, el minuto o el campo AM/PM.
   b. Desplácese hasta que aparezca la hora deseada al mismo nivel que los otros campos.
   c. Haga clic o pulse en el espacio blanco que rodea los campos de la hora.
   d. Repita el proceso hasta que se haya seleccionado el programa correcto.

NOTA: La operación de purificación de espacio libre puede llevar un plazo de tiempo considerable. Asegúrese de que su equipo esté conectado a una fuente de alimentación de CA. Si bien la purificación de espacio libre se realiza en segundo plano, un mayor uso del procesador puede afectar el rendimiento de su equipo. La purificación de espacio libre se puede realizar fuera del horario de servicio o cuando el equipo no esté en uso.

Protección de archivos de la trituración

Para proteger los archivos o carpetas de la trituración:

1. Abra File Sanitizer y luego haga clic o pulse en **Configuración**.
2. En **Lista de no triturar nunca**, haga clic o pulse en **Agregar carpeta** y luego navegue hasta el archivo o carpeta.
3. Haga clic o pulse en **Abrir** y luego haga clic o pulse en **Aceptar**.

NOTA: Los archivos de esta lista se encuentran protegidos mientras están en la lista.

Para eliminar un activo de la lista de exclusiones, desmarque la casilla de verificación de ese activo.

Tareas generales

Utilice File Sanitizer para realizar las siguientes tareas:

- **Usar el icono de File Sanitizer para iniciar la trituración**: arrastre archivos al icono de **File Sanitizer** en el escritorio de Windows. Para obtener detalles, consulte Uso del icono de File Sanitizer en la página 42.
- **Trituración manual de un activo específico o todos los activos seleccionados**: triture elementos en cualquier momento sin esperar la hora de trituración programada. Para obtener detalles, consulte Trituración haciendo clic con el botón derecho en la página 42 o Inicio manual de una operación de trituración en la página 42.
- **Activar manualmente la purificación de espacio libre**: active la purificación de espacio libre en cualquier momento. Para obtener detalles, consulte Inicio manual de blanqueamiento de espacio libre en la página 43.
- **Ver los archivos de registro**: vea los archivos de registro de la trituración y de la purificación de espacio libre, que contiene errores o fallas de la última operación de trituración o de purificación de espacio libre. Para obtener detalles, consulte Visualización de los archivos de registro en la página 43.

NOTA: La operación de eliminación definitiva o de limpieza para liberar espacio en disco puede tardar considerablemente. Aunque la trituración y la purificación de espacio libre se realizan en segundo plano, el aumento del uso del procesador puede afectar el rendimiento de su equipo.

Uso del icono de File Sanitizer

PRECAUCIÓN: Los elementos que han sido triturados no se pueden recuperar. Piense detenidamente qué elementos selecciona para la trituración manual.

Cuando inicie una operación de trituración manualmente, la lista de trituración estándar de la vista de File Sanitizer se triturará (consulte Procedimientos de configuración en la página 39).

Puede iniciar manualmente una operación de trituración de las formas siguientes:

1. Abra File Sanitizer (consulte Apertura de File Sanitizer en la página 39) y luego haga clic o pulse en **Triturar**.
2. Cuando se abra el cuadro de diálogo de confirmación, asegúrese de que los activos que desea triturar están marcados y luego haga clic o pulse en **Aceptar**.

– o –

1. Haga clic con el botón derecho o mantenga pulsado el icono de **File Sanitizer** en el escritorio de Windows, y luego seleccione **Triturar ahora**.
2. Cuando se abra el cuadro de diálogo de confirmación, asegúrese de que los activos que desea triturar están marcados y luego haga clic o pulse en **Triturar**.

Trituración haciendo clic con el botón derecho

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

Si se ha seleccionado **Activar trituración con el botón derecho** en la vista de File Sanitizer view, se puede triturar un activo de la forma siguiente:

1. Navegue hasta el documento o carpeta que desee triturar.
2. Haga clic con el botón derecho o mantenga pulsado el archivo o la carpeta y seleccione **HP File Sanitizer – Triturar**.

Inicio manual de una operación de trituración

PRECAUCIÓN: Los elementos que han sido triturados no se pueden recuperar. Piense detenidamente qué elementos selecciona para la trituración manual.

Cuando inicie una operación de trituración manualmente, la lista de trituración estándar de la vista de File Sanitizer se triturará (consulte Procedimientos de configuración en la página 39).

Puede iniciar manualmente una operación de trituración de las formas siguientes:

1. Abra File Sanitizer (consulte Apertura de File Sanitizer en la página 39) y luego haga clic o pulse en **Triturar**.
2. Cuando se abra el cuadro de diálogo de confirmación, asegúrese de que los activos que desea triturar están marcados y luego haga clic o pulse en **Aceptar**.

– o –

1. Haga clic con el botón derecho o mantenga pulsado el icono de **File Sanitizer** en el escritorio de Windows, y luego seleccione **Triturar ahora**.
2. Cuando se abra el cuadro de diálogo de confirmación, asegúrese de que los activos que desea triturar están marcados y luego haga clic o pulse en **Triturar**.

Inicio manual de blanqueamiento de espacio libre

Cuando inicie una operación de blanqueamiento manualmente, la lista de trituración estándar de la vista de File Sanitizer se blanqueará (consulte Procedimientos de configuración en la página 39).

Puede iniciar manualmente una operación de blanqueamiento de las formas siguientes:

1. Abra File Sanitizer (consulte Apertura de File Sanitizer en la página 39) y luego haga clic o pulse en **Blanquear**.
2. Cuando se abra el cuadro de diálogo de confirmación, haga clic o pulse en **Aceptar**.

– o –

1. Haga clic con el botón derecho o mantenga pulsado el icono de **File Sanitizer** en el escritorio de Windows, y luego seleccione **Blanquear ahora**.
2. Cuando se abra el cuadro de diálogo de confirmación, haga clic o pulse en **Blanquear**.

Visualización de los archivos de registro

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

NOTA: Los archivos que se trituraron o purificaron no aparecen en el registro de archivos.

Se crea un archivo de registro para las operaciones de trituración y otro archivo de registro para las operaciones de purificación de espacio libre. Ambos archivos de registro se encuentran en las siguientes carpetas de la unidad de disco duro:

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

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

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

7 HP Device Access Manager (solo en algunos modelos)

HP 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 48.

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

- Se crean perfiles de dispositivos para cada usuario con el fin de definir los dispositivos a los cuales se permite o se deniega el acceso.
- La autenticación Just In Time (JITA, Just In Time Authentication) permite a los usuarios predefinidos autenticarse con el fin de acceder a los dispositivos a los que por lo general se deniega el acceso.
- Es posible excluir a los administradores y usuarios de confianza de las restricciones sobre el acceso a dispositivos que impone Device Access Manager agregándolos al grupo de Administradores de dispositivos. La pertenencia a este grupo se administra con la Configuración avanzada.
- Se puede conceder o negar el acceso a los dispositivos en base a la pertenencia a un grupo o por usuarios individuales.
- En el caso de clases de dispositivos como unidades de CD-ROM y unidades de DVD, se puede permitir o negar el acceso a la lectura y el acceso a la escritura por separado.

HP Device Access Manager se configura automáticamente con los siguientes ajustes durante la ejecución del asistente de configuración de HP Client Security Setup Wizard:

- Just In Time Authentication (JITA) Removable Media está habilitado para Administradores y Usuarios.
- La política de dispositivos permite el acceso total a otros dispositivos.

Apertura de Device Access Manager

1. En la pantalla de Inicio, haga clic o toque la aplicación **HP Client Security** (Windows 8).

   – o –

   En el escritorio de Windows, haga doble clic o pulse dos veces en el icono de **HP Client Security** en el área de notificación, en el extremo derecho de la barra de tareas.

2. En **Dispositivo**, haga doble clic o pulse en **Permisos del dispositivo**.

   - Los usuarios estándar pueden ver su acceso al dispositivo actual (consulte Vista del usuario en la página 45).
   - Los administradores pueden ver y hacer cambios en el acceso al dispositivo que está configurado actualmente para el equipo haciendo clic o pulsando en **Cambiar** y luego introduciendo la contraseña de administrador (consulte Vista del sistema en la página 45).

Vista del usuario

Cuando se selecciona **Permisos del dispositivo**, aparecerá la vista del usuario. En función de la política, los usuarios estándar y los administradores pueden ver su propio acceso para clases de dispositivos o dispositivos individuales en este equipo.

- **Usuario actual**: aparecerá el nombre del usuario que ha iniciado sesión actualmente.
- **Clase de dispositivos**: aparecerán los tipos de dispositivos.
- **Acceso**: aparecerá su acceso a tipos de dispositivos o dispositivos específicos configurado actualmente.
- **Duración**: aparecerá el límite de tiempo de su acceso a unidades de CD/DVD-ROM o unidades de disco extraíbles.
- **Configuración**: los administradores pueden cambiar qué dispositivos tienen el acceso controlado por Device Access Manager.

Vista del sistema

En la vista del sistema, los administradores pueden permitir o denegar el acceso a dispositivos en este equipo para el grupo Usuarios o el grupo Administradores.

▲ Los administradores puede acceder a la vista del sistema haciendo clic o pulsando en **Cambiar**, introduciendo la contraseña de administrador y luego seleccionando entre las opciones siguientes:

- **Device Access Manager**: para iniciar HP Device Access Manager con Just In Time Authentication activada o desactivada, haga clic o pulse en **Activada** o **Desactivada**.
- **Usuarios y grupos en este equipo**: muestra el grupo Usuarios o el grupo Administradores que tiene permitido o denegado el acceso a las clases de dispositivos seleccionados.
- **Clase 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. Para expandir la lista, haga clic en el icono **+**. Se muestran todos los dispositivos conectados al

equipo y los grupos Administradores y Usuarios se expanden para mostrar quién pertenece a ellos. Para actualizar la lista de dispositivos, haga clic en el icono redondo de flecha (actualizar).

- La protección se aplica generalmente a una clase de dispositivo. Si el acceso se ajusta en **Permitir**, el usuario o grupo seleccionado será capaz de acceder a cualquier dispositivo de esa clase de dispositivos.
- La protección también se puede aplicar a dispositivos específicos.
- 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. Para obtener más información, consulte Configuración de JITA en la página 46.
- Permita o deniegue el acceso a otras clases de dispositivos, como medios extraíbles (por ejemplo unidades flash USB), puertos en serie y paralelos, dispositivos Bluetooth®, dispositivos módem, dispositivos PCMCIA/ExpressCard, dispositivos 1394, lector de huellas digitales y lector de smart card. Si se deniegan el lector de huellas digitales y el lector de smart card, se pueden utilizar como credenciales de autenticación, pero no se pueden utilizar al nivel de política de sesión.

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.

- Cuando seleccione un ajuste en el nivel de Grupo o Clase de dispositivos y se le pregunte si desea aplicar el ajuste a los objetos secundarios:

  Sí: el ajuste se propagará.

  No: el ajuste no se propagará.
- 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.

NOTA: El grupo Administradores no puede agregarse a la Lista de usuarios.

- **Acceso**: haga clic o pulse en la flecha hacia abajo y luego seleccione uno de los siguientes tipos de acceso para permitir o denegar el acceso:
  - **Permitir: acceso total**
  - **Permitir: solo lectura**
  - **Permitir: se requiere JITA**: para obtener más información, consulte Configuración de JITA en la página 46.

    Si se selecciona este tipo de acceso, en **Duración**, haga clic o pulse en la flecha hacia abajo para seleccionar un límite de tiempo.
  - **Denegar**
- **Duración**: haga clic o pulse en la flecha hacia abajo para seleccionar un límite de tiempo para el acceso a unidades de CD/DVD-ROM o unidades de disco extraíble (consulte Configuración de JITA en la página 46).

Configuración de JITA

La Configuración de JITA permite que el administrador vea y modifique las listas de usuarios y grupos a los que se les permite acceder a los dispositivos mediante Just In Time Authentication (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 dispositivos**.

El período de JITA puede autorizarse para una cantidad establecida de minutos o ilimitado. Los usuarios ilimitados tendrán acceso al dispositivo desde el momento en que se autentiquen hasta el momento en que apaguen el sistema.

Si el usuario tiene un periodo de JITA limitado, un minuto antes de que expire el periodo de JITA, se le preguntará al usuario si desea ampliar el acceso. En cuanto el usuario cierre sesión en el sistema u otro usuario inicie sesión, el periodo 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
- Unidades de disco extraíbles

Creación de una política de 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 (JITA)

1. Inicie **Device Access Manager** y luego haga clic o pulse en **Cambiar**.
2. Seleccione el usuario o el grupo y luego, en **Acceso**para **Unidades de disco extraíble** o **Unidades de DVD/CD-ROM**, haga clic o pulse en la flecha hacia abajo y luego seleccione **Permitir: se requiere JITA**.
3. En **Duración**, haga clic o pulse en la flecha hacia abajo para seleccionar un periodo de tiempo para el acceso con JITA.

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

Desactivación de una política de JITA para un usuario o un grupo

Los Administradores pueden desactivar el acceso de un usuario o grupo a los dispositivos mediante Just In Time Authentication.

1. Inicie **Device Access Manager** y luego haga clic o pulse en **Cambiar**.
2. Seleccione el usuario o el grupo y luego, en **Acceso**para **Unidades de disco extraíble** o **Unidades de DVD/CD-ROM**, haga clic o pulse en la flecha hacia abajo y luego seleccione **Denegar**.

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

Configuración

La vista **Configuración** permite a los administradores ver y cambiar las unidades que tienen el acceso controlado por Device Access Manager.

NOTA: Device Access Manager deben estar activado cuando se configure la lista de las letras de las unidades. (consulte Vista del sistema en la página 45).

Clases de dispositivos no administrados

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

- Dispositivos de entrada/salida
  - CD-ROM
  - Unidad de disco
  - Controlador de disco flexible (FDC)
  - Controlador de disco duro (HDC)
  - Clase de dispositivo de interfaz humana (HID)
  - Dispositivos infrarrojos de interfaz humana
  - Mouse
  - Múltiples puertos en serie
  - Teclado
  - Impresoras Plug and Play (PnP)
  - Impresora
  - Actualización de impresora
- Alimentación eléctrica
  - Soporte de administración de energía avanzada (APM)
  - Batería
- Varios
  - PC
  - Decodificador
  - Pantalla
  - Controlador de pantalla unificado Intel®
  - Legacard
  - Controlador de medios
  - Alterador de medios
  - Tecnología de memoria
  - Monitor
  - Multifunción
  - Cliente de red
  - Servicio de red
  - Transporte de red
  - Procesador
  - Adaptador del SCSI

- Acelerador de seguridad
- Dispositivos de seguridad
- Sistema
- Desconocido
- Volumen
- Instantánea de volumen

8 HP Trust Circles

HP Trust Circles es un archivo y una aplicación de seguridad de documentos, que combina encriptación de archivos y carpetas con capacidad de compartir documentos en un círculo de confianza. La aplicación encripta archivos ubicados en carpetas especificadas por el usuario, protegiéndolas dentro de un círculo de confianza. Una vez protegidos, los archivos solo pueden ser utilizados y compartidos por miembros del círculo de confianza. Si algún no miembro recibe un archivo protegido, el archivo permanece encriptado y el no miembro no podrá acceder a los contenidos.

Apertura de Trust Circles

1. En la pantalla de inicio, haga clic o pulse en la aplicación **HP Client Security**.

   – o –

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

2. En **Datos**, haga clic o pulse en **Trust Circles**.

Pasos iniciales

Hay dos maneras de enviar invitaciones por correo electrónico y de responder a ellas:

- **Uso de Microsoft® Outlook**: el uso de Trust Circles con Microsoft Outlook automatiza el procesamiento de las invitaciones y respuestas de Trust Circle de otros usuarios de Trust Circle.
- **Uso de Gmail, Yahoo, Outlook.com u otros servicios de correo electrónico (SMTP)**: al introducir su nombre, dirección de correo electrónico y contraseña, Trust Circles utiliza su servicio de correo electrónico para enviar invitaciones por correo electrónico a los miembros seleccionados para unirse a su círculo de confianza.

Para configurar su perfil básico:

1. Introduzca su nombre y su dirección de correo electrónico y luego haga clic o pulse en **Siguiente**.

   El nombre es visible para cualquier miembro que sea invitado a su círculo de confianza. La dirección de correo electrónico se utiliza para enviar, recibir o responder a invitaciones.

2. Introduzca la contraseña utilizada para la cuenta de correo electrónico y luego haga clic o pulse en **Siguiente**.

   Se enviará un correo electrónico de prueba para asegurarse que la configuración de correo electrónico es correcta.

   NOTA: El equipo debe estar conectado a una red.

3. En el campo **Nombre de Trust Circle**, introduzca un nombre para el círculo de confianza y luego haga clic o pulse en **Siguiente**.

4. Agregue miembros y carpetas y luego haga clic o pulse en **Siguiente**. Se crea el círculo de confianza con las carpetas seleccionadas y envía invitaciones por correo electrónico a los

miembros seleccionados. Si, por cualquier motivo, no se puede enviar una invitación, se muestra una notificación. Los miembros pueden ser invitados de nuevo en cualquier momento desde la vista de Trust Circle haciendo clic en **Sus Trust Circles** y luego haciendo clic o pulsando dos veces en el círculo de confianza. Para obtener más información, consulte Trust Circles en la página 51.

Trust Circles

Puede crear un círculo de confianza durante la configuración inicial después de introducir su dirección de correo electrónico, o en la vista de Trust Circle:

▲ En la vista de Trust Circle haga clic o pulse en **Crear Trust Circle** y luego introduzca el nombre del círculo de confianza.

- Para agregar miembros al círculo de confianza, haga clic o pulse en el icono **M+** que está junto a **Miembros** y luego siga las instrucciones que aparecen el pantalla.
- Para agregar carpetas al círculo de confianza, haga clic o pulse en el icono **+** que está junto a **Carpetas** y luego siga las instrucciones que aparecen el pantalla.

Agregar carpetas a un círculo de confianza

Agregar carpetas a un nuevo círculo de confianza:

- Durante la creación de un círculo de confianza, puede agregar carpetas haciendo clic o pulsando en el icono **+** que está junto a **Carpetas**y luego siguiendo las instrucciones que aparecen en la pantalla.

  – o –

- En el Explorador de Windows, haga clic con el botón derecho o mantenga pulsada una carpeta que actualmente no forme parte de un círculo de confianza, seleccione **Trust Circle** y luego seleccione **Crear Trust Circle desde carpeta**.

SUGERENCIA: Puede seleccionar una o más carpetas.

Agregar carpetas a un círculo de confianza existente:

- En la vista de Trust Circle, haga clic en **Sus Trust Circles**, haga doble clic o pulse dos veces en el círculo de confianza existente para mostrar las carpetas actuales, haga clic o pulse el icono **+** que está junto a **Carpetas** y luego siga las instrucciones que aparecen en pantalla.

  – o –

- En el Explorador de Windows, haga clic con el botón derecho o mantenga pulsada una carpeta que actualmente no forme parte de un círculo de confianza, seleccione **Trust Circle** y luego seleccione **Agregar a Trust Circle existente desde carpeta**.

SUGERENCIA: Puede seleccionar una o más carpetas.

Una vez que se haya agregado una carpeta a un círculo de confianza, Trust Circles encripta la carpeta y sus contenidos automáticamente. Cuando todos los archivos estén encriptados, se mostrará una notificación. Además, aparecerá un símbolo de candado verde sobre todos los iconos de carpeta y los iconos de archivo encriptados indicando que están totalmente protegidos.

Agregar miembros a un círculo de confianza

Para agregar miembros a un círculo de confianza se requieren tres pasos:

1. **Invitar**: en primer lugar, el propietario del círculo de confianza invita a los miembros. El correo electrónico de invitación puede enviarse a múltiples usuarios o listas/grupos de distribución.
2. **Aceptar**: el invitado recibe la invitación y decide si la acepta o la rechaza. Si el invitado acepta la invitación, se envía una respuesta por correo electrónico a la persona que le ha invitado. Si la invitación se ha enviado a un grupo, cada miembro recibe una invitación y decide si la acepta o la rechaza.
3. **Registrar**: la persona que invita tiene una última oportunidad de decidir si agrega al miembro al círculo de confianza. Si la persona que invita decide registrar al miembro, se envía un correo electrónico al invitado acusando recibo de la respuesta. La persona que invita y el invitado pueden verificar opcionalmente la seguridad del proceso de invitación. Aparecerá un código de invitación para el incitado, que se debe leer a la persona que invita por teléfono. Una vez que se haya verificado el código, la persona que invita puede enviar el correo electrónico de registro final.

Agregar miembros a un nuevo círculo de confianza:

▲ Durante la creación de un círculo de confianza, puede agregar miembros haciendo clic o pulsando en el icono **M+** que está junto a **Miembros**y luego siguiendo las instrucciones que aparecen en la pantalla.

- Si está utilizando Outlook, seleccione contactos de la agenda de Outlook y luego haga clic en **Aceptar**
- Si está utilizando otro servicio de correo electrónico, agregue las nuevas direcciones de correo electrónico manualmente al Trust Circle o puede recuperarlas de la dirección de correo electrónico registrada en Trust Circle.

Agregar miembros a un círculo de confianza existente:

▲ En la vista de Trust Circle, haga clic en **Sus Trust Circles**, haga doble clic o pulse dos veces en el círculo de confianza existente para mostrar los miembros actuales, haga clic o pulse el icono **M+** que está junto a **Miembros** y luego siga las instrucciones que aparecen en pantalla.

- Si está utilizando Outlook, seleccione contactos de la agenda de Outlook y luego haga clic en **Aceptar**.
- Si está utilizando otro servicio de correo electrónico, agregue las nuevas direcciones de correo electrónico manualmente al Trust Circle o puede recuperarlas de la dirección de correo electrónico registrada en Trust Circle

Agregar archivos a un círculo de confianza

Puede agregar archivos a un círculo de confianza de una de las formas siguientes:

- Copie o traslade el archivo a una carpeta del círculo de confianza existente.

  – o –

- En el Explorador de Windows, haga clic con el botón derecho o mantenga pulsado un archivo que actualmente no esté encriptado, seleccione **Trust Circle** y luego seleccione **Encriptar**. Se le pedirá que seleccione el círculo de confianza al que debe agregarse el archivo.

SUGERENCIA: Puede seleccionar uno o más archivos.

Carpetas encriptadas

Cualquier miembro de un círculo de confianza puede ver y editar archivos que pertenezcan a ese círculo de confianza.

NOTA: El Trust Circle Manager/Reader no sincroniza archivos entre los miembros.

Los archivos deben compartirse por los medios existentes, como por ejemplo correo electrónico, ftp o proveedores de almacenamiento en la nube. Los archivos copiados a, trasladados a, o creados dentro de un círculo de confianza se protegen automáticamente.

Eliminación de carpetas de un círculo de confianza

Al eliminar una carpeta de un círculo de confianza se desencripta la carpeta y todos sus contenidos y se le quita la protección.

- En la vista de Trust Circle, haga clic o pulse en **Sus Trust Circles**, haga doble clic o pulse dos veces en el círculo de confianza existente para mostrar las carpetas actuales y luego haga clic o pulse en el icono de **papelera** que está junto a esa carpeta.

  – o –

- En el Explorador de Windows, haga clic con el botón derecho o mantenga pulsada una carpeta que actualmente forme parte de un círculo de confianza, seleccione **Trust Circle** y luego seleccione **Eliminar de Trust Circle**.

SUGERENCIA: Puede seleccionar una o más carpetas.

Eliminación de un archivo de un círculo de confianza

Para eliminar un archivo de un círculo de confianza, en el Explorador de Windows, haga doble clic o mantenga pulsado un archivo que no esté encriptado actualmente, seleccione **Trust Circle** y luego **Desencriptar archivo**.

Eliminación de miembros de un círculo de confianza

Un miembro que se haya registrado completamente no se puede eliminar de un círculo de confianza. Una alternativa sería crear un nuevo círculo de confianza con todos los demás miembros, trasladar todos los archivos y carpetas al nuevo círculo de confianza y eliminar el círculo de confianza anterior. Esto garantizará que todos los nuevos archivos que reciba el miembro no serán accesibles, pero cualquier cosa que se haya compartido previamente seguirá siendo accesible para el miembro del círculo de confianza anterior.

Si un miembro no está totalmente registrado (ha sido invitado a unirse al círculo de confianza o no ha aceptado la invitación al círculo de confianza), puede eliminarlo del círculo de confianza de una de las siguientes formas:

- En la vista de Trust Circle, haga clic o pulse en **Sus Trust Circles** y luego haga doble clic o pulse dos veces en el círculo de confianza para mostrar la lista actual de miembros. Haga clic o pulse en el icono de **papelera** junto al nombre del miembro que se va a eliminar.
- En la vista de Trust Circle, haga clic o pulse en **Miembros** y luego haga doble clic o pulse dos veces en el miembro para mostrar los círculos de confianza a los que pertenece. Haga clic o pulse en el icono de **papelera** junto al círculo de confianza para eliminar al miembro de ese círculo de confianza .

Eliminación de un círculo de confianza

Para eliminar un círculo de confianza, es necesario ser el propietario del mismo.

▲ En la vista de Trust Circle, haga clic o pulse en **Sus Trust Circles** y luego haga clic o pulse en el icono de **papelera** junto al círculo de confianza que se va a eliminar.

De este modo se elimina en círculo de confianza de la página y se envían correos electrónicos a todos los miembros informándoles de que el círculo de confianza se ha eliminado. Los archivos o carpetas que estaban incluidos en esa círculo de confianza se desencriptan.

Configuración de preferencias

En la vista de Trust Circle, haga clic o pulse en **Preferencias**. Aparecerán tres fichas

- **Configuración de correo electrónico**

Opción	Descripción
Nombre de usuario	Se muestra el nombre de usuario que se está utilizando actualmente. Para cambiarlo, introduzca un nuevo nombre de usuario en el cuadro de diálogo Los cambios se guardan automáticamente.
Dirección de correo electrónico.	Se muestra la cuenta de correo electrónico que se está utilizando actualmente Para cambiarla, haga clic o pulse en **Cambiar configuración de correo electrónico** y siga las instrucciones que aparecen en pantalla.
Confirmación de nuevo miembro	Seleccione una de las opciones siguientes: ◦ **Confirmar automáticamente**: después de recibir la aceptación de los invitados, estos se confirman en el círculo de confianza sin necesidad de hacer nada y se envía un correo electrónico de confirmación a los invitados. ◦ **Confirmar manualmente**: después de recibir la aceptación de los invitados, es necesario introducir datos manualmente para registrar a los nuevos miembros en el círculo de confianza y luego se envía un correo electrónico de confirmación a los invitados. ◦ **Requerir verificación**: después de recibir la aceptación de los invitados, se requiere un código de verificación para registrar totalmente a los invitados. El propietario del círculo de confianza debe contactar con los invitados y obtener de ellos el código de verificación. Después de introducir el código correcto, se envían los correos electrónicos de confirmación.
Autenticación periódica	La autenticación periódica requiere que el usuario introduzca la contraseña de Windows después del intervalo de espera especificado (registrado en minutos) y también mientras se realizan operaciones sensibles. Este ajuste permite a los usuarios activar o desactivar la autenticación.
Intervalo de espera de autenticación	Seleccione el intervalo de espera especificado (registrado en minutos) antes de que se exija la autenticación.
No mostrar el mensaje de confirmación	Seleccione la casilla de verificación para no mostrar mensajes de confirmación o desmárquela para mostrar mensajes de confirmación.
Me gustaría ayudar a mejorar HP Trust Circle a través del seguimiento de uso anónimo	Seleccione la casilla de verificación para participar en el programa o desmárquela si no desea participar.

- **Copia de seguridad/restaurar**

Opción	Descripción
Copias de seguridad	Copia los datos de la aplicación Trust Circle Manager/Reader (configuraciones y círculos de confianza) a un archivo de copia de seguridad. En caso de fallo del sistema puede utilizar este archivo para restaurar su nueva instalación de Trust Circles al estado guardado en el archivo. **NOTA:** Solo se guardan los datos de su aplicación Trust Circle (círculos de confianza, configuraciones y miembros). No se hará una copia de seguridad de los archivos reales de las carpetas del círculo de confianza. Debería hacerse una copia de seguridad de esos archivos por separado. Para hacer una copia de seguridad de las configuraciones y datos de usuario de Trust Circle: **1.** Haga clic o pulse en **Copia de seguridad**. **2.** Elija un nombre de archivo y un directorio para el archivo de copia de seguridad y luego haga clic o pulse en **Guardar**. **3.** Introduzca una contraseña, confírmela y luego haga clic o pulse en **Aceptar**. Esta contraseña será necesaria para restaurar este archivo.
Restauración	Restaura las configuraciones y los círculos de confianza desde un archivo de copia de seguridad, normalmente después de un fallo del sistema o una migración a otro equipo. Para restaurar los ajustes y datos de usuario de Trust Circle Manager: **1.** Haga clic o pulse en **Restaurar**. **2.** Navegue hasta el directorio y el nombre de archivo del archivo de copia de seguridad y luego haga clic o pulse en **Abrir**. **3.** Introduzca la contraseña que se configuró mientras se hacía la copia de seguridad.

- **Acerca de**: se muestra la versión del software Trust Circle Manager/Reader. Se muestran vínculos que le permiten actualizar Trust Circle manager a la versión Pro o ver la declaración de privacidad de HP.

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

Computrace (se adquiere por separado) le permite supervisar, administrar y rastrear su equipo de manera remota.

Una vez activado, Computrace se configura desde el Centro de Clientes de Absolute Software. Desde el Centro de Clientes, el administrador puede configurar Computrace para supervisar o administrar el equipo. Si el sistema se extravía o lo roban, el Centro de Clientes puede ayudar a las autoridades locales a ubicar y recuperar el equipo. Si se lo configura, Computrace puede continuar funcionando incluso si alguien roba o sustituye la unidad de disco duro.

Para activar Computrace:

1. Conéctese a Internet.
2. Abra HP Client Security. Para obtener más información, consulte Apertura de HP Client Security en la página 9.
3. Haga clic en **Recuperación contra 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 acerca de Computrace.

10 Excepciones de la contraseña localizada

La localización de la contraseña no es del todo compatible a nivel de autenticación de inicio y de HP Drive Encryption. Para obtener más información, consulte Los IME de Windows no son compatibles a nivel de autenticación de inicio o a nivel de Drive Encryption en la página 57.

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. Abra HP Client Security y luego introduzca la contraseña de Windows.

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

  1. Cambie la contraseña de Windows para que utilice solo caracteres admitidos. Para obtener más información sobre caracteres no admitidos, consulte Manejo de teclas especiales en la página 58.
  2. Abra HP Client Security y luego introduzca la contraseña de Windows.

Los IME de Windows no son compatibles a nivel de autenticación de inicio o a nivel de 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 autenticación de inicio o de Drive Encryption. No puede introducirse una contraseña de Windows con un IME en la autenticación de inicio la pantalla de inicio de sesión 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 utilizan 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 se asigna un IME a una disposición del teclado compatible, HP Client Security puede admitir la configuración.

¡ADVERTENCIA! Cuando se implemente HP Client Security, 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 utilizando la página de usuarios de HP Client Security (a la que se accede desde el icono **Engranaje**de la página de inicio) para eliminar el usuario de HP Client Security, al seleccionar la disposición del teclado deseada en el sistema operativo y luego volver a ejecutar el asistente de configuración de HP Client Security para el mismo usuario. El BIOS guarda la disposición del teclado deseada y las contraseñas que pueden escribirse 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 los mismos caracteres. Por ejemplo, tanto la disposición del teclado Internacional (EE.UU.) (20409) como 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, la disposición del teclado Latinoamericano se configura 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 introduce una contraseña (por ejemplo, abcdef), debe introducir 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 autenticación de inicio 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 introduce una contraseña, debe introducir 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 autenticación de inicio y HP Drive Encryption.

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

Language (Idioma)	Windows	BIOS	Drive Encryption
Árabe	Las teclas ﻻ ,ﻷ, y ﻹ generan dos caracteres.	Las teclas ﻻ ,ﻷ, y ﻹ generan un carácter.	Las teclas ﻻ ,ﻷ, y ﻹ generan un carácter.
Francés canadiense	ç, è, à, y é con bloq mayús son Ç, È, À y É en Windows.	ç, è, à, y é con bloq mayús son ç, è, à, y é en la autenticación de inicio.	ç, è, à, y é con bloq mayús son ç, è, à, y é en HP Drive Encryption.

Language (Idioma)	Windows	BIOS	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)	◦ Se rechazan las teclas ¡, ¤, ‘, ’, ¥, y × en la fila superior. ◦ Se rechazan las teclas å, ®, y Þ en la segunda fila. ◦ Se rechazan las teclas á, ð, y ø en la tercera fila. ◦ Se rechaza la tecla æ en la fila inferior.	n/a	n/a
Checo	◦ Se rechaza la tecla ğ. ◦ Se rechaza la tecla į. ◦ Se rechaza la tecla ų. ◦ Se rechazan las teclas ė, ı, y ż. ◦ Se rechazan las teclas ģ, ķ, ļ, ņ, y ţ.	n/a	n/a
Eslovaco	Se rechaza la tecla ż.	◦ Se rechazan las teclas š, ś, y ş al escribirse, pero se aceptan cuando se introducen mediante el teclado en pantalla. ◦ La tecla inactiva ţ genera dos caracteres.	n/a
Húngaro	Se rechaza la tecla ż.	La tecla ţ genera dos caracteres.	n/a
Esloveno	La tecla żŻ se rechaza en Windows y la tecla alt genera una tecla inactiva en el BIOS.	Se rechazan las teclas ú, Ú, ů, Ů, ş, Ş, ś, Ś, š, y Š en el BIOS.	n/a
Japanese	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 que se debe completar antes de que se pueda acceder a los recursos de Drive Encryption. Los administradores pueden activar Drive Encryption mediante el asistente de configuración de HP Client Security o HP Client Security. El proceso de activación consiste en activar el software, encriptar la unidad y crear la clave de encriptación de copia de seguridad inicial 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 que usted es la persona que dice ser, a través del uso de credenciales, incluida la contraseña de Windows, su huella digital, una smart card, una tarjeta sin contactos o una tarjeta de proximidad.

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.

Autenticación Just In Time
Consulte la ayuda del software HP Device Access Manager.

Autenticación preinicio 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, o deben deslizar un dedo cuya huella digital esté registrada. Si se ha seleccionado el inicio de sesión en un paso, entonces la introducción de la información correcta en la pantalla de inicio de sesión de Drive Encryption le permitirá acceder directamente a Windows sin tener que volver a realizar el inicio de sesión en la pantalla de inicio de sesión de Windows.

Bluetooth
Tecnología que utiliza transmisiones de radio para activar equipos, impresoras, mouse, teléfonos móviles y otros dispositivos compatibles con Bluetooth para comunicación inalámbrica a corta distancia.

Carpeta de Trust Circle
Cualquier carpeta protegida por un círculo de confianza.

Chip de seguridad incorporado de Módulo de plataforma segura (TPM)
Un TPM autentica un equipo, más que un usuario, al almacenar información específica del sistema host, tal como claves de encriptación, certificados digitales y contraseñas. Un TPM minimiza el riesgo de que se acceda sin autorización a la información que se encuentra en el equipo, por ejemplo mediante un robo físico o el ataque de un hacker externo.

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

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.

credencial
Una información o un dispositivo de hardware específico utilizado para autenticar a un usuario individual.

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
Un usuario que está autorizado a iniciar sesión en una red o un equipo individual.

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

dispositivo conectado
Un dispositivo de hardware que está conectado a un puerto del equipo.

Dominio
Un grupo de equipos que forman parte de una red y comparten una base de datos de directorio común. Los dominios tienen un nombre único y cada uno tiene una serie de normas y procedimientos comunes.

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

DriveLock
Un recurso de seguridad que vincula la unidad de disco duro a un usuario y requiere que el usuario introduzca correctamente la contraseña de DriveLock cuando se inicia el equipo.

Eliminación definitiva
La ejecución de un algoritmo que sobrescribe los datos contenidos en un activo con datos insignificantes.

Eliminación definitiva automática
Trituración que usted programa en File Sanitizer.

Eliminación definitiva manual
Trituración inmediata de un activo o activos seleccionados, que se adelanta a una trituración programada.

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.

encriptación de hardware
El uso de unidades de autoencriptación que cumplan con la especificación OPAL de Trusted Computing Group en relación con la administración de unidades de autoencriptación para completar una encriptación instantánea. La encriptación de hardware es instantánea y puede tardar sólo unos cuantos minutos, pero la encriptación de software puede tardar varias horas.

encriptación de software
El uso de software para encriptar la unidad de disco duro sector a sector. Este proceso es más lento que la encriptación por hardware

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
Un extracto digital de la imagen de su huella digital. La imagen real de su huella digital nunca es almacenada por HP Client Security.

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

Inicio de sesión
Un objeto dentro de HP Client Security 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.

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

Página de inicio.
Una ubicación central donde puede acceder y administrar los recursos y la configuración de HP Client Security.

Pantalla de inicio de sesión de Drive Encryption
Permite ver la autenticación preinicio de Drive Encryption.

PIN
Número de identificación personal de un usuario registrado que se utiliza para la autenticación.

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.

purificación de espacio libre
La escritura de datos aleatorios en activos eliminados y espacio sin usar. Este procedimiento disminuye la existencia del activo eliminado, de modo que sea más difícil recuperar el activo original.

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 HP Client Security 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.

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

Smart card
Un dispositivo de hardware que puede utilizarse con un PIN para la autenticación.

Tarjeta de ID
Un gadget de escritorio de Windows que sirve para identificar visualmente su escritorio con su nombre de usuario e imagen elegida.

tarjeta de proximidad
Una tarjeta de plástico que contiene un chip de computación que se puede usar para autenticación en conjunto con otras credenciales para mayor seguridad.

tarjeta sin contactos
Una tarjeta de plástico que contiene un chip de computación que puede utilizarse para la autenticación.

Trust Circle
Proporciona contención de datos vinculando los datos a un grupo definido de usuarios de confianza. Esto impide que los datos caigan en malas manos de forma accidental o intencionada. Protegidos con la tecnología Zero Overhead Key Management de CryptoMill, los datos se vinculan criptográficamente a un círculo de confianza. Esto evita la desencriptación de documentos u otra información sensible fuera del círculo de confianza

Trust Circle Manager/Reader
Trust Circle Reader solo puede aceptar invitaciones enviadas por los usuarios de Trust Circle. Sin embargo, Trust Circle Manager permite la creación de círculos de confianza. Los recursos incluyen invitar a alguien a través del correo electrónico a un círculo de confianza y aceptar invitaciones a círculos de confianza de otros. Una vez que se establece un círculo de confianza entre homólogos, los archivos protegidos por ese círculo de confianza se pueden compartir con seguridad.

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