HP ProtectTools
Guía del usuario

Primera edición: junio de 2008

Número de referencia del documento: 481201-E51

Tabla de contenido

1 Introducción a la seguridad

El software HP ProtectTools Security Manager proporciona recursos de seguridad que sirven de protección contra el acceso no autorizado al equipo, a la red y a los datos más importantes. La funcionalidad de seguridad optimizada se suministra a través de los siguientes módulos de software:

- Credential Manager for HP ProtectTools
- Drive Encryption for HP ProtectTools (sólo en algunos modelos)
- Privacy Manager for HP ProtectTools (sólo en algunos modelos)
- File Sanitizer for HP ProtectTools
- BIOS Configuration for HP ProtectTools
- Embedded Security for HP ProtectTools (sólo en algunos modelos)
- Device Access Manager for HP ProtectTools (sólo en algunos modelos)

Los módulos de software disponibles para su equipo pueden variar según el modelo. Por ejemplo, Embedded Security for HP ProtectTools está disponible únicamente para los equipos en los que está instalado el chip Trusted Platform Module (TPM) de Embedded Security.

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

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

Recursos de HP ProtectTools

La siguiente tabla detalla los recursos clave de los módulos de HP ProtectTools:

Módulo	Recursos clave
Credential Manager for HP ProtectTools	• Credential Manager actúa como una bóveda de contraseña personal, optimizando el proceso de Single Sign On (Inicio de sesión único), que recuerda y aplica automáticamente las credenciales del usuario. • Single Sign On también ofrece protección adicional al requerir combinaciones de diferentes tecnologías de seguridad, como Java™ Card y biometría, para la autenticación del usuario. • El almacenamiento de la contraseña se encuentra protegido mediante encriptación de software y puede optimizarse a través del uso del chip de seguridad integrado TPM y/o de autenticación de un dispositivo de seguridad, como una Java Card o biometría.
Drive Encryption for HP ProtectTools (sólo en algunos modelos)	• Drive Encryption suministra una encriptación completa del volumen total de la unidad de disco duro. • Drive Encryption exige autenticación de preinicio para desencriptar y acceder a los datos.
Privacy Manager for HP ProtectTools (sólo en algunos modelos)	• Privacy Manager utiliza técnicas de inicio de sesión avanzadas para verificar la fuente, la integridad y la seguridad de las comunicaciones cuando se utiliza correo electrónico, documentos de Microsoft® Office o mensajería instantánea (IM).
File Sanitizer for HP ProtectTools	• File Sanitizer le permite eliminar definitivamente de forma segura activos digitales (información sensible que incluye archivos de aplicación, contenido histórico o relacionado con la web u otros datos confidenciales) de su equipo y limpiar periódicamente la unidad de disco duro.
BIOS Configuration for HP ProtectTools	• BIOS Configuration le brinda acceso a la administración de contraseñas de encendido de usuario y de administrador. • BIOS Configuration proporciona una alternativa a la utilidad de configuración BIOS de preinicio, conocida también como Computer Setup. • La activación de DriveLock automático, optimizado con el chip de seguridad integrado, por parte de BIOS Configuration ayuda a proteger una unidad de disco duro del acceso no autorizado, incluso si se la retira de un sistema, sin requerir que el usuario recuerde ninguna contraseña adicional además de la contraseña de usuario del chip de seguridad integrado.

Módulo	Recursos clave
Embedded Security for HP ProtectTools (sólo en algunos modelos)	• Embedded Security utiliza un chip Trusted Platform Module (TPM) de Embedded Security para ayudar a proteger contra el acceso no autorizado a datos sensibles del usuario o a credenciales almacenadas localmente en un PC. • Embedded Security permite la creación de una unidad personal segura (PSD), que es útil para proteger la información de los archivos y las carpetas del usuario. • Embedded Security admite aplicaciones de otros fabricantes (como Microsoft Outlook e Internet Explorer) para operaciones de certificados digitales protegidos.
Device Access Manager for HP ProtectTools (sólo en algunos modelos)	• Device Access Manager permite que los gerentes de TI controlen el acceso a los dispositivos según los perfiles de usuarios. • Device Access Manager evita que usuarios no autorizados eliminen datos utilizando medios de almacenamiento externo y que introduzcan virus en el sistema desde medios externos. • El administrador puede desactivar el acceso a los dispositivos grabables para personas o grupos de usuarios específicos.

Acceso a HP ProtectTools Security

Para acceder a HP ProtectTools Security Manager desde el Panel de control de Windows®:

1. En Windows Vista®, haga clic en **Inicio** y luego en **HP ProtectTools Security Manager for Administrators**.

   – o –

   En Windows XP, haga clic en **Inicio**, **Todos los programas** y entonces en **HP ProtectTools Security Manager**.

   NOTA: Si usted no es un administrador de HP Protect Tools, puede ejecutar HP Protect Tools en modo para no administradores para ver información, pero no podrá realizar cambios.

2. En el panel izquierdo, haga clic en **HP ProtectTools** y entonces en **Getting Started** (Pasos iniciales).

3. Haga clic en el botón **Security Manager Setup** (Configuración de Security Manager), debajo del icono del escudo de HP Protect Tools, para iniciar el asistente de Security Manager.

   Aparecerá la siguiente pantalla:

- El asistente de instalación guía al administrador del sistema operativo Windows a través de la configuración de los niveles de seguridad y de los métodos de inicio de sesión seguros que se utilizan en un entorno de preinicio, en Credential Manager y en Drive Encryption.
- Los usuarios también emplean el asistente de configuración para configurar sus métodos de inicio de sesión seguros.

NOTA: Para acceder a cada módulo de HP Protect Tools para confiigurar más recursos poderosos, haga clic en el icono del módulo.

NOTA: Después de haber configurado el módulo Credential Manager, también es posible abrir HP ProtectTools iniciando la sesión directamente en Credential Manager desde la pantalla de inicio de sesión de Windows. Para obtener más información, consulte “Inicio de sesión en Windows con Credential Manager en la página 17.”

Cómo lograr los objetivos clave de seguridad

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

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

Protección contra robo dirigido

Un ejemplo de este tipo de incidente sería el robo dirigido de un equipo que contiene datos confidenciales e información del cliente en un control de seguridad de un aeropuerto. Los siguientes recursos ayudan a proteger contra el robo dirigido:

- El recurso de autenticación preinicio, si está activado, ayuda a evitar el acceso al sistema operativo. Vea los siguientes procedimientos:
  - Credential Manager
  - Embedded Security
  - Drive Encryption
- DriveLock ayuda a asegurar que no se pueda acceder a sus datos, incluso si la unidad de disco duro es retirada e instalada en un sistema inseguro.
- El recurso Unidad personal segura, provisto por el módulo Embedded Security for HP ProtectTools, encripta datos sensibles para ayudar a garantizar que no se pueda acceder sin autenticación. Vea los siguientes procedimientos:
  - Embedded Security “Procedimientos de configuración en la página 74”
  - “Uso de la unidad segura personal (PSD) en la página 76”

Restricción de acceso a datos sensibles

Suponga que un auditor contratado está trabajando en el lugar y se le otorgó acceso al equipo para revisar datos financieros sensibles; usted no desea que el auditor pueda imprimir los archivos o guardarlos en un dispositivo grabable, como un CD. Los recursos siguientes ayudan a restringir el acceso a los datos:

- Device Access Manager for HP ProtectTools permite que los gerentes de TI restrinjan el acceso a los dispositivos grabables de modo tal que la información sensible no pueda imprimirse ni copiarse desde la unidad de disco duro a los medios extraíbles. Consulte “Configuración de clases de dispositivos (avanzado) en la página 82.”
- DriveLock ayuda a asegurar que no se pueda acceder a sus datos, incluso si la unidad de disco duro es retirada e instalada en un sistema inseguro.

Prevención de acceso no autorizado desde ubicaciones internas o externas

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

- El recurso de autenticación preinicio, si está activado, ayuda a evitar el acceso al sistema operativo. Vea los siguientes procedimientos:
  - Credential Manager
  - Embedded Security
  - Drive Encryption
- Embedded Security for HP ProtectTools ayuda a proteger datos sensibles del usuario o credenciales almacenadas localmente en un PC con los siguientes procedimientos:
  - Embedded Security “Procedimientos de configuración en la página 74”
  - “Uso de la unidad segura personal (PSD) en la página 76”
- Con los siguientes procedimientos, Credential Manager for HP ProtectTools ayuda a garantizar que un usuario no autorizado no pueda obtener las contraseñas ni acceder a las aplicaciones protegidas con contraseña:
  - Credential Manager - “Procedimientos de configuración en la página 12”
  - “Uso del Single Sign On (Inicio de sesión único) en la página 18”
- Device Access Manager for HP ProtectTools permite que los gerentes de TI restrinjan el acceso a los dispositivos grabables de modo tal que la información sensible no pueda copiarse desde la unidad de disco duro. Consulte “Configuración sencilla en la página 81.”
- El recurso Unidad personal segura encripta los datos sensibles para ayudar a garantizar que no se pueda acceder sin autenticación con los siguientes procedimientos:
  - Embedded Security - “Procedimientos de configuración en la página 74”
  - “Uso de la unidad segura personal (PSD) en la página 76”

Creación de políticas de contraseñas fuertes

Si se implementa una orden que exige el uso de una política firme de contraseñas para docenas de aplicaciones y bases de datos basadas en la Web, Credential Manager for HP ProtectTools proporciona un repositorio protegido para las contraseñas y la comodidad de Single Sign On (Inicio de sesión único) con los siguientes procedimientos:

- Credential Manager - “Procedimientos de configuración en la página 12”
- “Uso del Single Sign On (Inicio de sesión único) en la página 18”

Para una seguridad más sólida, Embedded Security for HP ProtectTools protege dicho repositorio de nombres de usuario y contraseñas. Esto permite que los usuarios mantengan múltiples contraseñas firmes sin tener que escribirlas ni intentar recordarlas. Vea Embedded Security - “Procedimientos de configuración en la página 74.”

Elementos de seguridad adicionales

Asignación de las funciones de seguridad

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

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

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

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

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

- Administrador de TI—Aplica y administra los recursos de seguridad definidos por el oficial de seguridad. También puede activar o desactivar algunos recursos. Por ejemplo, si el oficial de seguridad ha decidido implementar Java Card, el administrador de TI puede activar el modo de seguridad de Java Card en el BIOS.

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

Administración de contraseñas de HP ProtectTools

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

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

Contraseña de HP ProtectTools	Definida en este módulo de HP ProtectTools	Función
Contraseña de inicio de sesión de Credential Manager	Credential Manager	Esta contraseña ofrece dos opciones: • Puede ser utilizada en un inicio de sesión separado para acceder a Credential Manager después de iniciar la sesión de Windows. • Puede utilizarse en lugar del proceso de inicio de sesión de Windows, posibilitando el acceso a Windows y a Credential Manager simultáneamente.
Contraseña de archivo de recuperación de Credential Manager	Credential Manager, por el administrador de TI	Protege el acceso al archivo de recuperación de Credential Manager.

Contraseña de HP ProtectTools	Definida en este módulo de HP ProtectTools	Función
Contraseña de clave de usuario básico **NOTA:** También conocida como Contraseña de Embedded Security	Embedded Security	Utilizada para acceder a los recursos de Embedded Security, por ejemplo correo electrónico seguro, encriptación de archivos y carpetas. Cuando se utiliza para realizar la autenticación de inicio, también protege el acceso al contenido del equipo cuando éste se inicia, se reinicia o sale de la hibernación.
Contraseña de token de recuperación de emergencia **NOTA:** También conocida como Contraseña de clave de token de recuperación de emergencia	Embedded Security, por el administrador de TI	Protege el acceso al token de recuperación de emergencia, que es un archivo de copia de seguridad para el chip embedded security.
Contraseña de propietario	Embedded Security, por el administrador de TI	Protege al sistema y al chip TPM contra el acceso no autorizado a todas las funciones de propietario de Embedded Security.
PIN de Java™ Card	Java Card Security	Protege contra el acceso al contenido de la Java Card y autentica a los usuarios de la Java Card. Cuando se utiliza para realizar autenticación de inicio, el PIN de Java Card también protege contra el acceso a la utilidad de configuración y al contenido del equipo. Autentica los usuarios de Drive Encryption, si se selecciona el token de la Java Card.
Contraseña de configuración del equipo **NOTA:** También conocida como contraseña de administrador de BIOS, configuración f10 o configuración de seguridad	BIOS Configuration, por el administrador de TI	Protege contra el acceso no autorizado a la utilidad de configuración.
Contraseña de inicio	BIOS Configuration	Protege contra el acceso no autorizado al contenido del equipo cuando éste se inicia, se reinicia o sale de la hibernación.
Contraseña de inicio de sesión de Windows	Panel de control de Windows	Puede utilizarse para el inicio de sesión manual o puede guardarse en la Java Card.

Creación de una contraseña segura

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

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

Copia de seguridad y restauración de las credenciales de HP ProtectTools

Para realizar copias de seguridad y restaurar credenciales de todos los módulos HP ProtectTools admitidos, tenga en cuenta lo siguiente:

Creación de copias de seguridad de credenciales y configuración

Puede crear una copia de seguridad de las credenciales de las siguientes maneras:

- Use Drive Encryption for HP ProtectTools para seleccionar y realizar copias de seguridad de las credenciales de HP ProtectTools.

  También puede registrarse en el Servicio de recuperación de clave de encriptación de unidad de disco duro en línea para almacenar una copia de seguridad de su clave de encriptación, lo que le permite acceder a su equipo si se le olvida la contraseña y no tiene acceso a su copia de seguridad local.

  NOTA: Debe estar conectado a Internet y poseer una dirección de correo electrónico válida para registrarse y recuperar su contraseña a través de este servicio.

- Use Embedded Security for HP ProtectTools para realizar copias de seguridad de las credenciales de HP ProtectTools.

2 Credential Manager for HP ProtectTools

Credential Manager for ProtectTools protege contra el acceso no autorizado a su equipo con los siguientes recursos de seguridad:

- Alternativas a contraseñas al iniciar la sesión de Windows, como el uso de una Java Card o un lector biométrico. Para obtener información adicional, consulte “Registro de credenciales en la página 12.”
- Recurso de Single Sign On (Inicio de sesión único) que automáticamente recuerda las credenciales de los sitios Web, aplicaciones y recursos de red protegidos.
- Soporte para dispositivos de seguridad opcionales, como Java Card y lectores biométricos.
- Soporte para configuración de seguridad adicional, como la solicitud de autenticación con un dispositivo de seguridad opcional para desbloquear el equipo.

Procedimientos de configuración

Inicio de sesión en Credential Manager

Dependiendo de la configuración, se puede iniciar la sesión en Credential Manager de cualquiera de las siguientes maneras:

- Icono de HP ProtectTools Security Manager en el área de notificación
- En Windows Vista®, haga clic en **Inicio** y entonces en **HP ProtectTools Security Manager for Administrators**.
- En Windows XP, haga clic en **Inicio** y entonces en **HP ProtectTools Security Manager**.

NOTA: En Windows Vista, debe iniciar HP ProtectTools Security Manager for Administrators para realizar cambios.

Después de iniciar la sesión en Credential Manager, puede registrar credenciales adicionales, como una huella digital o una Java Card. Para obtener información adicional, consulte “Registro de credenciales en la página 12.”

En el próximo inicio de sesión, puede seleccionar la política de inicio de sesión y utilizar cualquier combinación de las credenciales registradas.

Uso del asistente de inicio de sesión de Credential Manager

Para iniciar la sesión en Credential Manager utilizando el asistente de inicio de sesión de Credential Manager:

1. Abra el asistente de inicio de sesión de Credential Manager en una de las siguientes formas:
   - Desde la pantalla de inicio de sesión de Windows
   - En el área de notificación, haga doble clic en el icono **HP ProtectTools Security Manager**
   - Desde la página “Credential Manager” de HP ProtectTools Security Manager, haciendo clic en el enlace **Log On** (Iniciar sesión), en la parte superior derecha de la ventana.
2. Siga las instrucciones en la pantalla para ingresar a Credential Manager.

Registro de credenciales

Es posible utilizar la página “My Identity” (Mi identidad) para registrar los varios métodos de autenticación o credenciales. Después de haberse registrado, puede utilizar estos métodos para iniciar la sesión en Credential Manager.

Registro de huellas digitales

Un lector de huellas digitales permite iniciar sesión en Windows utilizando una huella digital para autenticación, en lugar de utilizar una contraseña de Windows.

Configuración del lector de huellas digitales

1. En HP ProtectTools Security Manager, haga clic en **Credential Manager** en el panel izquierdo.
2. Haga clic en **My Identity** (Mi identidad) y luego en **Register Fingerprints** (Registrar huellas digitales).
3. Siga las instrucciones en pantalla para realizar el registro de sus huellas digitales y configurar el lector de huellas digitales.
4. Para configurar el lector de huellas digitales para un usuario diferente de Windows, inicie la sesión de Windows como ese usuario y luego repita los pasos indicados anteriormente.

Utilice su huella digital registrada para iniciar la sesión en Windows

1. Inmediatamente después de haber registrado sus huellas digitales, reinicie Windows.
2. En la pantalla de bienvenida de Windows, utilice una de sus huellas digitales registradas para iniciar la sesión en Windows.

Registro de Smart Card o Token

Una smart card es una tarjeta plástica del tamaño de una tarjeta de crédito con un microchip incorporado que puede cargarse con información. Las smart card suministran protección de la información y autenticación para usuarios individuales. El inicio de sesión en una red con una smart card ofrece una forma de autenticación sólida que usa identificación con base en criptografía y prueba de posesión al autenticar a un usuario en un dominio.

Un token USB es simplemente una smart card con un formato diferente. En lugar de presentar el chip inteligente en una tarjeta plástica tipo tarjeta de crédito, el chip inteligente se encuentra insertado en un token plástico, también conocido como llave USB. La principal diferencia entre una smart card y un token radica en la interfaz de acceso. Una tarjeta requiere un lector, mientras que un token se conecta directamente a cualquier puerto USB. No hay diferencias en la función principal, que es el almacenamiento y suministro de credenciales.

Un token USB se utiliza para realizar una autenticación fuerte. Ofrece seguridad mejorada y un acceso seguro a la información.

NOTA: Usted debe tener un lector de tarjeta configurado para este procedimiento. Si usted no tiene un lector instalado, es posible registrar un token virtual como se describe en “Creación de un token virtual en la página 15.”

1. En HP ProtectTools Security Manager, haga clic en **Credential Manager** en el panel izquierdo.
2. Haga clic en **My Identity** (Mi identidad) y luego en **Register Smart Card or Token** (Registrar tarjeta inteligente o símbolo).
3. En el cuadro de diálogo **Device Type** (Tipo de dispositivo), haga clic en el tipo de dispositivo deseado y luego en **Next** (Siguiente).
4. Si se seleccionó una smart card o un token USB como tipo de dispositivo, asegúrese de que la smart card esté insertada o que el token esté conectado a un puerto USB.

   NOTA: Si la smart card no está insertada o el token USB no está conectado, el botón Next (Siguiente) estará desactivado en el cuadro de diálogo Select Token (Seleccionar token).

5. En el cuadro de diálogo Device Type (Tipo de dispositivo), seleccione **Next** (Siguiente).

Aparece el cuadro de diálogo Token Properties (Propiedades del token).

6. Introduzca el PIN del usuario, seleccione **Register smart card or token for authentication** (Registrar tarjeta inteligente o símbolo para autenticación) y, a continuación, haga clic en **Finish** (Finalizar).

Registro de otras credenciales

1. En HP ProtectTools Security Manager, haga clic en **Credential Manager**.
2. Haga clic en **My Identity** (Mi identidad) y luego en **Register Credentials** (Registrar credenciales).

   Se abrirá el asistente de registro de Credential Manager.
3. Siga las instrucciones que aparecen en pantalla.

Tareas generales

Todos los usuarios tienen acceso a la página “My Identity” (Mi identidad) en Credential Manager. Desde la página “My Identity” (Mi identidad), es posible realizar las siguientes tareas:

- Cambiar la contraseña de inicio de sesión de Windows
- Cambiar el PIN de un token
- Bloquear una estación de trabajo

NOTA: Esta opción está disponible sólo si la solicitud de inicio clásico de Credential Manager está activada. Consulte “Ejemplo 1—Utilización de la página “Configuración avanzada” para permitir inicio de sesión en Windows desde Credential Manager en la página 24.”

Creación de un token virtual

Un token virtual funciona de manera similar a una Java Card o un a token USB. El token se guarda en el disco duro del equipo o en el registro de Windows. Cuando inicia la sesión con un token virtual, se le solicita un PIN de usuario para completar la autenticación.

Para crear un nuevo token virtual:

1. En HP ProtectTools Security Manager, haga clic en **Credential Manager** en el panel izquierdo.
2. Haga clic en **My Identity** (Mi identidad) y luego en **Register Smart Card or Token** (Registrar tarjeta inteligente o símbolo).
3. En el cuadro de diálogo **Device Type** (Tipo de dispositivo), haga clic en **Virtual Token** (Token virtual) y entonces en **Next** (Siguiente).
4. Especifique el nombre y la ubicación del token y haga clic en **Next** (Siguiente).

   Un nuevo token virtual puede almacenarse en un archivo o en la base de datos de registro de Windows.
5. En el cuadro de diálogo Token Properties (Propiedades de token), especifique el PIN maestro y el PIN de usuario para el nuevo token virtual creado, seleccione **Register smart card or token for authentication** (Registrar tarjeta inteligente o símbolo para autenticación) y entonces haga clic en **Finish** (Finalizar).

Cambio de la contraseña de inicio de sesión de Windows

1. En HP ProtectTools Security Manager, haga clic en **Credential Manager** en el panel izquierdo.
2. Haga clic en **My Identity** (Mi identidad) y luego en **Change Windows Password** (Cambiar contraseña de Windows).
3. Ingrese su contraseña antigua en la casilla **Contraseña anterior**.
4. Escriba la nueva contraseña en las casillas **Nueva contraseña** y **Confirmar contraseña**.
5. Haga clic en **Finalizar**.

Cambio del PIN de un token

1. En HP ProtectTools Security Manager, haga clic en **Credential Manager** en el panel izquierdo.
2. Haga clic en **My Identity** (Mi identidad) y luego en **Change Token PIN** (Cambiar contraseña de token).
3. En el cuadro de diálogo Device Type (Tipo de dispositivo), haga clic en el tipo de dispositivo deseado y luego en **Next** (Siguiente).
4. Seleccione el token del que desea cambiar el PIN y luego haga clic en **Siguiente**.
5. Siga las instrucciones que aparecen en pantalla para completar el cambio de PIN.

NOTA: Si ingresa el PIN incorrecto para el token varias veces en secuencia, el token se bloquea. Usted podrá quedar imposibilitado de usar ese token hasta que lo desbloquee.

Bloqueo del equipo (estación de trabajo)

Este recurso está disponible si usted inicia sesión en Windows utilizando Credential Manager. Para proteger el equipo cuando se encuentre fuera del escritorio, utilice el recurso de bloqueo de estación de trabajo. Esto evita que usuarios no autorizados obtengan acceso a su equipo. Sólo usted y los miembros del grupo de administradores del equipo pueden desbloquearlo.

NOTA: Esta opción está disponible sólo si la solicitud de inicio clásico de Credential Manager está activada. Consulte “Ejemplo 1—Utilización de la página “Configuración avanzada” para permitir inicio de sesión en Windows desde Credential Manager en la página 24.”

Para mayor seguridad, se puede configurar el recurso de bloqueo de estación de trabajo para que solicite una Java Card, un lector biométrico o un token para desbloquear el equipo. Para obtener más información, consulte “Configuración de los valores de Credential Manager en la página 24.”

1. En HP ProtectTools Security Manager, haga clic en **Credential Manager** en el panel izquierdo.
2. Haga clic en **My Identity** (Mi identidad).
3. Haga clic en **Lock Workstation** (Bloquear estación de trabajo) para bloquear su equipo de inmediato.

   Para desbloquear el equipo, debe utilizar una contraseña de Windows o el asistente de inicio de sesión de Credential Manager.

Uso de inicio de sesión en Windows

Es posible utilizar Credential Manager para iniciar una sesión en Windows, ya sea en un equipo local o en un dominio de red. Al iniciar sesión en Credential Manager por primera vez, el sistema agrega de forma automática la cuenta de usuario de Windows local como la cuenta para el servicio de inicio de sesión de Windows.

Inicio de sesión en Windows con Credential Manager

Se puede utilizar Credential Manager para iniciar la sesión en una cuenta local o red de Windows.

1. Si registró su huella digital para iniciar la sesión en Windows, deslice su dedo para iniciar la sesión.
2. En Windows XP, si no ha registrado su huella digital para iniciar sesión en Windows, haga clic en el icono del teclado en el ángulo superior izquierdo de la pantalla, cerca del icono de la huella digital. El asistente de inicio de sesión de Credential Manager se abrirá.

   En Windows Vista, si no ha registrado su huella digital para iniciar sesión en Windows, haga clic en el icono de **Credential Manager**, en la pantalla de inicio de sesión. El asistente de inicio de sesión de Credential Manager se abrirá.
3. Haga clic en la flecha de **Nombre de usuario** y a continuación haga clic en su nombre.
4. Escriba su contraseña en la casilla **Contraseña** y haga clic en **Siguiente**.

5. Seleccione **More** (Más) y entonces haga clic en **Wizard Options** (Opciones del asistente).

   a. Si desea que este sea el nombre de usuario predeterminado la próxima vez que inicie sesión en el equipo, seleccione la casilla de verificación **Utilizar el nombre del último usuario en el próximo inicio de sesión**.

   b. Si desea que este criterio de inicio de sesión sea el predeterminado, seleccione la casilla de verificación **Utilice este criterio de inicio de sesión la próxima vez que inicie sesión**.

6. Siga las instrucciones que aparecen en pantalla. Si la información de autenticación es correcta, iniciará sesión en su cuenta de Windows y en Credential Manager.

Uso del Single Sign On (Inicio de sesión único)

Credential Manager posee un recurso de Single Sign On (Inicio de sesión único) que almacena nombres de usuarios y contraseñas para varias aplicaciones de Windows e Internet, e ingresa de forma automática las credenciales de inicio de sesión al acceder a un programa registrado.

NOTA: La seguridad y la privacidad son importantes recursos de Single Sign On (Inicio de sesión único). Todas las credenciales son encriptadas y están disponibles sólo después de iniciar con éxito la sesión en Credential Manager.

NOTA: También es posible configurar el Single Sign On (Inicio de sesión único) para validar sus credenciales de autenticación con una Java Card, un lector biométrico o un token, antes de iniciar la sesión en un sitio seguro o en un programa seguro. Esto es particularmente útil cuando inicia la sesión en programas o sitios web que contienen información personal, como números de cuentas bancarias. Para obtener más información, consulte “Configuración de los valores de Credential Manager en la página 24.”

Registro de una nueva aplicación

Credential Manager le solicitará registrar cualquier aplicación que inicie mientras está registrado en Credential Manager. También puede registrar una aplicación manualmente.

Uso del registro automático

1. Abra una aplicación que requiera que inicie sesión.
2. Haga clic en el icono Credential Manager Single Sign On en el cuadro de diálogo de la contraseña de un programa o sitio web.
3. Escriba la contraseña para el programa o sitio web y a continuación haga clic en **Aceptar**. Aparece el cuadro de diálogo de **Credential Manager Single Sign On**.
4. Haga clic en **Más** y seleccione una de las siguientes opciones:
   - No utilice el recurso de Single Sign On (Inicio de sesión único - SSO) con este sitio o aplicación.
   - Solicite para seleccionar una cuenta para esta aplicación.
   - Escriba las credenciales pero no las envíe.
   - Autenticar usuario antes de enviar credenciales.
   - Muestre acceso directo de SSO para esta aplicación.
5. Haga clic en **Sí** para finalizar el registro.

Uso del registro manual (arrastrar y soltar)

1. En HP ProtectTools Security Manager, haga clic en **Credential Manager** y entonces haga clic en **Services and Applications** (Servicios y aplicaciones), en el panel izquierdo.
2. Haga clic en **Manage Services and Applications** (Administrar servicios y aplicaciones).

   Se abre el cuadro de diálogo Single Sign On (Inicio de sesión único) de Credential Manager.
3. Para modificar o quitar un sitio web o una aplicación registrada previamente, seleccione el registro deseado en la lista.
4. Siga las instrucciones que aparecen en pantalla.

Administración de aplicaciones y credenciales

Modificación de propiedades de aplicación

1. En HP ProtectTools Security Manager, haga clic en **Credential Manager** y entonces haga clic en **Services and Applications** (Servicios y aplicaciones), en el panel izquierdo.
2. Haga clic en **Manage Services and Applications** (Administrar servicios y aplicaciones).

   Se abre el cuadro de diálogo Single Sign On (Inicio de sesión único) de Credential Manager.
3. Seleccione la aplicación que desee modificar, y haga clic en **Propiedades**.
4. Haga clic en la ficha **General** para modificar el nombre y la descripción de la aplicación. Cambie la configuración seleccionando o desmarcando las casillas de verificación situadas junto a la configuración apropiada.
5. Haga clic en la ficha **Script** para ver y editar el script de la aplicación SSO.
6. Haga clic en **Aceptar**.

Eliminación de aplicaciones desde el Single Sign On (Inicio de sesión único)

1. En HP ProtectTools Security Manager, haga clic en **Credential Manager** y entonces haga clic en **Services and Applications** (Servicios y aplicaciones), en el panel izquierdo.
2. Haga clic en **Manage Services and Applications** (Administrar servicios y aplicaciones).

   Se abre el cuadro de diálogo Single Sign On (Inicio de sesión único) de Credential Manager.
3. Seleccione la aplicación que desea eliminar y haga clic en **Remove** (Quitar).
4. Haga clic en **Sí** en el cuadro de diálogo de confirmación.
5. Haga clic en **Aceptar**.

Exportación de aplicaciones

Es posible exportar aplicaciones para crear una copia de seguridad del script de aplicación de Single Sign On (Inicio de sesión único). Este archivo puede ser utilizado para recuperar la fecha del Single Sign On (Inicio de sesión único). Esto actúa como un complemento del archivo de copia de seguridad de identidad, que contiene sólo la información de la credencial.

Para exportar una aplicación:

1. En HP ProtectTools Security Manager, haga clic en **Credential Manager** y entonces haga clic en **Services and Applications** (Servicios y aplicaciones), en el panel izquierdo.
2. Haga clic en **Manage Services and Applications** (Administrar servicios y aplicaciones).

   Se abre el cuadro de diálogo Single Sign On (Inicio de sesión único) de Credential Manager.
3. Seleccione la aplicación que desea exportar y haga clic en **More** (Más).
4. Siga las instrucciones en pantalla para completar la exportación.
5. Haga clic en **Aceptar**.

Importación de aplicaciones

1. En HP ProtectTools Security Manager, haga clic en **Credential Manager** y entonces haga clic en **Services and Applications** (Servicios y aplicaciones), en el panel izquierdo.
2. Haga clic en **Manage Services and Applications** (Administrar servicios y aplicaciones).

   Se abre el cuadro de diálogo Single Sign On (Inicio de sesión único) de Credential Manager.
3. Seleccione la entrada de aplicación que desea importar y haga clic en **More** (Más).
4. Siga las instrucciones en pantalla para completar la importación.
5. Haga clic en **Aceptar**.

Modificación de credenciales

1. En HP ProtectTools Security Manager, haga clic en **Credential Manager** y entonces haga clic en **Services and Applications** (Servicios y aplicaciones).
2. Haga clic en **Manage Services and Applications** (Administrar servicios y aplicaciones).

   Se abre el cuadro de diálogo Single Sign On (Inicio de sesión único) de Credential Manager.
3. Seleccione la aplicación que desee modificar, y luego haga clic en **Más**.
4. Seleccione una de las siguientes opciones:
   - Aplicaciones
     - Agregar nuevas credenciales
     - Eliminar nuevas credenciales
     - Propiedades
     - Importar aplicación
     - Exportar aplicación
   - Credenciales
     - Crear nueva
   - Ver contraseña

NOTA: Usted debe autenticar su identidad antes de ver la contraseña.

5. Siga las instrucciones que aparecen en pantalla.
6. Haga clic en **Aceptar**.

Uso de la protección de aplicaciones

Este recurso permite configurar el acceso a aplicaciones. Es posible restringir el acceso con base en los siguientes criterios:

- Categoría de usuario
- Tiempo de uso
- Inactividad del usuario

Restricción de acceso a una aplicación

1. En HP ProtectTools Security Manager, haga clic en **Credential Manager**, en el panel izquierdo, y entonces haga clic en **Services and Applications** (Servicios y aplicaciones).
2. Haga clic en **Application Protection** (Protección de aplicación).
3. Seleccione una categoría de usuario cuyo acceso desea administrar.

NOTA: Si la categoría no es todos, es posible que sea necesario seleccionar **Anular configuración predeterminada** para anular la configuración para la categoría todos.

4. Haga clic en **Add** (Agregar).

   Se abre el asistente para agregar un programa.
5. Siga las instrucciones que aparecen en pantalla.

Eliminación de protección de una aplicación

Para eliminar restricciones de una aplicación:

1. En HP ProtectTools Security Manager, haga clic en **Credential Manager** en el panel izquierdo.
2. Haga clic en **Services and Applications** (Servicios y aplicaciones).
3. Haga clic en **Application Protection** (Protección de aplicación).
4. Seleccione una categoría de usuario cuyo acceso desea administrar.

NOTA: Si la categoría no es todos, es posible que sea necesario seleccionar **Anular configuración predeterminada** para anular la configuración para la categoría todos.

5. Seleccione la aplicación que desee eliminar, y haga clic en **Quitar**.
6. Haga clic en **Aceptar**.

Cambio de configuración de restricción para una aplicación protegida

1. Haga clic en **Application Protection** (Protección de aplicación).
2. Seleccione una categoría de usuario cuyo acceso desea administrar.

NOTA: Si la categoría no es todos, es posible que sea necesario seleccionar **Anular configuración predeterminada** para anular la configuración para la categoría todos.

3. Seleccione la aplicación que desee modificar, y luego haga clic en **Propiedades**. Aparece el cuadro de diálogo **Propiedades** para la aplicación.
4. Seleccione la ficha **General**. Seleccione una de las siguientes configuraciones:
   - Desactivado (No es posible utilizarlo)
   - Activado (Es posible utilizarlo sin restricciones)
   - Restringido (Uso depende de la configuración)
5. Cuando usted selecciona el uso restringido, están disponibles la siguientes configuraciones:
   a. Si usted desea restringir el uso con base en tiempo, día o fecha, haga clic en la ficha **Programar** y configurar la configuración.
   b. Si usted desea restringir el uso con base en inactividad, haga clic en la ficha **Avanzado** y seleccione el período de inactividad.
6. Haga clic en **Aceptar** para cerrar el cuadro de diálogo de **Propiedades** de aplicaciones.
7. Haga clic en **Aceptar**.

Tareas avanzadas (sólo para administradores)

La página “Autenticación y credenciales” y la página “Configuración avanzada” de Credential Manager están disponibles sólo para aquellos usuarios con derechos de administrador. Desde estas páginas, es posible realizar las siguientes tareas:

- Especificación de cómo los usuarios y los administradores inician la sesión
- Configuración de requisitos de autenticación personalizados
- Configuración de propiedades de credenciales
- Configuración de los valores de Credential Manager

Especificación de cómo los usuarios y los administradores inician la sesión

Desde la página “Autenticación y credenciales”, es posible identificar que tipo o combinación de credenciales son necesarias para usuarios o administradores.

Para especificar cómo los usuarios o administradores inician la sesión:

1. En HP ProtectTools Security Manager, haga clic en **Credential Manager** en el panel izquierdo.
2. Haga clic en **Multifactor Authentication** (Autenticación multifactor).
3. En el panel derecho, haga clic en la ficha **Autenticación**.

4. Seleccione la categoría (**Usuarios** o **Administradores**) en la lista de categoría.
5. Seleccione el tipo o la combinación de métodos de autenticación en la lista.
6. Haga clic en **Aplicar** y, a continuación, haga clic en **Aceptar**.

Configuración de requisitos de autenticación personalizados

Si el conjunto de credenciales de autenticación que usted desea no está listado en la ficha autenticación de la página “Autenticación y credenciales”, es posible crear requisitos personalizados.

Para configurar requisitos personalizados:

1. En HP ProtectTools Security Manager, haga clic en **Credential Manager** en el panel izquierdo.
2. Haga clic en **Multifactor Authentication** (Autenticación multifactor).
3. En el panel derecho, haga clic en la ficha **Autenticación**.
4. Seleccione la categoría (**Usuarios** o **Administradores**) en la lista de categoría.
5. Seleccione **Personalizado** en la lista de métodos de autenticación.
6. Haga clic en **Configurar**.
7. Seleccione los métodos de autenticación que desee utilizar.
8. Elija la combinación de métodos haciendo clic en una de las siguientes selecciones:
   - Uso y para combinar los métodos de autenticación

     (Los usuarios deben autenticarse con todos los métodos marcados cada vez que inician la sesión).
   - Uso o para requerir uno de dos o más métodos de autenticación

     (Los usuarios podrán elegir uno de los métodos seleccionados cada vez que inician la sesión).
9. Haga clic en **Aceptar**.
10. Haga clic en **Aplicar** y, a continuación, haga clic en **Aceptar**.

Configuración de propiedades de credenciales

Desde la ficha credenciales de la página “Autenticación y credenciales”, es posible visualizar la lista de métodos de autenticación disponibles, y modificar la configuración.

Para configurar las credenciales:

1. En HP ProtectTools Security Manager, haga clic en **Credential Manager** en el panel izquierdo.
2. Haga clic en **Multifactor Authentication** (Autenticación multifactor).
3. Haga clic en la ficha **Credentials** (Credenciales).

4. Haga clic en el tipo de credencial que desea modificar. Puede modificar la credencial utilizando una de las siguientes opciones:

   - Para registrar la credencial, haga clic en **Registrar** y luego siga las instrucciones que aparecen en pantalla.
   - Para eliminar la credencial, haga clic en **Clear** (Borrar) y luego haga clic en **Sí** en el cuadro de diálogo de confirmación.
   - Para modificar las propiedades de la credencial, haga clic en **Propiedades** y luego siga las instrucciones que aparecen en pantalla.

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

Configuración de los valores de Credential Manager

En la página “Advanced Settings” (Configuración avanzada) se puede acceder a varios valores y modificarlos a través de las siguientes fichas:

- General—Permite modificar la definición para configuración básica.
- Single Sign On (Inicio de sesión único)—Permite modificar la configuración para definir cómo el inicio único de sesión funciona para el usuario actual, de qué manera administra la detección de pantallas de inicio de sesión, inicio de sesión automático para diálogos registrados de inicio de sesión, y exhibición de contraseñas.
- Servicios y aplicaciones—Permite visualizar los servicios disponibles y modificar la configuración para esos servicios.
- Seguridad—Permite seleccionar el software del lector de huellas digitales y ajustar el nivel de seguridad del lector de huellas digitales.
- Smart Card y tokens—Permite visualizar y modificar propiedades para todas las Java Card y token disponibles.

Para modificar la configuración de Credential Manager:

1. En HP ProtectTools Security Manager, haga clic en **Credential Manager** en el panel izquierdo.
2. Haga clic en **Settings** (Configuración).
3. Haga clic en la ficha apropiada para la configuración que desea modificar.
4. Siga las instrucciones que aparecen en pantalla para modificar la configuración.
5. Haga clic en **Aplicar** y, a continuación, haga clic en **Aceptar**.

Ejemplo 1—Utilización de la página “Configuración avanzada” para permitir inicio de sesión en Windows desde Credential Manager

1. En HP ProtectTools Security Manager, haga clic en **Credential Manager** en el panel izquierdo.
2. Haga clic en **Settings** (Configuración).
3. Haga clic en la ficha **General**.
4. En **Seleccionar la forma en que los usuarios inician sesión en Windows (requiere reinicio)**, seleccione la casilla de verificación **Utilizar Credential Manager con solicitud clásica de inicio de sesión**.

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

6. Reinicie el equipo.

NOTA: Al seleccionar la casilla de verificación **Utilizar Credential Manager con solicitud clásica de inicio de sesión** permite bloquear el equipo. Consulte "Bloqueo del equipo (estación de trabajo) en la página 17."

Ejemplo 2—Utilización de la página "Configuración avanzada" para solicitar verificación del usuario antes del inicio único de sesión

1. En HP ProtectTools Security Manager, haga clic en **Credential Manager** y entonces haga clic en **Settings** (Configuración).

2. Haga clic en la ficha **Single Sign On** (Inicio de sesión único).

3. En **Cuando se detecte una ventana o una página web de inicio de sesión**, seleccione la casilla de verificación **Pedir confirmación antes de grabar credenciales**.

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

5. Reinicie el equipo.

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

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

Procedimientos de configuración

Apertura de Drive Encryption

1. Haga clic en Inicio, Todos los programas y entonces haga clic en **HP ProtectTools Security Manager**.
2. Haga clic en **Drive Encryption**.

Tareas generales

Activación de Drive Encryption

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

Desactivación de Drive Encryption

Use el asistente de configuración de HP ProtectTools Security Manager para desactivar Drive Encryption.

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

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

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

Tareas avanzadas

Administración de Drive Encryption (tarea de administrador)

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

Activación de una contraseña protegida por TPM (Trusted Protection Module) (sólo en algunos modelos)

Use la herramienta Embedded Security en HP ProtectTools para activar el TPM. Luego de la activación, para iniciar sesión en la pantalla de inicio de sesión de Drive Encryption es necesario que introduzca su nombre de usuario y la contraseña de Windows.

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

1. Use la herramienta Embedded Security en HP ProtectTools para activar el TPM.
2. Abra Drive Encryption y haga clic en **Encryption Management** (Administración de encriptación).
3. Seleccione la casilla de verificación **TPM-protected password** (Contraseña protegida por TPM).

Encriptación o desencriptación de unidades individuales

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

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

Copias de seguridad y recuperación (tarea de administrador)

La página “Recovery” (Recuperación) permite que los administradores hagan copias de seguridad y recuperen las claves de encriptación.

Creación de copias de seguridad de las claves

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

1. Abra Drive Encryption y haga clic en **Recovery** (Recuperación).
2. Presione **Backup Keys** (Crear copia de seguridad de las claves).

3. En la página “Select Backup Disk” (Elegir disco para copia de seguridad), haga clic en el nombre del dispositivo donde desea hacer la copia de seguridad de su clave de encriptación y entonces presione **Next** (Siguiente).

4. Lea la información en la siguiente página que aparece y luego haga clic en **Next** (Siguiente).

   La clave de encriptación se guarda en el dispositivo de almacenamiento que usted seleccionó.

5. Haga clic en **OK** (Aceptar) cuando se abra el cuadro de diálogo de confirmación.

Registro para recuperación en línea

El Servicio de recuperación de claves de Drive Encryption en línea almacena una copia de seguridad de su clave de encriptación, lo que le permitirá tener acceso a su equipo si se le olvida la contraseña y no tiene acceso a su copia de seguridad local.

NOTA: Debe estar conectado a Internet y poseer una dirección de correo electrónico válida para registrarse y recuperar su contraseña a través de este servicio.

1. Abra Drive Encryption y haga clic en **Recovery** (Recuperación).
2. Haga clic en **Register** (Registrar).
3. Haga clic en una de las siguientes opciones:

   - I want to create a new recovery account for this PC (Deseo crear una nueva cuenta de recuperación para este PC). Si elige esta opción, escriba su dirección de correo electrónico y otra información personal y luego haga clic en **Next** (Siguiente).
   - I want to add this PC to my existing web recovery account (Deseo agregar este PC a mi cuenta de recuperación basada en la web existente).

4. Cree y confirme una contraseña, seleccione preguntas seguridad y escriba las respuestas, y entonces haga clic en **Next** (Siguiente).

   NOTA: Se le enviará un código de activación de cuenta a la dirección de correo electrónico que usted suministró.

5. Escriba el código de activación y luego haga clic en **Next** (Siguiente).
6. Escriba el número de serie del equipo y luego haga clic en **Next** (Siguiente).

   NOTA: Para localizar el número de serie del equipo, haga clic en **Inicio** y en **Ayuda y soporte técnico**.

7. Si no tiene un cupón de suscripción, haga clic en el enlace **Click here to purchase coupons** (Haga clic aquí para comprar cupones).

   Al hacer clic en el enlace, se le enviará al sitio web del Servicio de recuperación de claves de la Encriptación de Unidades de Disco. No salga del asistente.

8. Haga clic en **Comprar cupón de código**.
9. Seleccione su país, el tipo de equipo y luego haga clic en **Iniciar**.
10. Haga clic en **Comprar**, al lado de la opción de suscripción por un año o por tres años.
11. Haga clic en **Verificación**.
12. Lea los términos y condiciones y luego haga clic en **Acepto**.

13. Escriba la información de facturación y luego haga clic en **Continuar**.
14. Introduzca la información de su tarjeta de crédito y luego haga clic en **Realizar pago**.
15. Anote el código de su cupón y luego vuelva a la página de “Account Activation” (Activación de cuenta) en el asistente.
16. Digite su código de activación de cuenta y luego haga clic en **Next** (Siguiente).
17. Cuando se abra el cuadro de diálogo de confirmación, haga clic en **OK** (Aceptar).

Administración de una cuenta de recuperación en línea existente

Después de crear una cuenta de recuperación en línea, puede acceder al sitio web del Servicio de recuperación de arranque seguro para recuperar el acceso a su equipo en caso de que haya perdido su contraseña, desee modificar sus configuraciones personales, quiera redefinir la contraseña que usa para la cuenta de recuperación en línea o desee ver o renovar su cuenta.

1. Abra Drive Encryption y haga clic en **Recovery** (Recuperación).
2. Haga clic en **Manage** (Administrar).
3. Cuando se abra la página web del Servicio de recuperación de claves de la Encriptación de Unidades de Disco, haga clic en **Gestionar cuentas** o en **Proceso de recuperación**.
4. En la página de inicio de sesión del servicio de recuperación, digite su dirección de correo electrónico, su contraseña y los números y letras que vea en el cuadro.
5. Haga clic en **Iniciar sesión**.
6. Haga clic en **Profile** (Perfil) para actualizar su información personal, como su teléfono o dirección de facturación.

   – o –

   Haga clic en **Reset Password** (Redefinir contraseña) para redefinir o cambiar su contraseña.

   – o –

   Haga clic en **My Subscriptions** (Mis suscripciones) para ver la información de su suscripción actual.

NOTA: La página “My Subscriptions” (Mis suscripciones) también le permite renovar su suscripción. Haga clic en **Renew Subscription** (Renovar suscripción) para realizar esta acción.

Realización de una recuperación

Realización de una recuperación local

1. Encienda el equipo.
2. Inserte el dispositivo de almacenamiento extraíble en el que está guardada su clave de respaldo.
3. Cuando se abra el cuadro de diálogo de inicio de sesión de Drive Encryption for HP ProtectTools, haga clic en **Cancel** (Cancelar).
4. Haga clic en **Options** (Opciones), en la esquina inferior izquierda de la pantalla, y luego haga clic en **Recovery** (Recuperación).
5. Haga clic en **Local Recovery** (Recuperación local) y luego en **Next** (Siguiente).
6. Seleccione el archivo que contiene su clave de respaldo, o haga clic en **Browse** (Explorar) para buscarlo, y luego haga clic en **Next** (Siguiente).
7. Cuando se abra el cuadro de diálogo de confirmación, haga clic en **OK** (Aceptar).

   El proceso de recuperación ha terminado y su equipo se inicia.

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

Realización de una recuperación en línea

NOTA: Esta sección describe cómo realizar una recuperación en línea cuando tiene acceso a un equipo diferente con una conexión a Internet. Si no tiene acceso a ese tipo de equipo, entre en contacto con el soporte técnico de HP.

1. Encienda el equipo.
2. Cuando se abra el cuadro de diálogo de inicio de sesión de Drive Encryption for HP ProtectTools, haga clic en **Cancel** (Cancelar).
3. Haga clic en **Options** (Opciones) en la esquina inferior izquierda de la pantalla, y luego haga clic en **Recovery** (Recuperación).
4. Haga clic en **Web Recovery** (Recuperación a través de la web) y luego en **Next** (Siguiente).
5. Registre el código de cliente y luego haga clic en **Next** (Siguiente).
6. En un equipo diferente con una conexión a internet, vaya al sitio web del Servicio de recuperación de claves de la Encriptación de Unidades de Disco en http://www.safeboot-hp.com.
7. Haga clic en **Proceso de recuperación**.
8. En la página de inicio de sesión del servicio de recuperación, escriba su dirección de correo electrónico, su contraseña y los números y letras que vea en el cuadro.
9. Haga clic en **Iniciar sesión**.
10. Haga clic en **Proceso de recuperación**.
11. Escriba el código de cliente que registró desde el equipo que está recuperando e ingrese los números y las letras que vea en el cuadro.
12. Haga clic en **Submit** (Enviar).

13. Registre cada línea de la clave de respuesta.
14. En el equipo que está recuperando, ingrese la línea 1 de la clave de respuesta que registró del sitio web del Servicio de recuperación de claves de la Encriptación de Unidades de Disco y luego haga clic en **intro**.
15. Ingrese la línea 2 de la clave de respuesta y luego haga clic en **intro**.
16. Ingrese la línea 3 de la clave de respuesta y luego haga clic en **intro**.
17. Ingrese la línea 4 de la clave de respuesta y luego haga clic en **intro**.

    NOTA: La línea 4 de la clave de respuesta es más corta que las primeras tres líneas.

18. Haga clic en **Finish** (Finalizar).

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

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

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

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

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

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

Apertura de Privacy Manager

Para abrir Privacy Manager:

1. Haga clic en **Inicio**, **Todos los programas** y entonces en **HP ProtectTools Security Manager**.
2. Haga clic en **Privacy Manager: Sign and Chat**.

– o –

Haga clic con el botón derecho en el icono de **HP ProtectTools** en el área de notificación, en el extremo derecho de la barra de tareas, y entonces haga clic en **Privacy Manager: Sign and Chat** y entonces haga clic en **Configuration** (Configuración).

– o –

En la barra de herramientas de un mensaje de correo electrónico de Microsoft Outlook, haga clic en **Send Securely** (Enviar con seguridad) y entonces haga clic en **Certificate Manager** o en **Trusted Contact Manager** (Administrador de contactos confiables).

– o –

En la barra de herramientas de un documento de Microsoft Outlook, haga clic en **Send Securely** (Enviar con seguridad) y entonces haga clic en **Certificate Manager** o en **Trusted Contact Manager** (Administrador de contactos confiables).

Procedimientos de configuración

Administración de certificados de Privacy Manager

El administrador de certificados protege datos y mensajes usando una tecnología criptográfica llamada infraestructura de clave pública (PKI). PKI requiere que los usuarios obtengan claves criptográficas y un certificado de Privacy Manager emitido por una autoridad de certificación (CA). A diferencia de la mayor parte del software de encriptación y autenticación, que solo le exige que se autentique periódicamente, Privacy Manager requiere autenticación cada vez que firma un mensaje de correo electrónico o un documento de Microsoft Office usando una clave criptográfica. Privacy Manager hace que el proceso de guardar y enviar su información importante sea seguro.

Solicitación e instalación de un certificado de Privacy Manager

Antes de que pueda usar los recursos de Privacy Manager, debe requerir e instalar un certificado de Privacy Manager (desde dentro de Privacy Manager) usando una dirección de correo electrónico válida. La dirección de correo electrónico debe configurarse como una cuenta dentro de Microsoft Outlook en el mismo equipo desde el que está solicitando el certificado de Privacy Manager.

Solicitud de un certificado de Privacy Manager

1. Abra Privacy Manager y haga clic en **Certificate Manager** (Administrador de certificados).
2. Haga clic en **Privacy Manager Certificate** (Certificado de Privacy Manager).
3. Lea el texto de bienvenida y entonces haga clic en **Next** (Siguiente).
4. En la página “License Agreement” (Acuerdo de licencia), lea el acuerdo de licencia.
5. Asegúrese de que la casilla al lado de **Check here to accept the terms of this license agreement** (Marque aquí para aceptar los términos de este acuerdo de licencia) esté marcada y entonces haga clic en **Next** (Siguiente).
6. En la página “Your Certificate Details” (Sus detalles de certificado), introduzca la información requerida y haga clic en **Next** (Siguiente).
7. En la página “Certificate Request Accepted” (Solicitud de certificado aceptada), haga clic en **Finish** (Finalizar).

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

Instalación de un certificado de Privacy Manager

1. Cuando reciba el mensaje de correo electrónico con su certificado de Privacy Manager adjunto, abra el mensaje y haga clic en el botón **Setup** (Configuración), en la esquina inferior derecha del mensaje.
2. Autentíquese usando su método de inicio de sesión seguro elegido.
3. En la página “Certificate Installed” (Certificado instalado), haga clic en **Next** (Siguiente).
4. En la página “Certificate Backup” (Copia de seguridad de certificado), ingrese un lugar y un nombre para el archivo de copia de seguridad o haga clic en **Browse** (Explorar) para buscar una ubicación.

△ **PRECAUCIÓN:** Asegúrese de que ha guardado el archivo en un lugar que no sea su undad de disco duro para ponerlo en un lugar seguro. Este archivo debe ser para su uso exclusivo y se necesitará en caso de que precise restaurar su certificado de Privacy Manager y las claves asociadas.

5. Escriba y confirme una contraseña y haga clic en **Next** (Siguiente).
6. Autentíquese usando su método de inicio de sesión seguro elegido.
7. Si ha elegido comenzar con el proceso de invitación de contacto confiable, siga las instrucciones en la pantalla.

   – o –

   Si hace clic en Cancelar, consulte Administración de contactos confiables para sabe cómo adicionar un contacto confiable más adelante.

Visualización de detalles del certificado de Privacy Manager

1. Abra Privacy Manager y haga clic en **Certificate Manager** (Administrador de certificados).
2. Haga clic en un certificado de Privacy Manager
3. Haga clic en **Certificate details** (Detalles del certificado).
4. Cuando haya finalizado la visualización de los detalles, haga clic en **OK** (Aceptar).

Renovación de un certificado de Privacy Manager

Cuando su certificado de Privacy Manager está por expirar, se le notificará que debe renovarlo:

1. Abra Privacy Manager y haga clic en **Certificate Manager** (Administrador de certificados).
2. Haga clic en un certificado de Privacy Manager
3. Haga clic en **Renew certificate** (Renovar certificado).
4. Siga las instrucciones en la pantalla para comprar un nuevo certificado de Privacy Manager.

NOTA: El proceso de renovación de certificados de Privacy Manager no sustituye su antiguo certificado de Privacy Manager. Usted deberá comprar un nuevo certificado de Privacy Manager e instalarlo siguiendo el mismo procedimiento descripto en Solicitación e instalación de un certificado de Privacy Manager.

Configuración de un certificado de Privacy Manager predeterminado

Dentro de Privacy Manager sólo es posible ver los certificados de Privacy Manager, incluso si en su equipo se encuentran instalados certificados adicionales de otras autoridades de certificación.

Si tiene más de un certificado de Privacy Manager en su equipo, que fue instalado desde el interior de Privacy Manager, podrá especificar uno de ellos como el certificado predeterminado:

1. Abra Privacy Manager y haga clic en **Certificate Manager** (Administrador de certificados).
2. Haga clic en el certificado de Privacy Manager que desea usar como certificado predeterminado y entonces haga clic en **Set default** (Predeterminar).
3. Haga clic en **OK** (Aceptar).

NOTA: Usted no está obligado a usar su certificado de Privacy Manager predeterminado. Desde el interior de las diversas funciones de Privacy Manager, puede elegir cualquiera de los certificados de Privacy Manager para su utilización.

Eliminación de un certificado de Privacy Manager

Si elimina un certificado de Privacy Manager, no podrá abrir archivos ni ver ningún dato que haya encriptado con ese certificado. Si ha borrado accidentalmente un certificado de Privacy Manager, puede restaurarlo usando el archivo de copia de seguridad que ha creado cuando instaló el certificado.

Para eliminar un certificado de Privacy Manager:

1. Abra Privacy Manager y haga clic en **Certificate Manager** (Administrador de certificados).
2. Haga clic en el certificado de Privacy Manager que desea eliminar y entonces haga clic en **Advanced** (Avanzado).
3. Haga clic en **Delete** (Eliminar).
4. Cuando se abra el cuadro de diálogo de confirmación, haga clic en **Yes** (Sí).
5. Haga clic en **Close** (Cerrar) y, a continuación, en **Apply** (Aplicar).

Restauración de un certificado de Privacy Manager

Si ha borrado accidentalmente un certificado de Privacy Manager, puede restaurarlo usando el archivo de copia de seguridad que ha creado cuando instaló o exportó el certificado:

1. Abra Privacy Manager y haga clic en **Migration** (Migración).
2. Haga clic en **Import migration file** (Importar archivo de migración).
3. Haga clic en la página “Migration File” (Archivo de migración), haga clic en **Browse** (Explorar) para buscar el archivo .dppsm que creó cuando instaló o exportó el certificado de Privacy Manager, y entonces haga clic en **Next** (Siguiente).
4. En la página “Migration File Import” (Importación de archivo de migración), haga clic en **Finish** (Finalizar).
5. Haga clic en **Close** (Cerrar) y, a continuación, en **Apply** (Aplicar).

NOTA: Consulte Instalación de un certificado de Privacy Manager o Exportación de certificados de Privacy Manager y Contactos confiables para obtener más información.

Revocación de su certificado de Privacy Manager

Si considera que la seguridad de su certificado de Privacy Manager está amenazada, puede revocar su propio certificado:

NOTA: Un certificado de Privacy Manager revocado no es eliminado. El certificado todavía puede utilizarse para ver archivos encriptados.

1. Abra Privacy Manager y haga clic en **Certificate Manager** (Administrador de certificados).
2. Haga clic en **Advanced** (Avanzado).
3. Haga clic en el certificado de Privacy Manager que desea revocar y entonces haga clic en **Revoke** (Revocar).

4. Cuando se abra el cuadro de diálogo de confirmación, haga clic en **Yes** (Sí).
5. Autentíquese usando su método de inicio de sesión seguro elegido.
6. Siga las instrucciones en la pantalla.

Administración de contactos confiables

Los contactos confiables son usuarios con los que ha intercambiado certificados de Privacy Manager, lo que les permite comunicarse de forma segura.

Agregado de contactos confiables

1. Usted envía un mensaje de correo electrónico a un destinatario contacto confiable
2. El destinatario contacto confiable responde al mensaje de correo electrónico.
3. Usted recibe el mensaje de respuesta del destinatario contacto confiable y hace clic en Aceptar.

Puede enviar invitaciones de contacto confiable a través del correo electrónico a destinatarios individuales o puede enviar una invitación a todos los contactos de su lista de direcciones de Microsoft Outlook.

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

Agregado de un contacto confiable

1. Abra Privacy Manager, haga clic en **Trusted Contacts Manager** (Administrador de contactos confiables), y entonces haga clic en **Invite Contacts** (Invitar contactos).

   – o –

   En Microsoft Outlook, haga clic en la flecha abajo al lado de **Send Securely** (Enviar con seguridad), en la barra de herramientas, y entonces haga clic en **Invite Contacts** (Invitar contactos).
2. Si se abre el cuadro de diálogo Select Certificate (Seleccionar certificado), haga clic en el certificado de Privacy Manager que desea usar y entonces haga clic en **OK** (Aceptar).
3. Cuando se abre el cuadro de diálogo Trusted Contact Invitation (Invitación de contacto confiable), lea el texto y haga clic en **OK** (Aceptar).

   Se generará un mensaje de correo electrónico automáticamente.
4. Ingrese una o más direcciones de correo electrónico de los destinatarios a quienes desea agregar como contactos confiables.
5. Edite el texto y firme con su nombre (opcional).
6. Haga clic en **Send** (Enviar).

   NOTA: Si no ha obtenido un certificado de Privacy Manager, un mensaje le informa que debe tener un certificado de Privacy Manager para enviar una solicitación de contacto confiable. Haga clic en Aceptar para iniciar el asistente de solicitud de certificado.
7. Autentíquese usando su método de inicio de sesión seguro elegido.

8. Cuando reciba un mensaje de correo electrónico de respuesta de un destinatario aceptando la invitación para convertirse en un contacto confiable, haga clic en Aceptar, en la esquina inferior derecha del mensaje.

   Se abrirá un cuadro de diálogo confirmando que el destinatario ha sido agregado con éxito a su lista de contactos confiables.

9. Haga clic en **OK** (Aceptar).

Agregado de contactos confiables usando su libreta de direcciones de Microsoft Outlook

1. Abra Privacy Manager, haga clic en **Trusted Contacts Manager** (Administrador de contactos confiables), y luego en **Invite Contacts** (Invitar contactos).

   – o –

   En Microsoft Outlook, haga clic en la flecha abajo al lado de **Send Securely** (Enviar con seguridad), en la barra de herramientas, y entonces haga clic en **Invite All My Outlook Contacts** (Invitar a todos mis contactos de Outlook).

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

3. Cuando se abra la página “Sending Invitation” (Enviando una invitación), haga clic en **Finish** (Finalizar).

   Se generará automáticamente un mensaje de correo electrónico con las direcciones de correo electrónico de Microsoft Outlook seleccionadas.

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

5. Haga clic en **Send** (Enviar).

NOTA: Si no ha obtenido un certificado de Privacy Manager, un mensaje le informa que debe tener un certificado de Privacy Manager para enviar una solicitación de contacto confiable. Haga clic en **OK** (Aceptar) para iniciar el Asistente de solicitud de certificado.

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

NOTA: Cuando el destinatario recibe el mensaje de correo electrónico, debe abrir el mensajey hacer clic en Aceptar en el ángulo inferior derecho del mensaje, y luego debe hacer clic en OK (Aceptar) cuando se abra el cuadro de diálogo de confirmación.

7. Cuando reciba un mensaje de correo electrónico de respuesta de un destinatario aceptando la invitación para convertirse en un contacto confiable, haga clic en OK (Aceptar), en la esquina inferior derecha del mensaje.

   Se abrirá un cuadro de diálogo confirmando que el destinatario ha sido agregado con éxito a su lista de contactos confiables.

8. Haga clic en **OK** (Aceptar).

Visualización de detalles de contactos confiables

1. Abra Privacy Manager y haga clic en **Trusted Contacts Manager** (Administrador de contactos confiables).

2. Haga clic en un contacto confiable.

3. Haga clic en **Contact details** (Detalles del contacto).
4. Una vez que haya terminado de ver los detalles, haga clic en **OK** (Aceptar).

Eliminación de un contacto confiable

1. Abra Privacy Manager y haga clic en **Trusted Contacts Manager** (Administrador de contactos confiables).
2. Haga clic en el contacto confiable que desea eliminar.
3. Haga clic en **Delete contact** (Eliminar contacto).
4. Cuando se abra el cuadro de diálogo de confirmación, haga clic en **Yes** (Sí).

Verificación del estado de revocación de un contacto confiable

1. Abra Privacy Manager y haga clic en **Trusted Contacts Manager** (Administrador de contactos confiables).
2. Haga clic en un contacto confiable.
3. Haga clic en el botón **Advanced** (Avanzado).

   Se abre el cuadro de diálogo Administración avanzada de contactos confiables.
4. Haga clic en **Check Revocation** (Verificar revocación).
5. Haga clic en **Close** (Cerrar).

Tareas generales

Uso de Privacy Manager en Microsoft Office

Después de instalar su certificado de Privacy Manager, aparecerá un botón Sign and Encrypt (Firmar y encriptar) en el lado derecho de la barra de herramientas de todos los documentos de Microsoft Word, Microsoft Excel y Microsoft PowerPoint.

Configuración de Privacy Manager en un documento de Microsoft Office

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

   – o –

   En la barra de herramientas de un documento de Microsoft Office, haga clic en la flecha abajo al lado de **Sign and Encrypt** (Firmar y encriptar) y entonces haga clic en **Settings** (Configuración).

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

Firma de un documento de Microsoft Office

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

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

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

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

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

1. En Microsoft Word o Microsoft Excel, cree y guarde un documento.
2. Haga clic en el menú **Home** (Inicio).
3. Haga clic en la flecha abajo al lado de **Sign and Encrypt** (Firmar y encriptar) y entonces haga clic en **Add Signature Line Before Signing** (Agregar línea de firma antes de firmar).

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

4. Haga clic en la flecha abajo al lado de **Sign and Encrypt** (Firmar y encriptar) y entonces haga clic en **Sign Document** (Firmar documento).

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

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

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

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

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

2. Haga clic en el menú **Insert** (Insertar).

3. En el grupo **Text** (Texto), en la barra de herramientas, haga clic en la flecha al lado de **Signature Line** (Línea de firma) y entonces haga clic en **Privacy Manager Signature Provider** (Proveedor de firma de Privacy Manager).

   Se abre el cuadro de diálogo de Configuración de firma.

4. En la casilla debajo de **Suggested signer** (Firmante sugerido), ingrese el nombre del firmante sugerido.

5. En la casilla debajo de **Instructions to the signer** (Instrucciones para el firmante), escriba un mensaje para este firmante sugerido.

NOTA: Este mensaje aparecerá en el lugar de un título y es borrado o sustituido por el título del usuario cuando se firma el documento.

6. Seleccione la casilla de verificación **Show sign date in signature line** (Mostrar fecha de firma en la línea de firma) para mostrar la fecha.

7. Seleccione la casilla de verificación **Show signer's title in signature line** (Mostrar título del firmante en la línea de firma) para mostrar el título.

NOTA: Como el propietario de un documento designa nos firmantes sugeridos para su documento, y si las casillas de verificación **Show sign date in signature line** (Mostrar fecha de firma en la línea de firma) y/o **Show signer's title in signature line** (Mostrar título del firmante en la línea de firma) no están seleccionadas, el firmante sugerido no podrá mostrar la fecha y/o el título en la línea de firma, incluso si las configuraciones de documento del firmante sugerido están definidas para eso.

8. Haga clic en **OK** (Aceptar).

Agregado de una línea de firma para un firmante sugerido

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

Para firmar el documento:

1. Haga doble clic en la línea de firma adecuada.
2. Autentíquese usando su método de inicio de sesión seguro elegido.

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

Encriptación de un documento de Microsoft Office

Puede encriptar un documento de Microsoft Office para usted y sus contactos confiables. Cuando encripta un documento y lo cierra, usted y los contactos confiables seleccionados de la lista deberán autenticarse antes de abrirlo.

Para encriptar un documento de Microsoft Office:

1. En Microsoft Word, Microsoft Excel o Microsoft PowerPoint, cree y guarde un documento.
2. Haga clic en el menú **Home** (Inicio).
3. Haga clic en la flecha abajo al lado de **Sign and Encrypt** (Firmar y encriptar) y entonces haga clic en **Encrypt Document** (Encriptar documento).

   Se abre el cuadro de diálogo Seleccionar contactos confiables.
4. Haga clic en el nombre de un contacto confiable que podrá abrir el documento y ver su contenido.

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

5. Haga clic en **OK** (Aceptar).
6. Autentíquese usando su método de inicio de sesión seguro elegido.

Si más adelante decide editar el documento, siga los pasos indicados en **Firma de un documento de Microsoft Office**. Cuando se elimina la encriptación, puede editar el documento. Siga los pasos que se indican en esta sección para encriptar el documento nuevamente.

Eliminación de la encriptación de un documento de Microsoft Office

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

Para eliminar la encriptación de un documento de Microsoft Office:

1. Abra un documento encriptado de Microsoft Word, Microsoft Excel o Microsoft PowerPoint.
2. Autentíquese usando su método de inicio de sesión seguro elegido.
3. Haga clic en el menú **Home** (Inicio).
4. Haga clic en la flecha abajo al lado de **Sign and Encrypt** (Firmar y encriptar) y entonces haga clic en **Remove encryption** (Eliminar encriptación).

Envío de un documento de Microsoft Office encriptado

Puede adjuntar un documento encriptado de Microsoft Office a un mensaje de correo electrónico sin firmar ni encriptar el propio mensaje. Para hacer esto, cree y envíe un mensaje de correo electrónico

con un documento firmado o encriptado como lo haría normalmente con cualquier mensaje con un archivo adjunto.

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

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

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

Visualización de un documento de Microsoft Office firmado

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

Cuando un documento de Microsoft Office firmado se abre, se abre un cuadro de diálogo de Firmas al lado del documento, mostrando el nombre del usuario que firmó el documento y la fecha en la que lo firmó. Puede hacer clic con el botón derecho del mouse en el nombre para ver detalles adicionales.

Visualización de un documento de Microsoft Office encriptado

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

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

Uso de Privacy Manager en Microsoft Outlook

Cuando se instala Privacy Manager, un botón de Privacidad se mostrará en la barra de herramientas de Microsoft Outlook, y se mostrará un botón de Envío seguro en la barra de herramientas de cada mensaje de correo electrónico de Microsoft Outlook.

Configuración de Privacy Manager para Microsoft Outlook

1. Abra **Privacy Manager**, haga clic en **Settings** (Configuración) y luego en la ficha **E-mail** (Correo electrónico).

   – o –

   En la barra de herramientas de Microsoft Outlook, haga clic en la flecha abajo al lado de **Privacy** (Privacidad) y entonces haga clic en **Settings** (Configuraciones).

   – o –

   En la barra de herramientas de un mensaje de correo electrónico de Microsoft, haga clic en la flecha abajo al lado de **Send Securely** (Enviar con seguridad) y entonces haga clic en **Settings** (Configuración).

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

Firma y envío de un mensaje de correo electrónico

- En Microsoft Outlook, haga clic en **Nuevo** o en **Responder**.
- Redacte su mensaje de correo electrónico.
- Haga clic en la flecha abajo al lado de **Send Securely** (Enviar con seguridad) y entonces haga clic en **Sign and send** (Firmar y enviar).
- Autentíquese usando su método de inicio de sesión seguro elegido.

Sellado y envío de un mensaje de correo electrónico

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

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

1. En Microsoft Outlook, haga clic en **Nuevo** o en **Responder**.
2. Redacte su mensaje de correo electrónico.
3. Haga clic en la flecha abajo al lado de **Send Securely** (Enviar con seguridad) y entonces haga clic en **Seal for Trusted Contacts and send** (Sellar para contactos confiables y enviar).
4. Autentíquese usando su método de inicio de sesión seguro elegido.

Visualización de un mensaje de correo electrónico sellado

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

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

Uso de Privacy Manager en Windows Live Messenger

Agregado de la actividad Privacy Manager Chat

Para agregar el recurso Privacy Manager Chat a Windows Live Messenger, siga estos pasos:

1. Inicie la sesión en Windows Live Home.
2. Haga clic en el icono de **Windows Live** y entonces en **Windows Live Services**.
3. Haga clic en **Gallery** (Galería) y luego en **Messenger**.
4. Haga clic en **Activities** (Actividades) y luego en **Safety and Security** (Seguridad).
5. Haga clic en **Privacy Manager Chat** y siga las instrucciones en la pantalla.

Inicio de Privacy Manager Chat

NOTA: Para usar Privacy Manager Chat, ambas partes deben tener Privacy Manager y un certificado de Privacy Manager instalados. Para obtener detalles acerca de la instalación de un certificado Privacy Manager, vea Solicitación e instalación de un certificado de Privacy Manager, en la página 5.

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

   a. Haga clic con el botón derecho en un contacto Live Messenger que esté en línea y seleccione **Start an Activity** (Iniciar una actividad).

   b. Haga clic en **Start Privacy Manager Chat** (Iniciar Privacy Manager Chat).

   – o –

   a. Haga doble clic en un contacto Live Messenger que esté en línea y haga clic en el menú **Conversation** (Conversación).

   b. Haga clic en **Action** (Acción) y luego en **Start Privacy Manager Chat** (Iniciar Privacy Manager Chat).

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

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

Configuración de Privacy Manager Chat para Windows Live Messenger

1. En Privacy Manager Chat, haga clic en el botón **Settings** (Configuración).

   – o –

   En Privacy Manager, haga clic en **Settings** (Configuración) y luego en la ficha **Chat**.

   – o –

   En el Visualizador de historial de Privacy Manager, haga clic en el botón **Settings** (Configuración).

2. Para especificar el tiempo que Privacy Manager Chat espera antes de bloquear su sesión, seleccione un número en la casilla **Lock session after _ minutes of inactivity** (Bloquear sesión después de _ minutos de inactividad).
3. Para especificar una carpeta de historial para sus sesiones de chat, haga clic en **Browse** (Explorar) para buscar una carpeta y entonces haga clic en **OK** (Aceptar).

4. Para encriptar y guardar automáticamente sus sesiones cuando las cierra, seleccione la casilla de verificación **Automatically save secure chat history** (Guardar automáticamente el historial de chat de forma segura).

5. Haga clic en **OK** (Aceptar).

Realización de un chat en la ventana de Privacy Manager Chat

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

- **Save** (Guardar): Haga clic en este botón para guardar su sesión de chat en la carpeta especificada en su configuración. También puede configurar Privacy Manager Chat para que guarde automáticamente cada sesión cuando se cierra.
- **Hide all** (Ocultar todo) y **Show all** (Mostrar todo): Haga clic en el botón apropiado para expandir o cerrar los mensajes que se muestran en la ventana de Comunicaciones seguras. Usted también puede ocultar o mostrar mensajes individuales haciendo clic en el encabezamiento del mensaje.
- **Are you there?** (¿Está usted ahí?): Haga clic en este botón para solicitar la autenticación de su contacto.
- **Lock** (Bloquear): Haga clic en este botón para cerrar la ventana de Privacy Manager Chat y volver a la ventana de entrada de chat. Para mostrar nuevamente la ventana de Comunicaciones seguras, haga clic en **Resume the session** (Reiniciar la sesión) y entonces autentíquese usando su método de inicio de sesión seguro.
- **Send** (Enviar): Haga clic en este botón para enviar un mensaje encriptado a su contacto.
- **Send signed** (Enviar firmado): Seleccione esta casilla de verificación para firmar y encriptar electrónicamente sus mensajes. Entonces, si el mensaje es interferido, estará marcado con no válido cuando el destinatario lo reciba. Debe autenticarse cada vez que envíe un mensaje firmado.
- **Send hidden** (Enviar oculto): Seleccione esta casilla de verificación para encriptar y enviar un mensaje mostrando sólo el encabezamiento del mensaje. Su contacto deberá autenticarse para leer el contenido del mensaje.

Visualilzación del historial de chat

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

Inicio del visualizador de historial de chat

1. Haga clic en **Inicio**, **Todos los programas** y entonces en **HP ProtectTools Security Manager**.
2. Haga clic en **Privacy Manager: Sign and Chat** y entonces haga clic en **Chat History Viewer** (Visualizador de historial de chat).

– o –

▲ En una sesión de chat, haga clic en **History Viewer** (Visualizador de historial) o **History** (Historial).

– o –

▲ En la página “Chat Configuration" (Configuración de chat), haga clic en **Start Live Messenger History Viewer** (Iniciar visualizador de historial de Live Messenger).

Revelación de todas las sesiones

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

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

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

Revelación de sesiones de una cuenta específica

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

1. En el Visualizador de historial de chat, haga clic con el botón derecho en cualquier sesión y luego seleccione **Reveal Session** (Revelar sesión).
2. Autentíquese usando su método de inicio de sesión seguro elegido.

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

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

Visualización de una identidad de sesión

▲ En el visualizador de historial de chat, haga clic con el botón derecho en cualquier sesión revelada y luego seleccione **View session ID** (Ver identidad de sesión).

Visualización de una sesión

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

1. En el Visualizador de historial de chat, haga clic con el botón derecho en cualquier sesión revelada y luego seleccione **View** (Ver).
2. Si se le solicita, autentíquese usando su método de inicio de sesión seguro elegido.

El contenido de la sesión se desencripta.

Búsqueda de un texto específico en las sesiones

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

1. En el Visualizador de historial de chat, haga clic en el botón **Search** (Buscar).
2. Escriba el texto que desea buscar, configure cualquier parámetro deseado y luego haga clic en **OK** (Aceptar).

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

Eliminación de una sesión

1. Seleccione una sesión del historial de chat.
2. Haga clic en **Delete** (Eliminar).

Agregado o eliminación de columnas

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

Para agregar columnas:

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

Para quitar columnas:

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

Filtrado de sesiones mostradas

Se muestra una lista de sesiones de todas sus cuentas en el Visualizador de historial de chat.

Exhibición de sesiones de una cuenta específica

▲ En el Visualizador de historial de chat, seleccione una cuenta del menú **Display history for** (Mostrar historial de).

Exhibición de sesiones entre dos fechas determinadas

1. En el Visualizador de historial de chat, haga clic en el icono **Advanced Filter** (Filtro avanzado).

   Se abre el cuadro de diálogo Advanced Filter (Filtro avanzado).
2. Seleccione la casilla de verificación **Display only sessions within specified date range** (Mostrar sólo sesiones entre las fechas especificadas).

3. En las casillas **From date** (Desde) y **To date** (Hasta), escriba el día, mes y/o año o haga clic en la flecha al lado del calendario para seleccionar las fechas.

4. Haga clic en **OK** (Aceptar).

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

1. En el Visualizador de historial de chat, haga clic en el icono **Advanced Filter** (Filtro avanzado).

2. Seleccione la casilla de verificación **Use an alternate history files folder** (Usar una carpeta de historial de archivos alternativa).

3. Ingrese la ubicación de la carpeta o haga clic en **Browse** (Explorar) para buscar una carpeta.

4. Haga clic en **OK** (Aceptar).

Tareas avanzadas

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

Puede migrar sus certificados de Privacy Manager y sus contactos confiables a otro equipo de forma segura. Para ello, expórtelos como un archivo protegido por una contraseña a un local de red o a cualquier dispositivo de almacenamiento extraíble y entonces importe el archivo al nuevo equipo.

Exportación de certificados de Privacy Manager y contactos confiables

Para exportar sus certificados de Privacy Manager y sus contactos confiables a un archivo protegido por una contraseña, siga estos pasos:

1. Abra Privacy Manager y haga clic en **Migration** (Migración).

2. Haga clic en **Export migration file** (Exportar archivo de migración).

3. En la página “Select Data” (Seleccionar datos), elija las categorías de datos que se incluirán en el archivo de migración y entonces haga clic en **Next** (Siguiente).

4. En la página “Migration File” (Archivo de migración), ingrese un nombre de archivo o haga clic en **Browse** (Explorar) para buscar una ubicación, y entonces haga clic en **Next** (Siguiente).

5. Ingrese y confirme una contraseña y haga clic en **Next** (Siguiente).

NOTA: Guarde esta contraseña en un lugar seguro, ya que la necesitará cuando importe su archivo de migración.

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

7. En la página “Migration File Saved” (Archivo de migración guardado), haga clic en **Finish** (Finalizar).

Importación de certificados de Privacy Manager y contactos confiables

Para importar sus certificados de Privacy Manager y sus contactos confiables a un archivo protegido por una contraseña, siga estos pasos:

1. Abra Privacy Manager y haga clic en **Migration** (Migración).
2. Haga clic en **Import migration file** (Importar archivo de migración).
3. En la página “Select Data” (Seleccionar datos), elija las categorías de datos que se incluirán en el archivo de migración y entonces haga clic en **Next** (Siguiente).
4. En la página “Migration File” (Archivo de migración), ingrese un nombre de archivo o haga clic en **Browse** (Explorar) para buscar una ubicación, y entonces haga clic en **Next** (Siguiente).
5. En la página “Migration File Import” (Importación de archivo de migración), haga clic en **Finish** (Finalizar).

5 File Sanitizer for HP ProtectTools

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

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

Acerca de la eliminación definitiva

La eliminación de un activo en Windows no elimina totalmente el contenido del activo de su unidad de disco duro. Windows sólo elimina la referencia del activo. El contenido del activo permanece en la unidad de disco duro hasta que otro activo sobrescribe la misma área de la unidad de disco duro con nueva infomación.

La eliminación difiere de la eliminación normal de Windows® (también conocida como eliminación simple en File Sanitizer) en que al realizar la eliminación definitiva de un archivo, se utiliza un algoritmo que oscurece los datos, lo que hace prácticamente imposible la recuperación del activo original.

Al elegir un perfil de eliminación definitiva de activos (Alta seguridad, Seguridad media o Baja seguridad), se selecciona automáticamente una lista de activos y un método de borrado para la eliminación definitiva. También puede personalizar un perfil de eliminación definitiva, lo que le permite especificar el número de ciclos de eliminación definitiva, qué activos incluir para la eliminación definitiva, qué activos precisan confirmación antes de la eliminación definitiva y qué activos deben excluirse de la eliminación definitiva.

Puede configurar una programación de eliminación definitiva automática y también puede eliminar definitivamente archivos de forma manual siempre que lo desee.

La limpieza para liberar espacio le permite grabar datos aleatorios sobre los activos eliminados, evitando que los usuarios vean el contenido original de los activos eliminados.

Acerca de la limpieza para liberar espacio

NOTA: La limpieza para liberar espacio es para aquellos activos que elimina usando la Papelera de reciclaje de Windows o aquellos que elimina manualmente. La limpieza para liberación de espacio no suministra seguridad adicional a los activos eliminados definitivamente.

Puede configurar una programación de limpieza para liberar espacio o puede activar el recurso manualmente usando el icono de HP ProtectTools en el área de notificación, en el extremo derecho de la barra de tareas.

Procedimientos de configuración

Apertura de File Sanitizer

Para abrir File Sanitizer:

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

   – o –

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

  – o –

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

Programación de una eliminación definitiva

1. Abra File Sanitizer y haga clic en **Shred** (Eliminación definitiva).
2. Seleccione una opción de eliminación definitiva:

   - **Windows startup** (Inicio de Windows): Elija esta opción para eliminar definitivamente todos los activos seleccionados cuando se inicia Windows.
   - **Windows shutdown** (Cierre de Windows): Elija esta opción para eliminar definitivamente todos los activos seleccionados cuando se cierra Windows.

   NOTA: Cuando se selecciona esta opción, se abre un cuadro de diálogo en el momento del cierre preguntando si desea continuar con la eliminación definitiva de los activos seleccionados o si desea omitir este procedimiento. Haga clic en **Yes** (Sí) para omitir el proceso de eliminación definitiva o en **No** para continuar con la eliminación definitiva.

   - **Web browser open** (Apertura del navegador web): Elija esta opción para eliminar definitivamente todos los activos relacionados con la web seleccionados, como el historial de direcciones del navegador, cuando abre el navegador web.
   - **Web browser quit** (Cierre del navegador web): Elija esta opción para eliminar definitivamente todos los activos relacionados con la web seleccionados, como el historial de direcciones del navegador, cuando cierra el navegador web.
   - **Scheduler** (Programador): Seleccione la casilla de verificación Activate Scheduler (Activar programador), ingrese su contraseña de Windows y entonces escriba un día y una hora para eliminar definitivamente los activos seleccionados.
3. Haga clic en **Apply** (Aplicar) y, a continuación, en **OK** (Aceptar).

Pogramación de una limpieza para liberar espacio

NOTA: La limpieza para liberar espacio es para aquellos activos que elimina usando la Papelera de reciclaje de Windows o aquellos que elimina manualmente. La limpieza para liberar espacio no suministra seguridad adicional a los activos eliminados definitivamente.

Para programar una limpieza para liberar espacio:

1. Abra File Sanitizer y haga clic en **Free Space Bleaching** (Limpieza para liberar espacio).
2. Seleccione la casilla de verificación **Activate Scheduler** (Activar programador), ingrese su contraseña de Windows y entonces escriba un día y una hora para realizar una limpieza en su unidad de disco duro.
3. Haga clic en **Apply** (Aplicar) y, a continuación, en **OK** (Aceptar).

NOTA: La operación de limpieza para liberar espacio puede llevar bastante tiempo. Aunque el procedimiento puede realizarse en segundo plano, su equipo puede funcionar más lentamente debido al aumento del uso del procesador.

Selección o creación de un perfil de eliminación definitiva

Puede especificar un método de eliminación y elegir el activo para eliminar definitivamente seleccionando un perfil predefinido o creando su propio perfil.

Selección de un perfil de eliminación definitiva predefinido

Al elegir un perfil de eliminación definitiva predefinido (Alta seguridad, Seguridad media o Baja seguridad), se selecciona automáticamente una lista de activos y un método de borrado predefinido. Puede hacer clic en el botón View Details (Ver detalles) para ver la lista predefinida de activos seleccionados para su eliminación definitiva.

Para seleccionar un perfil de eliminación definitiva predefinido:

1. Abra **File Sanitizer** y haga clic en **Settings** (Configuración).
2. Haga clic en un perfil de eliminación definitiva predefinido.
3. Haga clic en **View Details** (Ver detalles) para ver la lista de activos seleccionados para su eliminación definitiva.
4. Debajo de **Shred the following** (Eliminar definitivamente lo siguiente), marque la casilla de verificación al lado de cada activo que desee confirmar antes de su eliminación definitiva.
5. Haga clic en **Cancel** (Cancelar) y, a continuación, haga clic en **OK** (Aceptar).

Personalización de un perfil de eliminación definitiva

Al crear un perfil de eliminación definitiva, usted especifica el número de ciclos de eliminación definitiva, qué activos incluir para la eliminación definitiva, qué activos precisan confirmación antes de la eliminación definitiva y qué activos deben excluirse de la eliminación definitiva.

1. Abra File Sanitizer y haga clic en **Settings** (Configuración), en **Advanced Security Settings** (Configuración de seguridad avanzada), y luego haga clic en **View Details** (Ver detalles).

2. Especifique el número de ciclos de eliminación definitiva.

NOTA: El número de ciclos de eliminación definitiva seleccionado se realizará para cada activo. Por ejemplo, si elige tres ciclos de eliminación definitiva, un algoritmo que oscurece los datos se ejecuta tres veces. Si elige el número mayor de ciclos de eliminación definitiva, el proceso puede durar bastante tiempo. Sin embargo, mientras mayor sea el número de ciclos de eliminación definitiva especificado, mayor será la seguridad del equipo.

3. Seleccione los activos que desea eliminar definitivamente:

   a. Debajo de **Available shred options** (Opciones de eliminación disponibles), agregue un activo y entonces haga clic en **Add** (Agregar).

   b. Para agregar un activo personalizado, haga clic en Add Custom Option (Agregar opción personalizada), escriba el nombre de un archivo o de una carpeta y luego haga clic en **OK** (Aceptar). Haga clic en el activo personalizado y luego haga clic en **Add** (Agregar).

   NOTA: Para eliminar un activo de las opciones de eliminación definitiva disponibles, haga clic en el activo y luego en **Delete** (Eliminar).

4. Debajo de **Shred the following** (Eliminar definitivamente lo siguiente), marque la casilla de verificación al lado de cada activo que desee confirmar antes de su eliminación definitiva.

NOTA: Para quitar un activo de la lista de eliminación definitiva, haga clic en el activo y luego en **Remove** (Quitar).

5. Debajo de **Do not shred the following** (No eliminar definitivamente lo siguiente), haga clic en **Add** (Agregar) para seleccionar el activo específico que desea excluir de la eliminación definitiva.

NOTA: Sólo pueden excluirse de la eliminación definitiva extensiones de archivo. Por ejemplo, si usted ha agregado la extensión de archivo .BMP, todos los archivos con la extensión .BMP serán excluidos de la eliminación definitiva.

Para quitar un activo de la lista de exclusiones, haga clic en el activo y luego en **Delete** (Eliminar).

6. Cuando haya terminado de configurar el perfil de eliminación definitiva, haga clic en **Apply** (Aplicar) y luego en **OK** (Aceptar).

Personalización de un perfil de eliminación simple

El perfil de eliminación simple realiza una eliminación de activo estándar sin efectuar una eliminación definitiva. Cuando personaliza un perfil de eliminación simple, usted especifica qué archivos se incluirán en la eliminación simple, qué archivos deberán confirmarse antes de ejecutar una eliminación simple y qué activos deben excluirse de una eliminación simple:

NOTA: Se recomienda enfáticamente que ejecute una limpieza para liberar espacio habitualmente si usa la opción de eliminación simple.

1. Abra **File Sanitizer**, haga clic en **Settings** (Configuración), en **Simple Delete Setting** (Configuración de eliminación simple), y luego haga clic en **View Details** (Ver detalles).
2. Seleccione los activos que desea eliminar:
   a. Debajo de **Available shred options** (Opciones de eliminación definitiva disponibles), haga clic en un activo y entonces haga clic en **Add** (Agregar).
   b. Para agregar un activo personalizado, haga clic en **Add Custom Option** (Agregar opción personalizada), escriba el nombre de un archivo o de una carpeta y luego haga clic en **OK** (Aceptar). Haga clic en el activo personalizado y luego haga clic en **Add** (Agregar).

   NOTA: Para eliminar un activo de las opciones de eliminación disponibles, haga clic en el activo y luego en **Delete** (Eliminar).
3. Debajo de **Delete the following** (Eliminar lo siguiente), marque la casilla de verificación al lado de cada activo que desee confirmar antes de su eliminación.

NOTA: Para quitar un activo de la lista de eliminación, haga clic en el activo y luego en **Remove** (Quitar).

4. Debajo de **Do not shred the following** (No eliminar definitivamente lo siguiente), haga clic en **Add** (Agregar) para seleccionar los activos específicos que desea excluir de la eliminación definitiva.

NOTA: Sólo pueden excluirse de la eliminación extensiones de archivo. Por ejemplo, si usted ha agregado la extensión de archivo .BMP, todos los archivos con la extensión .BMP serán excluidos de la eliminación.

Para quitar un activo de la lista de exclusiones, haga clic en el activo y luego en **Delete** (Eliminar).

5. Cuando haya terminado de configurar el perfil de eliminación simple, haga clic en **Apply** (Aplicar) y luego en **OK** (Aceptar).

Programación de una eliminación definitiva

1. Abra File Sanitizer y haga clic en **Shred** (Eliminación definitiva).
2. Seleccione una opción de eliminación definitiva:
   - **Windows startup** (Inicio de Windows): Elija esta opción para eliminar definitivamente todos los activos seleccionados cuando se inicia Windows.
   - **Windows shutdown** (Cierre de Windows): Elija esta opción para eliminar definitivamente todos los activos seleccionados cuando se cierra Windows.

     NOTA: Cuando se selecciona esta opción, se abre un cuadro de diálogo en el momento del cierre preguntando si desea continuar con la eliminación definitiva de los activos seleccionados o si desea omitir este procedimiento. Haga clic en Yes (Sí) para omitir el proceso de eliminación definitiva o en No para continuar con la eliminación definitiva.
   - **Web browser open** (Apertura del navegador web): Elija esta opción para eliminar definitivamente todos los activos relacionados con la web seleccionados, como el historial de direcciones del navegador, cuando abre el navegador web.

- **Web browser quit** (Cierre del navegador web): Elija esta opción para eliminar definitivamente todos los activos relacionados con la web seleccionados, como el historial de direcciones del navegador, cuando cierra el navegador web.
- **Scheduler** (Programador): Seleccione la casilla de verificación Activate Scheduler (Activar programador), ingrese su contraseña de Windows y entonces escriba un día y una hora para eliminar definitivamente los activos seleccionados.

3. Haga clic en **Apply** (Aplicar) y, a continuación, en **OK** (Aceptar).

Pogramación de una limpieza para liberar espacio

NOTA: La limpieza para liberar espacio es para aquellos activos que elimina usando la Papelera de reciclaje de Windows o aquellos que elimina manualmente. La limpieza para liberar espacio no suministra seguridad adicional a los activos eliminados definitivamente.

Para programar una limpieza para liberar espacio:

1. Abra File Sanitizer y haga clic en **Free Space Bleaching** (Limpieza para liberar espacio).
2. Seleccione la casilla de verificación **Activate Scheduler** (Activar programador), ingrese su contraseña de Windows y entonces escriba un día y una hora para realizar una limpieza en su unidad de disco duro.
3. Haga clic en **Apply** (Aplicar) y, a continuación, en **OK** (Aceptar).

NOTA: La operación de limpieza para liberar espacio puede llevar bastante tiempo. Aunque el procedimiento puede realizarse en segundo plano, su equipo puede funcionar más lentamente debido al aumento del uso del procesador.

Selección o creación de un perfil de eliminación definitiva

Selección de un perfil de eliminación definitiva predefinido

Al elegir un perfil de eliminación definitiva predefinido (Alta seguridad, Seguridad media o Baja seguridad), se selecciona automáticamente una lista de activos y un método de borrado predefinido. Puede hacer clic en el botón View Details (Ver detalles) para ver la lista predefinida de activos seleccionados para su eliminación definitiva.

Para seleccionar un perfil de eliminación definitiva predefinido:

1. Abra **File Sanitizer** y haga clic en **Settings** (Configuración).
2. Haga clic en un perfil de eliminación definitiva predefinido.
3. Haga clic en **View Details** (Ver detalles) para ver la lista de activos seleccionados para su eliminación definitiva.
4. Debajo de **Shred the following** (Eliminar definitivamente lo siguiente), marque la casilla de verificación al lado de cada activo que desee confirmar antes de su eliminación definitiva.
5. Haga clic en **Cancel** (Cancelar) y, a continuación, haga clic en **OK** (Aceptar).

Personalización de un perfil de eliminación definitiva

Al crear un perfil de eliminación definitiva, usted especifica el número de ciclos de eliminación definitiva, qué activos incluir para la eliminación definitiva, qué activos precisan confirmación antes de la eliminación definitiva y qué activos deben excluirse de la eliminación definitiva.

1. Abra File Sanitizer y haga clic en **Settings** (Configuración), en **Advanced Security Settings** (Configuración de seguridad avanzada), y luego haga clic en **View Details** (Ver detalles).
2. Especifique el número de ciclos de eliminación definitiva.

NOTA: El número de ciclos de eliminación definitiva seleccionado se realizará para cada activo. Por ejemplo, si elige tres ciclos de eliminación definitiva, un algoritmo que oscurece los datos se ejecuta tres veces. Si elige el número mayor de ciclos de eliminación definitiva, el proceso puede durar bastante tiempo. Sin embargo, mientras mayor sea el número de ciclos de eliminación definitiva especificado, mayor será la seguridad del equipo.

3. Seleccione los activos que desea eliminar definitivamente:
   a. Debajo de **Available shred options** (Opciones de eliminación disponibles), agregue un activo y entonces haga clic en **Add** (Agregar).
   b. Para agregar un activo personalizado, haga clic en Add Custom Option (Agregar opción personalizada), escriba el nombre de un archivo o de una carpeta y luego haga clic en **OK** (Aceptar). Haga clic en el activo personalizado y luego haga clic en **Add** (Agregar).

NOTA: Para eliminar un activo de las opciones de eliminación definitiva disponibles, haga clic en el activo y luego en **Delete** (Eliminar).

4. Debajo de **Shred the following** (Eliminar definitivamente lo siguiente), marque la casilla de verificación al lado de cada activo que desee confirmar antes de su eliminación definitiva.

NOTA: Para quitar un activo de la lista de eliminación definitiva, haga clic en el activo y luego en **Remove** (Quitar).

5. Debajo de **Do not shred the following** (No eliminar definitivamente lo siguiente), haga clic en **Add** (Agregar) para seleccionar el activo específico que desea excluir de la eliminación definitiva.

NOTA: Sólo pueden excluirse de la eliminación definitiva extensiones de archivo. Por ejemplo, si usted ha agregado la extensión de archivo .BMP, todos los archivos con la extensión .BMP serán excluidos de la eliminación definitiva.

Para quitar un activo de la lista de exclusiones, haga clic en el activo y luego en **Delete** (Eliminar).

6. Cuando haya terminado de configurar el perfil de eliminación definitiva, haga clic en **Apply** (Aplicar) y luego en **OK** (Aceptar).

Personalización de un perfil de eliminación simple

El perfil de eliminación simple realiza una eliminación de activo estándar sin realizar una eliminación definitiva. Cuando personaliza un perfil de eliminación simple, usted especifica qué archivos se incluirán en la eliminación simple, qué archivos deberán confirmarse antes de ejecutar una eliminación simple y qué activos deben excluirse de una eliminación simple:

NOTA: Se recomienda enfáticamente que ejecute una limpieza para liberar espacio habitualmente si usa la opción de eliminación simple.

1. Abra **File Sanitizer**, haga clic en **Settings** (Configuración), en **Simple Delete Setting** (Configuración de eliminación simple), y luego haga clic en **View Details** (Ver detalles).
2. Seleccione los activos que desea eliminar:
   - Debajo de **Available shred options** (Opciones de eliminación definitiva disponibles), haga clic en un activo y entonces haga clic en **Add** (Agregar).
   - Para agregar un activo personalizado, haga clic en **Add Custom Option** (Agregar opción personalizada), escriba el nombre de un archivo o de una carpeta y luego haga clic en **OK** (Aceptar). Haga clic en el activo personalizado y luego haga clic en **Add** (Agregar).

     NOTA: Para eliminar un activo de las opciones de eliminación disponibles, haga clic en el activo y luego en **Delete** (Eliminar).
3. Debajo de **Delete the following** (Eliminar lo siguiente), marque la casilla de verificación al lado de cada activo que desee confirmar antes de su eliminación.

NOTA: Para quitar un activo de la lista de eliminación, haga clic en el activo y luego en **Remove** (Quitar).

4. Debajo de **Do not delete the following** (No eliminar lo siguiente), haga clic en **Add** (Agregar) para seleccionar los activos específicos que desea excluir de la eliminación definitiva.

NOTA: Sólo pueden excluirse de la eliminación extensiones de archivo. Por ejemplo, si usted ha agregado la extensión de archivo .BMP, todos los archivos con la extensión .BMP serán excluidos de la eliminación.

Para quitar un activo de la lista de exclusiones, haga clic en el activo y luego en **Delete** (Eliminar).

5. Cuando haya terminado de configurar el perfil de eliminación simple, haga clic en **Apply** (Aplicar) y luego en **OK** (Aceptar).

Tareas generales

Uso de una secuencia de teclas para iniciar la eliminación definitiva

Para configurar una secuencia de teclas, siga estos pasos:

1. Abra **File Sanitizer** y haga clic en **Shred** (Eliminación definitiva).
2. Seleccione la casilla de verificación **Key sequence** (Secuencia de teclas).
3. Escriba un carácter en la casilla disponible y luego seleccione **CTRL**, **ALT** o **MAYÚS**, o seleccione las tres.

   Por ejemplo, para iniciar la eliminación definitiva automática usando la tecla s y ctrl+mayús, escriba s en la casilla y luego seleccione las opciones **CTRL** y **MAYÚS**.

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

Para iniciar la eliminación definitiva usando una secuencia de teclas:

1. Mantenga presionada la tecla ctrl, alt, o mayús (o la combinación que haya especificado) mientras presiona el carácter elegido.
2. Cuando se abra el cuadro de diálogo de confirmación, haga clic en **Yes** (Sí).

Uso del icono de File Sanitizer

△ **PRECAUCIÓN:** Los activos eliminados definitivamente no pueden recuperarse. Considere cuidadosamente qué elementos selecciona para la eliminación definitiva manual.

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

Eliminación definitiva manual de un activo

△ **PRECAUCIÓN:** Los activos eliminados definitivamente no pueden recuperarse. Considere cuidadosamente qué elementos selecciona para la eliminación definitiva manual.

1. Haga clic con el botón derecho en el icono de **HP ProtectTools** en el área de notificación, en el extremo derecho de la barra de tareas, haga clic en **File Sanitizer** y luego en **Shred One** (Eliminar definitivamente un activo).
2. Cuando se abra el cuadro de diálogo de exploración, navegue hasta el activo que desea eliminar definitivamente y entonces haga clic en **OK** (Aceptar).

   NOTA: El activo seleccionado puede ser un archivo o carpeta individual.

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

– o –

1. Haga clic con el botón derecho en el icono **File Sanitizer** en el escritorio, y entonces haga clic en **Shred One** (Eliminar definitivamente un activo).
2. Cuando se abra el cuadro de diálogo de exploración, navegue hasta el activo que desea eliminar definitivamente y entonces haga clic en **OK** (Aceptar).
3. Cuando se abra el cuadro de diálogo de confirmación, haga clic en **Yes** (Sí).

– o –

1. Abra File Sanitizer y haga clic en **Shred** (Eliminar definitivamente).
2. Haga clic en el botón **Browse** (Explorar).
3. Cuando se abra el cuadro de diálogo de exploración, navegue hasta el activo que desea eliminar definitivamente y entonces haga clic en **OK** (Aceptar).
4. Cuando se abra el cuadro de diálogo de confirmación, haga clic en **Yes** (Sí).

– o –

1. Abra File Sanitizer y haga clic en **Shred** (Eliminar definitivamente).
2. Haga clic en el botón **Shred Now** (Eliminar definitivamente ahora).
3. Cuando se abra el cuadro de diálogo de confirmación, haga clic en **Yes** (Sí).

Eliminación definitiva manual de todos los elementos seleccionados

1. Haga clic con el botón derecho en el icono de **HP ProtectTools** en el área de notificación, en el extremo derecho de la barra de tareas, haga clic en **File Sanitizer** y luego en **Shred Now** (Eliminar definitivamente ahora).
2. Cuando se abra el cuadro de diálogo de confirmación, haga clic en **Yes** (Sí).

– o –

1. Haga clic con el botón derecho en el icono **File Sanitizer** en el escritorio, y entonces haga clic en **Shred Now** (Eliminar definitivamente ahora).
2. Cuando se abra el cuadro de diálogo de confirmación, haga clic en **Yes** (Sí).

Activación manual de la limpieza para liberar espacio

1. Haga clic con el botón derecho en el icono de **HP ProtectTools** en el área de notificación, en el extremo derecho de la barra de tareas, haga clic en **File Sanitizer** y luego en **Bleach now** (Limpiar ahora).
2. Cuando se abra el cuadro de diálogo de confirmación, haga clic en **Yes** (Sí).

– o –

1. Abra File Sanitizer y haga clic en **Free Space Bleaching** (Limpieza para liberar espacio).
2. Haga clic en **Bleach Now** (Limpiar ahora).
3. Cuando se abra el cuadro de diálogo de confirmación, haga clic en **Yes** (Sí).

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

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

Para interrumpir la operación:

▲ Haga clic en el mensaje y entonces haga clic en **Stop** (Detener) para cancelar la operación.

Visualización de archivos de registro

Cada vez que se realiza una eliminación definitiva o una limpieza para liberar espacio, se genera un archivo de registro sobre cualquier error o falla ocurrido. Los archivos de registro siempre se actualizan de acuerdo con la última eliminación definitiva o limpieza para liberar espacio.

NOTA: Los archivos eliminados definitivamente o limpiados no aparecen en los archivos de registro.

Se crea un archivo de registro para las operaciones de eliminación definitiva y uno para las operaciones de limpieza para liberar espacio. Ambos archivos de registro se ubican en la unidad de disco duro, en:

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

6 BIOS Configuration for HP ProtectTools

BIOS Configuration for ProtectTools otorga acceso a los valores de configuración y seguridad de la utilidad de configuración. Esto proporciona a los usuarios acceso a través de Windows a los recursos de seguridad del sistema que son administrados por la utilidad de configuración.

Con BIOS Configuration, puede lograr los siguientes objetivos:

- Administrar contraseñas de administrador.
- Configurar otros recursos de autenticación de inicio, como autenticación de Embedded Security.
- Activar y desactivar recursos de hardware, como arranque por CD-ROM o por puertos de hardware.
- Configurar opciones de arranque, que incluyen la activación de MultiBoot y el cambio del orden de inicio.

NOTA: Muchos de los recursos de BIOS Configuration for ProtectTools están también disponibles en la utilidad de configuración.

Tareas generales

BIOS Configuration le permite administrar varios valores de configuración del equipo a los que sólo podría accederse pulsando f10 en el inicio e ingresando a la utilidad de configuración.

Acceso a BIOS Configuration

Para acceder a BIOS Configuration:

1. Haga clic en **Inicio**, en **Configuración** y, finalmente, en **Panel de control**.
2. Haga clic en **HP ProtectTools Security Manager** y luego en **BIOS Configuration**.

   También puede acceder a BIOS Configuration desde un icono en el área de notificación, en el extremo derecho de la barra de tareas.

   NOTA: Para visualizar el icono de HP ProtectTools Security Manager, haga clic en **Mostrar iconos ocultos** (**<** o **<<**) en el área de notificación.

   - En el área de notificación, haga clic con el botón derecho en el icono **HP ProtectTools Security Manager**.
   - Haga clic en **BIOS Configuration**.
3. Si usted es un usuario de HP ProtectTools, escriba su contraseña de Windows.
   - Si ingresa correctamente la contraseña de Windows pero usted no es un administrador de BIOS, su capacidad para realizar cambios varía de acuerdo con la configuración de nivel de seguridad. Consulte Definición de opciones de seguridad del sistema en la página 67

     NOTA: Un usuario de HP ProtectTools puede ser o no un administrador de BIOS.
   - Si ingresa la contraseña de Windows de forma incorrecta, sólo podrá ver la configuración de BIOS Configuration pero no podrá modificarla.
4. Si usted no es un usuario de HP ProtectTools, el software BIOS Configuration verifica si se ha definido una contraseña de administrador de BIOS.
   - Si se definió una contraseña de administrador de BIOS, debe ingresarla.
     - Si ingresa correctamente una contraseña de administrador de BIOS, podrá ver y realizar modificaciones en la configuración de BIOS Configuration.
     - Si se definió una contraseña de administrador de BIOS pero usted no la ingresa, o la ingresa de forma incorrecta, podrá ver la configuración de BIOS Configuration pero no podrá modificarla.
   - Si no se ha definido una contraseña de administrador de BIOS, podrá ver y realizar cambios en la configuración de BIOS Configuration.

Visualización o cambio de configuraciones

Para ver o cambiar la configuración:

1. Haga clic en una de las páginas de BIOS Configuration:
   - File (Archivo)
   - Security (Seguridad)
   - System Configuration (Configuración de sistema)
2. Realice los cambios y entonces haga clic en **Apply** (Aplicar) para guardar los cambios y dejar la ventana abierta.

   – o –

   Realice los cambios y entonces haga clic en **OK** (Aceptar) para guardar los cambios y cerrar la ventana.
3. Salga y reinicie el equipo.

   Sus cambios se harán efectivos al reiniciar el equipo.

NOTA: Los cambios de contraseña se hacen efectivos de inmediato sin necesidad de reiniciar el equipo.

Visualización de información del sistema

Use la página “File” (Archivo) para ver los siguientes tipos de información:

- Información de identificación del equipo (incluido el número de serie) y de las baterías que se encuentran en el sistema
- Información de las especificaciones del procesador, caché y tamaño de la memoria; versión del video; versión del controlador del teclado y ROM del sistema.

NOTA: La página “File” (Archivo) tiene fines informativos únicamente. Ninguno de los datos mostrados puede modificarse.

Para ver información del sistema:

▲ Acceda a BIOS Configuration y haga clic en **File** (Archivo).

Tareas avanzadas

Definición de opciones de seguridad

Use la página “Security” (Seguridad) de BIOS Configuration para mejorar la seguridad de su equipo.

NOTA: No todas las opciones están disponibles en todos los equipos y también pueden incluirse opciones adicionales.

Para definir las opciones de seguridad:

1. Acceda a BIOS Configuration y haga clic en **Security** (Seguridad).
2. Seleccione una de las opciones enumeradas en el cuadro que aparece a continuación.
3. Cambie la configuración según sea necesario.
4. Haga clic en **Apply** (Aplicar) para aplicar la nueva configuración y dejar la ventana abierta.

   – o –

   Haga clic en **OK** (Aceptar) para aplicar la nueva configuración y cerrar la ventana.

Security (Seguridad)

Opción	Acción
BIOS Administrator Password (Contraseña de administrador de BIOS) **NOTA:** Esta opción puede denominarse “Setup Password” (Contraseña de configuración).	Haga clic en el botón **Set** (Configurar) para definir una contraseña de administrador del BIOS.

System IDs (Identificaciones del sistema)

Opción	Acción
Ownership Tag (Etiqueta de propiedad)	Entrar, ver o modificar.
Asset Tracking Number (Número de rastreo de activo)	Entrar, ver o modificar.

TPM Embedded Security (Seguridad incorporada de TPM)

NOTA: Este recurso sólo se admite en PC equipados con el chip de HP ProtectTools Embedded Security (TPM).

Opción	Acción
Reset of TPM from OS (Restaurar TPM desde el SO)	Activar o desactivar.
OS Management of TPM (Administración de TPM mediante el SO)	Activar o desactivar.
Embedded Security Device Availability (Disponibilidad de dispositivo de seguridad integrada)	Seleccionar disponible u oculto.

Opción	Acción
Power-On Authentication Support (Soporte de autenticación de inicio)	Activar o desactivar soporte para autenticación de inicio de smart card **NOTA:** Este recurso se admite sólo en equipos con lectores de smart card opcionales.
Automatic Drivelock Support (Soporte para Drivelock Automático)	Activar o desactivar.

Administrator Tools (Herramientas de administrador)

Opción	Acción
HP SpareKey	Activar o desactivar.
Fingerprint Reset on Reboot (Reinicio del lector de huellas digitales al arrancar) (si hay uno)	Activar o desactivar.

Password Policy (Política de contraseñas)

Opción	Acción
At least one symbol required (Se requiere por lo menos un símbolo)	Activar o desactivar.
At least one number required (Se requiere por lo menos un número)	Activar o desactivar.
At least one upper case character required (Se requiere por lo menos un carácter en mayúscula)	Activar o desactivar.
At least one lower case character required (Se requiere por lo menos un carácter en minúscula)	Activar o desactivar.
Are spaces allowed in password (Se permiten espacios en la contraseña)	Activar o desactivar.

Hard Disk Sanitization Report (Informe de limpieza de unidad de disco duro)

Opción	Acción
Hard Disk Sanitization (Limpieza de unidad de disco duro)	Si se ha ejecutado una limpieza de unidad de disco duro al menos una vez, puede ver la información sobre los procedimientos de limpieza de disco duro más recientes que se han realizado en el equipo. **NOTA:** Esta opción borra los datos sensibles de una unidad de disco duro del equipo. Si se ha limpiado una unidad de disco duro y luego se la extrajo del equipo, aún estará disponible la información sobre dicho proceso de limpieza.

Definición de opciones de seguridad del sistema

Use la página “System Configuration” (Configuración de sistema) para ver y modificar la configuración del sistema.

NOTA: No todas las opciones están disponibles en todos los equipos y también pueden incluirse opciones adicionales.

Para ajustar las opciones de configuración del sistema:

1. Acceda a **BIOS Configuration** y a continuación haga clic en **System Configuration** (Configuración del sistema).
2. Seleccione una de las opciones del cuadro que aparece a continuación:
   - **Port options (Opciones de puerto)**
   - **Boot options (Opciones de arranque)**
   - **Device configuration options (Opciones de configuración del dispositivo)**
   - **Built-in device options (Opciones de dispositivo integrado)**
   - **AMT options (Opciones AMT) (sólo en algunos modelos)**
   - **Security level options (Opciones de nivel de seguridad)**
3. Cambie la configuración según sea necesario.
4. Haga clic en **Apply** (Aplicar) para aplicar la nueva configuración y dejar la ventana abierta.

   – o –

   Haga clic en **OK** (Aceptar) en la ventana de HP ProtectTools Security Manager para aplicar las nuevas configuraciones al sistema y cerrar la ventana.

Port options (Opciones de puerto)

Opción	Acción
Flash Media Reader (Lector de medios flash)	Activar o desactivar.
USB Ports (Puertos USB)	Activar o desactivar.
1394 port (Puerto 1394)	Activar o desactivar.
Express Card slot (Ranura para Express Card)	Activar o desactivar.

Boot options (Opciones de arranque)

Opción	Acción
Startup Check Delay (Sec) (Demora en la verificación de arranque [seg.])	Definir la demora en la verificación de arranque, en segundos.
Custom Logo (Logotipo personalizado)	Activar o desactivar.
Express Boot Popup Delay (Sec) (Express Boot Popup Delay [seg.])	Determinar la demora emergente de Express Boot en segundos.

Opción	Acción
CD-ROM Boot (Arranque desde CD-ROM)	Activar o desactivar.
SD Card Boot (Arranque desde tarjeta SD)	Activar o desactivar.
Boot from EFI File (Arranque desde archivo EFI)	Activar o desactivar.
Floppy boot (Arranque desde disquete)	Activar o desactivar.
PXE Internal NIC boot (Arranque de NIC interna PXE)	Activar o desactivar.
Boot Order (Orden de arranque)	Definir el orden de arranque de los dispositivos del sistema.

Device configuration options (Opciones de configuración del dispositivo)

Opción	Acción
USB Legacy Support (Soporte USB heredado)	Activar o desactivar.
Parallel port mode (Modo de puerto paralelo)	Seleccionar un modo de puerto paralelo: estándar, bidireccional,EPP (Enhanced Parallel Port) o ECP (Enhanced Capabilities Port).
Fan always on while on AC power (Ventilador siempre encendido mientras se usa la alimentación de CA)	Activar o desactivar el ventilador del sistema cuando está conectado a una toma eléctrica de CA.
Data execution prevention (Prevención de ejecución de datos)	Activar o desactivar la opción para monitorear el uso de la memoria y cerrar programas sospechosos.
SATA device mode (Modo de dispositivo SATA)	Seleccionar IDE, AHCI o RAID.
Dual core CPU (CPU de núcleo doble)	Activar o desactivar.
Secondary battery fast charge (Carga rápida de la batería secundaria)	Activar o desactivar.
HP QuickLook 2	Activar o desactivar.
TXT technology (Tecnología TXT)	Activar o desactivar.
Display Diagnostic URL (Mostrar URL de diagnóstico)	Activar o desactivar.
HDD Translation Mode (Modo de traducción HDD)	Seleccionar Bit-shift (Cambio de bits) o LBA-assisted (Asistido por LBA).
Virtualization technology (Tecnología de virtualización)	Activar o desactivar la opción que permite que múltiples equipos virtuales se ejecuten simultáneamente en el mismo equipo.

Built-in device options (Opciones de dispositivo integrado)

Opción	Acción
Wireless Button State (Estado del botón de conexiones inalámbricas)	Activar o desactivar.
Embedded WWAN Device Radio (Radio de dispositivo WWAN integrado)	Activar o desactivar.
Fingerprint Device (Dispositivo lector de huellas digitales)	Activar o desactivar.

Opción	Acción
Notebook MultiBay (Compartimento multiuso del PC portátil)	Activar o desactivar.
Network Interface Controller (LAN) (Controladora de interfaz de red [LAN])	Activar o desactivar.
Ambient light sensor (Sensor de luz ambiental)	Activar o desactivar.
Embedded Bluetooth® Device Radio (Radio de dispositivo Bluetooth® integrado)	Activar o desactivar.
Wake on LAN	Esta opción le permite encender el equipo de forma remota desde otro equipo conectado a la misma red.

AMT options (Opciones AMT) (sólo en algunos modelos)

Opción	Acción
Terminal Emulation Mode (Modo de emulación de terminal)	Seleccionar ANSI o VT100.
Firmware Verbosity (Verbosidad de firmware)	Activar o desactivar.
Firmware Progress Event Support (Soporte de evento de firmware en progreso)	Activar o desactivar.
Unconfigure AMT on next boot (Desconfigurar AMT en el próximo arranque)	Activar o desactivar.

Security Level options (Opciones de nivel de seguridad)

NOTA: Estos ajustes controlan el nivel de acceso de los usuarios de HP ProtectTools.

Opción	Acción
CD-ROM Boot Security Level (Nivel de seguridad de arranque desde CD-ROM)	Cambiar, ver u ocultar.
Floppy Boot Security Level (Nivel de seguridad de arranque desde disquete)	Cambiar, ver u ocultar.
Internal Network Adapter Boot Security Level (Nivel de seguridad de arranque por adaptador de red interno)	Cambiar, ver u ocultar.
USB Legacy Support Security Level (Nivel de seguridad de soporte USB heredado)	Cambiar, ver u ocultar.
Fan Always on while on AC Power Security Level (Nivel de seguridad de ventilador siempre encendido mientras se usa la alimentación de CA)	Cambiar, ver u ocultar.
Flash Media Reader Security Level (Nivel de seguridad con lector de medios flash)	Cambiar, ver u ocultar.
Startup Check Delay (Sec) Security Level (Nivel de seguridad de la demora en la verificación de arranque [seg.])	Cambiar, ver u ocultar.

Parallel Port Mode Security Level (Nivel de seguridad del modo de puerto paralelo)	Cambiar, ver u ocultar.
Express Boot Popup Delay (Sec) Security Level (Nivel de seguridad de la demora en la ventana emergente de Express Boot [seg.])	Cambiar, ver u ocultar.
LAN/WLAN Switching Security Level (Nivel de seguridad de la alternancia LAN/WLAN)	Cambiar, ver u ocultar.
Embedded Bluetooth Device Radio Security Level (Nivel de seguridad de radio de dispositivo Bluetooth integrado)	Cambiar, ver u ocultar.
Embedded WWAN Device Radio Security Level (Nivel de seguridad de radio de dispositivo WWAN integrado)	Cambiar, ver u ocultar.
Power-On Authentication Support Security Level (Nivel de seguridad de soporte de autenticación de arranque)	Cambiar, ver u ocultar.
Automatic Drivelock Support Security Level (Nivel de seguridad de soporte de Drivelock automático)	Cambiar, ver u ocultar.
Data Execution Prevention Security Level (Nivel de seguridad de prevención de ejecución de datos)	Cambiar, ver u ocultar.
SATA Device Mode Security Level (Nivel de seguridad de modo de dispositivo SATA)	Cambiar, ver u ocultar.
USB Ports Security Level (Nivel de seguridad de puertos USB)	Cambiar, ver u ocultar.
1394 Port Security Level (Nivel de seguridad del puerto 1394)	Cambiar, ver u ocultar.
Express Card Slot Security Level (Nivel de seguridad de ranura para Express Card)	Cambiar, ver u ocultar.
Dual Core CPU Security Level (Nivel de seguridad de CPU de núcleo doble)	Cambiar, ver u ocultar.
Wake on LAN Security Level (Nivel de seguridad de Wake on LAN)	Cambiar, ver u ocultar.
Ambient Light Sensor Security Level (Nivel de seguridad del sensor de luz ambiente)	Cambiar, ver u ocultar.
Secondary Battery Fast Charge Security Level (Nivel de seguridad de carga rápida de la batería secundaria)	Cambiar, ver u ocultar.
Embedded Security Device Availability Security Level (Nivel de seguridad de disponibilidad de dispositivo de seguridad incorporado)	Cambiar, ver u ocultar.
HDD Translation Mode Security Level (Nivel de seguridad de modo de traducción de HDD)	Cambiar, ver u ocultar.
Fingerprint Device Security Level (Nivel de seguridad de dispositivo lector de huellas digitales)	Cambiar, ver u ocultar.
Optical Disk Drive Security Level (Nivel de seguridad de unidad de disco óptico)	Cambiar, ver u ocultar.

Network Interface Controller (LAN) Security Level (Nivel de seguridad de controlador de interfaz de red [LAN])	Cambiar, ver u ocultar.
OS Management of TPM Security Level (Nivel de seguridad de administración de SO de TPM)	Cambiar, ver u ocultar.
Reset of TPM from OS Security Level (Nivel de seguridad de restaurar TPM desde SO)	Cambiar, ver u ocultar.
Virtualization Technology Security Level (Nivel de seguridad de tecnología de virtualización)	Cambiar, ver u ocultar.
Terminal Emulation Mode Security Level (Nivel de seguridad de modo de emulación de terminal)	Cambiar, ver u ocultar.
Firmware Verbosity Security Level (Nivel de seguridad de verbosidad del firmware)	Cambiar, ver u ocultar.
Firmware Progress Event Support Security Level (Nivel de seguridad de soporte de evento en progreso del firmware)	Cambiar, ver u ocultar.
Unconfigure AMT Security Level (Nivel de seguridad de desconfigurar AMT)	Cambiar, ver u ocultar.
Asset Tracking Number Security Level (Nivel de seguridad de número de seguimiento de activo)	Cambiar, ver u ocultar.
Ownership Tag Security Level (Nivel de seguridad de etiqueta de propiedad)	Cambiar, ver u ocultar.
Boot Order Security Level (Nivel de seguridad de orden de arranque)	Cambiar, ver u ocultar.
Custom Logo Policy (Política de logotipo personalizado)	Cambiar, ver u ocultar.
Unconfigure AMT on next boot Security Level (Nivel de seguridad de desconfigurar AMT en el próximo arranque)	Cambiar, ver u ocultar.
SD Card Boot Security Level (Nivel de seguridad de arranque con tarjeta SD)	Cambiar, ver u ocultar.
Boot From EFI File Security Level (Nivel de seguridad de arranque desde archivo EFI)	Cambiar, ver u ocultar.
HP QuickLook 2 Security Level (Nivel de seguridad de HP QuickLook 2)	Cambiar, ver u ocultar.
Wireless Button State Security Level (Nivel de seguridad de estado del botón de conexiones inalámbricas)	Cambiar, ver u ocultar.
Modem Device Security Level (Nivel de seguridad de dispositivo de módem)	Cambiar, ver u ocultar.
Finger Print reset Security Level (Nivel de seguridad de restaurar lector de huellas digitales)	Cambiar, ver u ocultar.
HP SpareKey Security Level (Nivel de seguridad de HP SpareKey)	Cambiar, ver u ocultar.

TXT Technology Security Level (Nivel de seguridad de tecnología TXT)	Cambiar, ver u ocultar.
Diagnostic URL Security Level (Nivel de seguridad de URL de diagnóstico)	Cambiar, ver u ocultar.

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

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

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

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

El chip TPM embedded security optimiza y activa otros recursos de seguridad de HP ProtectTools Security Manager. Por ejemplo, Credential Manager for ProtectTools puede utilizar el chip embedded como un factor de autenticación cuando el usuario inicia la sesión de Windows. En determinados modelos, el chip embedded security TPM también activa recursos de seguridad de BIOS optimizados a los cuales se accede mediante BIOS Configuration for ProtectTools.

Procedimientos de configuración

△ **PRECAUCIÓN:** Para reducir el riesgo de seguridad, se recomienda enfáticamente que su administrador de TI inmediatamente inicialice el chip embedded security. Si no se inicializa el chip embedded security, esto podría provocar que usuarios no autorizados, gusanos o virus informáticos tomen el control del equipo o de las tareas del propietario, como el manejo del archivo de recuperación de emergencia y la configuración del acceso de usuario.

Siga los pasos presentados en las siguientes dos secciones para activar e inicializar el chip embedded security.

Activación del chip embedded security

El chip embedded security debe activarse en la utilidad de configuración. Este procedimiento no puede realizarse en BIOS Configuration for ProtectTools.

Para activar/desactivar el chip embedded security:

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

Inicialización del chip embedded security

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

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

Para inicializar el chip embedded security:

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

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

2. Siga las instrucciones que aparecen en pantalla.

Configuración de una cuenta de usuario básico

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

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

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

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

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

   Aparecerá el asistente para la inicialización de usuario de Embedded Security.

4. Siga las instrucciones que aparecen en pantalla.

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

Tareas generales

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

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

Uso de la unidad segura personal (PSD)

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

Encriptación de archivos y carpetas

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

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

Para encriptar archivos y carpetas:

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

Envío y recepción de correo electrónico encriptado

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

Cambio de la contraseña de la clave de usuario básico

Para cambiar la contraseña clave de usuario básico:

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

Tareas avanzadas

Creación y restauración de copias de seguridad

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

Creación de un archivo de copia de seguridad

Para crear un archivo de copia de seguridad:

1. Haga clic en **Inicio**, **Todos los programas** y entonces en **HP ProtectTools Security Manager**.
2. En el panel izquierdo, haga clic en **Embedded Security**, y luego haga clic en **Copia de seguridad**.
3. En el panel derecho, haga clic en **Copia de seguridad**. Se abrirá el asistente de Embedded Security for ProtectTools Backup.
4. Siga las instrucciones que aparecen en pantalla.

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

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

1. Haga clic en **Inicio**, **Todos los programas** y entonces en **HP ProtectTools Security Manager**.
2. En el panel izquierdo, haga clic en **Embedded Security**, y luego haga clic en **Copia de seguridad**.
3. En el panel derecho, haga clic en **Restaurar**. Se abrirá el asistente de Embedded Security for ProtectTools Backup.
4. Siga las instrucciones que aparecen en pantalla.

Cambio de la contraseña de propietario

Para cambiar la contraseña de propietario:

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

Redefinición de una contraseña de usuario

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

Activación y desactivación de Embedded Security

Es posible desactivar los recursos de Embedded Security si desea trabajar sin la función de seguridad.

Los recursos de Embedded Security pueden activarse o desactivarse en dos niveles diferentes:

- Desactivación temporaria—Con esta opción, embedded security es automáticamente reactivado en el reinicio de Windows. Esta opción está disponible de forma predeterminada para todos los usuarios.
- Desactivación permanente—Con esta opción, la contraseña del propietario es necesaria para reactivar Embedded Security. Esta opción está disponible sólo para administradores.

Desactivación permanente de Embedded Security

Para desactivar permanentemente Embedded Security:

1. Haga clic en **Inicio**, **Todos los programas** y entonces en **HP ProtectTools Security Manager**.
2. En el panel izquierdo, haga clic en **Embedded Security**, y luego haga clic en **Avanzado**.
3. En el panel derecho, en **Embedded Security**, haga clic en **Deshabilitar**.
4. Ingrese su contraseña de propietario cuando se le solicite y luego haga clic en **Aceptar**.

Activación de Embedded Security después de desactivarlo permanentemente

Para activar Embedded Security después de desactivarlo permanentemente:

1. Haga clic en **Inicio**, **Todos los programas** y entonces en **HP ProtectTools Security Manager**.
2. En el panel izquierdo, haga clic en **Embedded Security**, y luego haga clic en **Avanzado**.
3. En el panel derecho, en **Embedded Security**, haga clic en **Habilitar**.
4. Ingrese su contraseña de propietario cuando se le solicite y luego haga clic en **Aceptar**.

Migración de claves con el asistente de migración

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

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

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

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

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

Inicio de servicio en segundo plano

Para que sean aplicados perfiles de dispositivos, el servicio de bloqueo/auditoría de dispositivos en segundo plano de HP ProtectTools debe estar en ejecución. La primera vez que usted intenta aplicar perfiles de dispositivos, HP ProtectTools Security Manager abre una caja de diálogo para preguntar si usted desea iniciar el servicio de segundo plano. Haga clic en **Sí** para iniciar el servicio de segundo plano y definirlo para que inicie automáticamente cuando el sistema inicia.

Configuración sencilla

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

- Dispositivos USB para todos los que no son administradores
- Todos los medios extraíbles (unidades de disquete, pen drives, etc.) para todos los que no son administradores
- Todas las unidades DVD/CD-ROM para todos los que no son administradores
- Todos los puertos en serie y paralelos para todos los que no son administradores

Para negar acceso a una clase de dispositivo para todos los que no son administradores:

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

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

5. Haga clic en **Aceptar**.

Configuración de clases de dispositivos (avanzado)

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

Agregado de un usuario o grupo

1. Haga clic en **Inicio**, **Todos los programas** y entonces en **HP ProtectTools Security Manager**.
2. En el panel izquierdo, haga clic en **Device Access Manager**, y a continuación haga clic en **Configuración de clases de dispositivos**.
3. En la lista de dispositivos, haga clic en la clase de dispositivo que desea configurar.
4. Haga clic en **Agregar**. Aparece el cuadro de diálogo **Seleccionar usuarios o grupos**.
5. Haga clic en **Advanced** (Avanzado) y luego en **Find Now** (Buscar ahora) para buscar usuarios o grupos para agregar.
6. Haga clic en un usuario o grupo para agregarlo a la lista de usuarios y grupos disponibles, y a continuación haga clic en **Aceptar**.
7. Haga clic en **Aceptar**.

Eliminación de un usuario o grupo

1. Haga clic en **Inicio**, **Todos los programas** y entonces en **HP ProtectTools Security Manager**.
2. En el panel izquierdo, haga clic en **Device Access Manager**, y a continuación haga clic en **Configuración de clases de dispositivos**.
3. En la lista de dispositivos, haga clic en la clase de dispositivo que desea configurar.
4. Seleccione el usuario o grupo que desea eliminar, y luego haga clic en **Quitar**.
5. Haga clic en **Aplicar** y, a continuación, haga clic en **Aceptar**.

Negación de acceso a un usuario o grupo

1. Haga clic en **Inicio**, **Todos los programas** y entonces en **HP ProtectTools Security Manager**.
2. En el panel izquierdo, haga clic en **Device Access Manager**, y a continuación haga clic en **Configuración de clases de dispositivos**.
3. En la lista de dispositivos, haga clic en la clase de dispositivo que desea configurar.
4. En **Usuario/Grupos**, haga clic en el usuario o grupo al que se debe negar el acceso.
5. Haga clic en **Denegar**, en el usuario o grupo usuario o grupo al que se le negará el acceso.
6. Haga clic en **Aplicar** y, a continuación, haga clic en **Aceptar**.

Permiso de acceso a una clase de dispositivo para un usuario o grupo

Es posible permitir el acceso de un usuario a una clase de dispositivo mientras niega acceso a todos los otros miembros del grupo de ese usuario.

Para permitir acceso a un usuario pero no al grupo:

1. Haga clic en **Inicio**, **Todos los programas** y entonces en **HP ProtectTools Security Manager**.
2. En el panel izquierdo, haga clic en **Device Access Manager**, y a continuación haga clic en **Configuración de clases de dispositivos**.
3. Haga clic en la clase de dispositivo que desea configurar en la lista de dispositivos.
4. En **Usuario/Grupos**, agregue el grupo grupo al que se le negará el acceso.
5. Haga clic en **Denegar** en el grupo al que se le negará el acceso.
6. Navegue hasta la carpeta debajo de la clase requerida y agregue el usuario específico. Haga clic en **Permitir** para otorgar acceso a este usuario.
7. Haga clic en **Aplicar** y, a continuación, haga clic en **Aceptar**.

Permiso de acceso a un dispositivo específico para un usuario o grupo

Es posible permitir el acceso a un usuario para un dispositivo específico mientras niega acceso a todos los otros miembros del grupo de ese usuario a todos los dispositivos en la clase.

Para permitir el acceso a un dispositivo específico para un usuario pero no al grupo:

1. Haga clic en **Inicio**, **Todos los programas** y entonces en **HP ProtectTools Security Manager**.
2. En el panel izquierdo, haga clic en **Device Access Manager**, y luego haga clic en **Configuración de clases de dispositivos**.
3. En la lista de dispositivos, haga clic en la clase de dispositivo que desea configurar, y a continuación navegue hasta la carpeta que se encuentra debajo.
4. En **Usuario/Grupos**, agregue el grupo al que se le negará el acceso.
5. Haga clic en **Denegar** en el grupo al que se le negará el acceso.
6. Navegue al dispositivo específico que será permitido para el usuario en la lista de dispositivos.
7. Haga clic en **Agregar**. Aparece el cuadro de diálogo **Seleccionar usuarios o grupos**.
8. Haga clic en **Advanced** (Avanzado) y luego en **Find Now** (Buscar ahora) para buscar usuarios o grupos para agregar.
9. Haga clic en un usuario para permitir el acceso, y luego haga clic en **Aceptar**.
10. Haga clic en **Permitir** para otorgar acceso a este usuario.
11. Haga clic en **Aplicar** y, a continuación, haga clic en **Aceptar**.

9 Solución de problemas

Credential Manager for HP ProtectTools

Breve descripción	Detalles	Solución
Con la opción Cuentas de red de Credential Manager, un usuario puede seleccionar en qué cuenta de dominio iniciará la sesión. Cuando se utiliza autenticación TPM, esta opción no está disponible. Todos los otros métodos de autenticación funcionan correctamente.	Con la autenticación TPM, el usuario sólo puede iniciar sesión en el equipo local.	El uso de las herramientas de Single Sign On (Inicio de sesión único) de Credential Manager permite que el usuario autentique otras cuentas.
Las smart cards y tokens USB no están disponibles en Credential Manager si se instalan después de la instalación de Credential Manager.	Para usar smart cards o tokens USB en Credential Manager, el software de soporte (controladores, proveedores PKCS#11, etc.) debe instalarse antes de la instalación de Credential Manager. Si ya ha instalado Credential Manager, siga estos pasos después de la instalación de software para soporte de smart card o token:	Inicie la sesión en Credential Manager. En HP ProtectTools Security Manager, haga clic en **Credential Manager**, en **Advanced Settings** (Configuración avanzada) y luego en la ficha **Smart Cards and Tokens** (Smart cards y tokens). Se mostrará una lista de tokens disponibles debajo de Tokens locales. Acceda a un menú emergente haciendo clic con el botón derecho en el nodo Tokens locales y entonces seleccione Scan for New Smart Cards and Tokens (Buscar nuevas smart cards y tokens). Si se le indica, reinicie el equipo.
Algunas páginas web de aplicaciones crean errores que evitan que el usuario realice o complete tareas.	Algunas aplicaciones basadas en la web dejan de funcionar e informan errores debido al patrón de funcionalidad de desactivación de Single Sign On (Inicio de sesión único). Por ejemplo, un **!** dentro de un triángulo amarillo en Internet Explorer indica que se ha producido un error.	Inicio de sesión único de Credential Manager no admite todas las interfaces web de software. Desactive el soporte para inicio de sesión único para las páginas web específicas apagando el soporte para inicio de sesión único. Vea la documentación completa sobre inicio de sesión único disponible en los archivos de ayuda del software Credential Manager. Si no puede desactivarse un Single Sign On (Inicio de sesión único) específico para una aplicación dada, llame a asistencia técnica de HP y solicite soporte de tercer nivel a través de su contacto de Servicio de HP.
La opción **Browse for Virtual Token** (Buscar token virtual) no aparece durante el proceso de inicio de sesión.	El usuario no puede mover la ubicación de un token virtual registrado en Credential Manager porque se eliminó la opción de buscar para reducir los riesgos de seguridad.	Se eliminó la opción de buscar porque permitía que los no usuarios borraran y cambiaran el nombre de los archivos y tomaran el control de Windows.

Breve descripción	Detalles	Solución
Los administradores de dominio no pueden cambiar la contraseña de Windows ni siquiera con autorización.	Esto sucede después de que un administrador de dominio inicia una sesión en un dominio y registra la identidad del dominio en Credential Manager utilizando una cuenta con derechos de Administrador en el dominio y en el equipo local. Cuando el administrador de dominio intenta cambiar la contraseña de Windows desde Credential Manager, el administrador obtiene un error de falla de inicio de sesión: **Restricción de cuenta de usuario**.	Credential Manager no puede cambiar la contraseña de la cuenta de un usuario de dominio a través de **Change Windows password** (Cambiar contraseña de Windows). Credential Manager sólo puede cambiar las contraseñas de cuentas de PC locales. El usuario de dominio puede cambiar su contraseña a través de la opción **Change password** (Cambiar contraseña) de **Windows security** (Seguridad de Windows) pero, como el usuario de dominio no tiene una cuenta física en el PC local, Credential Manager sólo puede cambiar la contraseña utilizada para iniciar la sesión.
Credential Manager tiene problemas de incompatibilidad con la contraseña GINA de Corel WordPerfect 12.	Si el usuario inicia la sesión en Credential Manager, crea un documento en WordPerfect y lo guarda con protección de contraseña, Credential Manager no puede detectar ni reconocer, ya sea manual o automáticamente, la contraseña GINA.	HP está investigando una solución para mejorías futuras del producto.
Credential Manager no reconoce el botón **Conectar** en la pantalla.	Si las credenciales de Single Sign On (Inicio de sesión único) para Conexión remota de escritorio (Remote Desktop Connection, RDP) están configuradas en **Conectar**, cuando se reinicia Single Sign On (Inicio de sesión único), siempre ingresa **Guardar como** en lugar de **Conectar**.	HP está investigando una solución para mejorías futuras del producto.
Los usuarios pueden perder todas las credenciales de Credential Manager protegidas por TPM.	Si el módulo TPM se elimina o daña, los usuarios pueden perder todas las credenciales protegidas por TPM.	Esto se debe a su diseño. El Módulo TPM está diseñado para proteger las credenciales de Credential Manager. HP recomienda que el usuario cree una copia de seguridad de su identidad desde Credential Manager antes de retirar el módulo TPM.
El usuario no puede iniciar la sesión en Credential Manager después de pasar del estado de suspensión a la hibernación en Windows XP Service Pack 1 únicamente.	Después de permitir que el sistema pase a la hibernación y a la suspensión, el Administrador o usuario no puede iniciar la sesión en Credential Manager y la pantalla de inicio de sesión de Windows continúa apareciendo sin importar qué credencial de inicio de sesión se seleccione (contraseña, huella digital o Java Card).	Actualice Windows a Service Pack 2 a través de Windows Update. Consulte el artículo 813301 de la base de conocimiento de Windows en http://www.microsoft.com para obtener más información sobre el motivo del problema. A fin de iniciar la sesión, el usuario debe seleccionar Credential Manager e iniciar la sesión. Después iniciar la sesión en Credential Manager, se solicita al usuario que inicie la sesión en Windows (el usuario puede tener que seleccionar la opción de inicio de sesión de Windows) para completar el proceso de inicio de sesión. Si el usuario primero inicia la sesión en Windows, a continuación el usuario debe iniciar la sesión manualmente en Credential Manager.
La restauración de Embedded Security hace que Credential Manager falle.	Credential Manager no registra ninguna credencial después de que la ROM se restaura a la configuración de fábrica.	Credential Manager no accede a TPM si se restaura la ROM a la configuración de fábrica después de instalar Credential Manager. El chip TPM de Embedded Security puede activarse utilizando la utilidad de configuración f10, BIOS Configuration o HP Client Manager. Para activar el chip

Breve descripción	Detalles	Solución
		TPM de Embedded Security utilizando la utilidad de configuración, siga estos pasos: 1. Abra la utilidad de configuración iniciando o reiniciando el equipo y entonces presione f10 mientras aparece el mensaje **F10 = ROM Based Setup** en el ángulo inferior izquierdo de la pantalla. 2. Utilice las teclas de flecha para hacer clic en **Security** (Seguridad) y a continuación en **Setup Password** (Contraseña de arranque). Defina una contraseña. 3. Seleccione **Embedded Security Device (Dispositivo de Embedded Security)**. 4. Utilice las teclas de flechas para seleccionar **Embedded Security Device—Disable (Dispositivo de Embedded Security—Desactivar)**. Utilice las teclas de flechas para cambiar a **Embedded Security Device—Enable (Dispositivo de Embedded Security—Activar)**. 5. Haga clic en **Enable** (Activar) y luego en **Save changes and exit** (Guardar cambios y salir). HP está investigando opciones de resolución para las futuras versiones de software de cliente.
El proceso de seguridad **Restore Identity (Restaurar identidad)** pierde la asociación con el token virtual.	Cuando el usuario restaura la identidad, Credential Manager puede perder la asociación con la ubicación del token virtual en la pantalla de inicio de sesión. Aunque Credential Manager tiene registrado el token virtual, el usuario debe volver a registrar el token para restaurar la asociación.	Esto es actualmente debido al diseño. Cuando se desinstala Credential Manager sin mantener las identidades, la parte del sistema (servidor) del token se destruye, de modo que el token no puede utilizarse más para iniciar la sesión, incluso si la parte cliente del token se restaura a través de la restauración de la identidad. HP está investigando opciones de resolución a largo plazo.

Embedded Security for HP ProtectTools (sólo en algunos modelos)

Breve descripción	Detalles	Solución
La encriptación de carpetas, subcarpetas y archivos en una PSD causa un mensaje de error.	Si el usuario copia archivos y carpetas en una PSD e intenta encriptar carpetas/archivos o carpeta/subcarpetas, aparecerá el mensaje **Error Applying Attributes** (Error al aplicar atributos). El usuario puede encriptar los mismos archivos en la unidad C:\ o una unidad de disco duro adicional instalada.	Esto se debe a su diseño. Si se mueven archivos/carpetas a una PSD, automáticamente se encriptan. No es necesaria la "doble encriptación" de los archivos/carpetas. Intentar la doble encriptación en una PSD con EFS produce este mensaje de error.
No se puede tomar la propiedad con otro SO en la plataforma MultiBoot.	Si se configura una unidad para inicio múltiple del SO, la propiedad sólo puede tomarse con el asistente para la inicialización de la plataforma en un sistema operativo.	Esto se debe al diseño, por motivos de seguridad.
Un administrador no autorizado puede visualizar, eliminar, cambiar el nombre o mover el contenido de las carpetas EFS encriptadas.	La encriptación de una carpeta no evita que un usuario no autorizado con derechos administrativos visualice, elimine o mueva el contenido de la carpeta.	Esto se debe a su diseño. Este es un recurso de EFS, no del TPM de Embedded Security. Embedded Security utiliza el software EFS de Microsoft y EFS preserva los derechos de acceso al archivo/carpeta para todos los administradores.
El usuario no tiene opciones de encriptación cuando intenta restaurar la unidad de disco duro utilizando FAT32.	Si el usuario intenta restaurar la unidad de disco duro utilizando FAT32, no habrá opciones de encriptación para los archivos/carpetas que utilicen EFS.	Esto se debe a su diseño. No debe instalarse software en una restauración con una partición de FAT32. EFS de Microsoft se admite únicamente en NTFS y no funciona en FAT32. Esta es una característica de EFS de Microsoft y no se relaciona con el software HP ProtectTools.
El usuario puede encriptar o eliminar el archivo XML del archivo de recuperación.	Por diseño, no se configuran ACL para esta carpeta; por lo tanto, un usuario puede involuntaria o deliberadamente encriptar o eliminar el archivo, haciéndolo inaccesible. Después de haber encriptado o eliminado este archivo, nadie puede utilizar el software TPM.	Esto se debe a su diseño. Los usuarios tienen derechos de acceso a un archivo de emergencia para poder guardar/actualizar su copia de seguridad de la Clave de usuario básico. Debe instruirse a los usuarios para que nunca encripten ni eliminen los archivos del archivo de recuperación.
La interacción de Embedded Security EFS con Symantec Antivirus o McAfee Total Protection produce tiempos más prolongados de encriptación y desencriptación y de exploración.	Los archivos encriptados interfieren con la exploración de virus de Symantec Antivirus o McAfee Total Protection. La encriptación de archivos usando Embedded Security EFS tarda más cuando se ejecuta Symantec Antivirus o McAfee Total Protection.	Para reducir el tiempo necesario para escanear los archivos EFS de Embedded Security, el usuario puede escribir la contraseña de encriptación antes del escaneo o desencriptar antes del escaneo. Para reducir el tiempo necesario para encriptar y desencriptar datos usando Embedded Security EFS, el usuario deberá desactivar la protección automática en Symantec Antivirus o McAfee Total Protection.
El archivo de recuperación de emergencia no puede guardarse en medios extraíbles.	Si el usuario inserta una tarjeta de memoria MultMediaCard o Secure Digital (SD) cuando se crea la ruta del archivo de recuperación de emergencia durante la inicialización de Embedded Security, aparecerá un mensaje de error.	Esto se debe a su diseño. No se admite el almacenamiento del archivo de recuperación en medios extraíbles. El archivo de recuperación puede almacenarse en una unidad de red o en otra unidad local distinta de la unidad C.
Se producen errores después de que una	Si se produce una pérdida de energía durante la inicialización del chip de	Realice el siguiente procedimiento para recuperarse de la pérdida de energía:

Breve descripción	Detalles	Solución
perdida de energía interrumpe la inicialización de Embedded Security.	Embedded Security, surgen los siguientes problemas: • Cuando se intenta iniciar el asistente para la inicialización de Embedded Security, aparece el siguiente mensaje de error: **Embedded security no puede inicializarse debido a que el chip de Embedded Security ya tiene un propietario de Embedded Security.** • Cuando se intenta iniciar el asistente para la inicialización de usuario, aparece el siguiente mensaje de error: **No se inicializa Embedded Security. Para utilizar el asistente, primero se debe inicializar Embedded Security.**	**NOTA:** Utilice las teclas de flecha para seleccionar varios menús, elementos de menú y cambiar valores (a menos que se especifique lo contrario). 1. Inicie o reinicie el equipo. 2. Presione f10 cuando aparece el mensaje **f10=Setup** en la pantalla. 3. Seleccione la opción de idioma adecuada. 4. Presione intro. 5. Seleccione **Security** (Seguridad) y entonces haga clic en **Embedded Security**. 6. Configure la opción **Embedded Security Device (Dispositivo de Embedded Security)** para **Enable (Activar)**. 7. Presione f10 para aceptar el cambio. 8. Seleccione **Archivo** y luego **Salir guardando los cambios**. 9. Presione intro. 10. Presione f10 para guardar los cambios y salir de la utilidad.
La contraseña de la utilidad de configuración (**f10**) puede eliminarse después de activar el Módulo TPM.	La activación del módulo TPM requiere una contraseña de la utilidad de configuración (**f10**). Cuando el módulo ha sido activado, el usuario puede eliminar la contraseña. Esto permite que cualquiera con acceso directo al sistema reinicie el módulo TPM y ocasione una posible pérdida de datos.	Esto se debe a su diseño. La contraseña de la utilidad de configuración (**f10**) sólo puede ser eliminada por un usuario que la conozca. Sin embargo, HP recomienda enfáticamente que se proteja la contraseña de la utilidad de configuración (**f10**) en todo momento.
Ya no aparece el cuadro de contraseña de una PSD cuando el sistema se activa después del modo de espera.	Cuando un usuario inicia una sesión en el sistema después de crear una PSD, TPM solicita la contraseña de usuario básico. Si el usuario no escribe la contraseña y el sistema inicia el modo de espera, el cuadro de diálogo de la contraseña ya no está disponible cuando el usuario reanuda.	Esto se debe a su diseño. El usuario tiene que cerrar la sesión y volver a iniciar para visualizar de nuevo el cuadro de la contraseña de una PSD.
No se necesita contraseña para cambiar las Políticas de seguridad de la plataforma.	El acceso a las Políticas de seguridad de la plataforma (tanto Equipo como Usuario) no requiere una contraseña de TPM para los usuarios que tienen derechos administrativos en el sistema.	Esto se debe a su diseño. Cualquier administrador puede modificar las Políticas de la plataforma de seguridad con o sin la inicialización del usuario de TPM.
Cuando se visualiza un certificado, se muestra como no confiable.	Después de configurar HP ProtectTools y ejecutar el asistente para la inicialización del usuario, el usuario tiene la capacidad de visualizar el certificado emitido; sin embargo, cuando se visualiza el certificado, se muestra como no confiable. Si bien el certificado puede instalarse en este momento al hacer clic en el botón Instalar, la instalación no lo hace confiable.	Los certificados autofirmados no son confiables. En un entorno empresarial debidamente configurado, los certificados de EFS son emitidos por las Autoridades de Certificación en línea y son confiables.

Breve descripción	Detalles	Solución
Se produce un error intermitente de encriptación y desencriptación: **El proceso no puede acceder al archivo porque está siendo utilizado por otro proceso.**	Este es un error extremadamente intermitente durante la encriptación y desencriptación del archivo que se produce porque el archivo está siendo utilizado por otro proceso, aunque dicho archivo o carpeta no está siendo procesado por el sistema operativo u otras aplicaciones.	Para resolver la falla: 1. Reinicie el sistema. 2. Cierre la sesión. 3. Vuelva a iniciar la sesión.
Se produce la pérdida de datos en el almacenamiento extraíble si se extraen los medios de almacenamiento antes de completar la generación o transferencia de nuevos datos.	La extracción de los medios de almacenamiento como la unidad de disco duro MultiBay aún muestra la disponibilidad de una PSD y no genera errores mientras se agregan/modifican datos en una PSD. Después de reiniciar el sistema, la PSD no refleja los cambios del archivo que se produjeron mientras no estaba disponible el almacenamiento extraíble.	No extraiga una PSD antes de finalizar la generación o transferencia de los datos. Este problema sólo se experimenta si el usuario accede a la PSD, luego extrae la unidad de disco duro antes de finalizar la generación o la transferencia de los nuevos datos. Si el usuario intenta acceder a la PSD cuando la unidad de disco duro extraíble no está presente, se muestra un mensaje de error que indica que **el dispositivo no está listo**.
Durante la desinstalación, si el usuario no ha inicializado el usuario básico y abre la herramienta de Administración, la opción **Desactivar** no está disponible y el Desinstalador no continuará hasta que se cierre la herramienta de Administración.	El usuario tiene la opción de desinstalar, ya sea sin desactivar el TPM o desactivando primero el TPM (a través de la herramienta de Administración), y luego desinstalando. El acceso a la herramienta de Administración requiere la inicialización de la Clave de usuario básico. Si no se ha producido la inicialización básica, todas las opciones están inaccesibles para el usuario. Debido a que el usuario ha optado expresamente por abrir la herramienta de Administración (haciendo clic en **Sí** en el cuadro de dialogo que solicita **Click Yes to open Embedded Security Administration tool**) (Haga clic en Sí para abrir la herramienta de Administración de Embedded Security), la desinstalación aguarda hasta que se cierre la herramienta de Administración. Si el usuario hace clic en **No** en dicho cuadro de diálogo, la herramienta de Administración no se abre en absoluto y continúa la desinstalación.	La herramienta de Administración se utiliza para desactivar el chip TPM, pero dicha opción no está disponible a menos que ya se haya inicializado la Clave de usuario básico. Si no ha sido inicializada, seleccione **Aceptar** o **Cancelar** para continuar con la desinstalación.
Se produce el bloqueo intermitente del sistema después de crear una PSD en cuentas de dos usuarios y utilizar la conmutación de usuario rápida en configuraciones de sistema de 128 MB.	El sistema se puede bloquear con una pantalla negra y un teclado y mouse que no responden en lugar de mostrar la pantalla de bienvenida (inicio de sesión) cuando se utiliza la conmutación rápida de usuario con RAM mínima.	Se sospecha que la causa fundamental es un problema de tiempo en configuraciones de memoria baja. Los gráficos integrados utilizan arquitectura UMA que lleva 8 MB de memoria, lo que deja únicamente 120 MB disponibles para el usuario. El error se genera cuando estos 120 MB son compartidos por ambos usuarios que inician sesión y tienen conmutación rápida de usuario. La solución consiste en reiniciar el sistema y aumentar la configuración de la memoria (HP no provee configuraciones de 128 MB con los módulos de seguridad).

Breve descripción	Detalles	Solución
La Autenticación del usuario EFS (solicitud de contraseña) se agota con **acceso negado**.	La contraseña de Autenticación del usuario EFS se reabre después de que el usuario hace clic en **Aceptar** o el sistema sale del modo de espera.	Esto es por diseño (para evitar problemas con EFS de Microsoft, se creó un temporizador de vigilancia de 30 segundos para generar el mensaje de error).
Se observa un truncamiento menor durante la configuración de japonés en descripciones funcionales.	Se truncan las descripciones funcionales durante la opción de configuración personalizada durante el asistente de instalación.	HP corregirá esto en una versión futura.
EFS Encryption funciona sin que se escriba una contraseña en el indicador.	Al permitir que se agote el tiempo del indicador de la contraseña del Usuario, aún se dispone de encriptación en el archivo o la carpeta.	La capacidad de encriptar no requiere la autenticación de contraseña, debido a que esta es una característica de encriptación de EFS de Microsoft. La desencriptación requerirá que se proporcione la contraseña del usuario.
El correo electrónico seguro no es compatible, aun cuando no se especifica el correo electrónico seguro en el asistente para la inicialización del usuario o cuando la configuración de correo electrónico seguro está desactivada en las políticas del usuario.	El software Embedded Security y el asistente no controlan la configuración de un cliente de correo electrónico (Outlook, Outlook Express, o Netscape).	Este comportamiento se debe a su diseño. La configuración de los valores de correo electrónico de TPM no prohíbe la edición de la configuración de encriptación directamente en un cliente de correo electrónico. El uso de correo electrónico seguro es configurado y controlado por aplicaciones de terceros. El asistente de HP permite la vinculación a las tres aplicaciones de referencia para su personalización inmediata.
La ejecución de Large Scale Deployment una segunda vez en el mismo equipo o en un equipo previamente inicializado sobrescribe los archivos de recuperación de emergencia y token de emergencia. Los nuevos archivos no son útiles para la recuperación.	La ejecución de Large Scale Deployment en cualquier sistema HP ProtectTools Embedded Security previamente inicializado inutiliza los archivos de recuperación y los tokens de recuperación al sobrescribir dichos archivos XML.	HP está trabajando para resolver el problema de sobreescritura del archivo XML y proporcionará una solución en un futuro SoftPaq.
Los scripts automatizados de inicio de sesión no funcionan durante la restauración del usuario en Embedded Security.	El error se produce después de que el usuario realiza las siguientes acciones: • Inicializa el propietario y el usuario en Embedded Security (utilizando las ubicaciones predeterminadas—**Mis Documentos**). • Reconfigura el chip con la configuración de fábrica en el BIOS. • Reinicia el equipo. • Comienza a restaurar Embedded Security. Durante el proceso de restauración, Credential Manager pregunta si el sistema puede automatizar el inicio de sesión a Autenticación del usuario de TPM de Infineon. Si el usuario	Haga clic en el botón **Examinar** en la pantalla para seleccionar la ubicación y el proceso de restauración continúa.

Breve descripción	Detalles	Solución
	selecciona **Sí**, la ubicación de SPEmRecToken se muestra automáticamente en el cuadro de texto. Si bien esta ubicación es correcta, aparece el siguiente mensaje de error: **No Emergency Recovery Token is provided. Select the token location the Emergency Recovery Token should be retrieved from** (No se proporciona token de recuperación de emergencia. Seleccione la ubicación del token desde donde debe recuperarse el token de recuperación de emergencia).	
Las PSD de usuarios múltiples no funcionan como un entorno de conmutación rápida de usuario.	Este error se produce cuando se han creado múltiples usuarios y se ha otorgado una PSD con la misma letra de unidad. Si se intenta hacer una conmutación de rápida de usuario entre los usuarios cuando se carga la PSD, la PSD del segundo usuario no está disponible.	La PSD del segundo usuario estará disponible únicamente si se reconfigura para utilizar otra letra de unidad o si el primer usuario cierra la sesión.
La PSD está desactivado y no puede eliminarse después de formatear la unidad de disco duro en la que se generó la PSD.	El icono de la PSD aún está visible, pero aparece el mensaje de error **no puede accederse a la unidad** cuando el usuario intenta acceder a la PSD. El usuario no puede eliminar la PSD y aparece el siguiente mensaje: **your PSD is still in use, please be sure that your PSD contains no open files and is not accessed by another process** (su PSD aún está en uso, asegúrese de que su PSD no contenga archivos abiertos y de que no acceda ningún otro proceso). El usuario debe reiniciar el sistema a fin de eliminar la PSD y no se carga después del reinicio.	De acuerdo con el diseño: Si un cliente elimina por la fuerza o se desconecta de la ubicación de almacenamiento de los datos de la PSD, la emulación de la unidad PSD de Embedded Security continúa funcionando y producirá errores basados en la falta de comunicación con los datos faltantes. Resolución: Después del próximo reinicio, las emulaciones no se cargan y el usuario puede eliminar la emulación anterior de la PSD y crear una nueva PSD.
Se detecta un error interno cuando el usuario restaura desde el archivo de copia de seguridad automática.	En Embedded Security, si el usuario hace clic en la opción **Restore under Backup** (Restaurar en copia de seguridad) para restaurar desde el archivo de copia de seguridad automática y luego selecciona **SPSystemBackup.xml**, falla el asistente de Restauración y aparece el siguiente mensaje de error: **The selected Backup Archive does not match the restore reason. Please select another archive and continue** (El archivo de copia de seguridad seleccionado no coincide con el motivo de la restauración. Seleccione otro archivo y continúe).	Si el usuario selecciona **SpSystemBackup.xml** cuando se requiere SpBackupArchive.xml, el asistente de Embedded Security falla y aparece el siguiente mensaje: **An internal Embedded Security error has been detected** (Se ha detectado un error interno de Embedded Security). El usuario debe seleccionar el archivo XML correcto que coincida con el motivo requerido. Los procesos funcionan de acuerdo con el diseño y de forma correcta; sin embargo, el mensaje de error interno de Embedded Security no es claro y debería indicar un mensaje más adecuado. HP está trabajando para mejorar esto en productos futuros.
El sistema de seguridad muestra un error de restauración con múltiples usuarios.	Durante el proceso de restauración, si el administrador selecciona usuarios para restaurar, los usuarios no seleccionados no pueden restaurar las claves cuando	Los usuarios no seleccionados pueden restaurarse al reconfigurar el TPM, ejecutar el proceso de restauración y seleccionar todos los usuarios antes de que se ejecute la próxima copia de seguridad diaria

Breve descripción	Detalles	Solución
	lo intentan posteriormente. Aparece un mensaje de error **ha fallado el proceso de desencriptación**.	predeterminada. Si se ejecuta la copia de seguridad automática, se sobrescriben los usuarios no restaurados y se pierden sus datos. Si se almacena una nueva copia de seguridad del sistema, los usuarios no seleccionados previamente no pueden restaurarse. Asimismo, el usuario debe restaurar toda la copia de seguridad del sistema. Una copia de seguridad de archivo puede restaurarse individualmente.
La reconfiguración de la ROM del sistema al valor predeterminado oculta el TPM.	La reconfiguración de la ROM del sistema al valor predeterminado oculta el TPM para Windows. Esto no permite que el software de seguridad funcione correctamente y hace que los datos encriptados del TPM sean inaccesibles.	Revelar el TPM en el BIOS: Abra la utilidad de configuración (**f10**), navegue hasta **Security** (Seguridad) > **Device security** (Seguridad de dispositivo), y entonces cambie el campo **Hidden** (Oculto) por **Available** (Disponible).
La copia de seguridad automática no funciona con la unidad mapeada.	Cuando un administrador configura la copia de seguridad automática en Embedded Security, crea una entrada en **Windows** > **Tareas** > **Tareas programadas**. La tarea programada de Windows está configurada para usar NT AUTHORITY\SYSTEM para los derechos para ejecutar la copia de seguridad. Esto funciona adecuadamente en cualquier unidad local. En cambio, cuando el administrador configura la copia de seguridad automática para guardar en una unidad asociada, el proceso falla debido a que NT AUTHORITY\SYSTEM no tiene los derechos para utilizar la unidad asociada. Si se programa la copia de seguridad automática para que se realice en el inicio de sesión, el icono de Embedded Security TNA muestra el siguiente mensaje: **Actualmente no puede accederse a la ubicación del archivo de copia de seguridad. Haga clic aquí si desea una copia de seguridad en un archivo temporal hasta que pueda accederse nuevamente al archivo de copia de seguridad.** Sin embargo, si se programa una copia de seguridad automática para una hora específica, la copia de seguridad falla sin mostrar el aviso de la falla.	La solución consiste en cambiar NT AUTHORITY \SYSTEM a (nombre del equipo)\(nombre del administrador). Esta es la configuración predeterminada si la Tarea programada se crea manualmente. HP está trabajando para proveer las versiones futuras del producto con una configuración predeterminada que incluya nombre del equipo\nombre del administrador.
Embedded Security no puede desactivarse temporalmente en la GUI de Embedded Security.	El software 4.0 actual fue diseñado para las implementaciones de HP Notebook 1.1B, así como también es compatible con HP Desktop 1.2. Esta opción de desactivación aún se admite en la interfaz del software para las plataformas TPM 1.1.	HP resolverá este problema en versiones futuras.

Device Access Manager for HP ProtectTools

Breve descripción	Detalles	Solución
Se ha negado el acceso a los usuarios a dispositivos dentro de Device Access Manager, pero los dispositivos aún están accesibles.	Se han utilizado Configuración sencilla y/o Configuración de clases de dispositivos en Device Access Manager para negar a los usuarios el acceso a los dispositivos. A pesar se haberse negado el acceso, los usuarios aún pueden acceder a los dispositivos.	Verifique que se haya iniciado el servicio de Bloqueo de dispositivos de HP ProtectTools. Como un usuario administrativo, navegue hasta **Panel de control > Herramientas administrativas > Servicios**. En la ventana **Servicios**, busque el servicio **HP ProtectTools Device Locking/Auditing** (Bloqueo/auditoría de dispositivo HP ProtectTools). Asegúrese de que el servicio esté iniciado y de que el tipo de inicio sea **Automatic** (Automático).
Un usuario tiene acceso inesperado a un dispositivo o inesperadamente se niega el acceso de un usuario a un dispositivo.	Se ha utilizado Device Access Manager para negar el acceso de los usuarios a algunos dispositivos y permitir que los usuarios accedan a otros dispositivos. Cuando el usuario está utilizando el sistema, pueden acceder a dispositivos para los cuales consideran que Device Access Manager ha negado el acceso y se les niega el acceso a dispositivos que consideran que Device Access Manager debería permitir.	Debería utilizarse la Configuración de clases de dispositivos en Device Access Manager para investigar la configuración de dispositivos de los usuarios. Haga clic en **Security Manager**, luego en **Device Access Manager** y en **Device Class Configuration** (Configuración de clase de dispositivo). Expanda los niveles del árbol de clase de dispositivo y revise la configuración aplicable al usuario. Verifique si hay permisos denegados que puedan configurarse para el usuario o algún grupo de Windows del que pueda ser miembro, como Usuarios o Administradores.
Permitir o negar ¿cuál tiene prioridad?	En Configuración de clases de dispositivos, puede definirse la siguiente configuración: • Se ha otorgado el privilegio Permitir a un grupo de Windows (por ejemplo, BUILTIN\Administrators) y se ha otorgado el privilegio Negar permiso a otro grupo de Windows (por ejemplo, BUILTIN\Users) en el mismo nivel en la jerarquía de clase de dispositivo (por ejemplo, unidades de DVD/CD-ROM). Si un usuario es miembro de ambos grupos (por ejemplo, Administrador), ¿cuál tiene prioridad?	Se ha negado al usuario el acceso al dispositivo. Negar tiene prioridad sobre Permitir. Se niega el acceso debido a la forma en la que Windows define el permiso efectivo para el dispositivo. Se le niega un grupo y se le permite un grupo, pero el usuario es miembro de ambos grupos. Se le niega al usuario porque negar el acceso tiene prioridad sobre permitir el acceso. Una solución es negar el grupo de Usuarios a nivel de las unidades de DVD/CD-ROM y permitir el grupo de Administradores al nivel por debajo de las unidades de DVD/CD-ROM. Una solución adicional sería tener grupos específicos de Windows, uno para permitir el acceso a DVD/CD y uno para negar el acceso a DVD/CD. Los usuarios específicos se agregarían entonces al grupo correspondiente.

Varios

Software afectado: breve descripción	Detalles	Solución
Security Manager-Advertencia recibida: **The security application can not be installed until the HP Protect Tools Security Manager is installed** (La aplicación de seguridad no puede instalarse hasta que HP Protect Tools Security Manager no esté instalado).	Todas las aplicaciones de seguridad como Embedded Security, Java Card Security, y biométrica tienen complementos expansibles para la interfaz de Security Manager. Security Manager debe estar instalado antes de poder cargarse un complemento de seguridad aprobado por HP.	El software Security Manager debe estar instalado antes de instalar cualquier complemento de seguridad.
Utilidad de actualización de firmware de TPM para los modelos que contienen TPM activado por Broadcom: la herramienta provista a través del sitio web de soporte de HP informa que **se requiere propiedad**.	Este es el comportamiento esperado de la utilidad de firmware de TPM para los modelos que contienen TPM activados con Broadcom. La herramienta de actualización del firmware permite que el usuario actualice el firmware, con o sin una clave de aprobación (EK). Cuando no existe EK, no se requiere autorización para completar la actualización del firmware. Cuando existe una EK, debe existir un propietario de TPM, debido a que la actualización requiere la autorización del propietario. Después de la actualización satisfactoria, debe reiniciarse la plataforma para que el firmware surta efecto. Si el TPM del BIOS está configurado de fábrica, se elimina la propiedad y la se evita la capacidad de actualización del firmware hasta que la plataforma del software Embedded Security y el asistente para la inicialización del usuario se hayan configurado. **NOTA:** Siempre se recomienda un reinicio después de realizar una actualización del firmware. La versión del firmware no se identifica correctamente hasta después del reinicio.	1. Reinstale el software Embedded Security. 2. Ejecute el Asistente de configuración de plataforma y usuario. 3. Asegúrese de que el sistema contenga la instalación de Microsoft .NET framework 1.1: **a.** Haga clic en **Inicio**. **b.** Haga clic en **Panel de control**. **c.** Haga clic en **Agregar o quitar programas**. **d.** Asegúrese de que se enumere **Microsoft .NET Framework 1.1**. 4. Verifique la configuración de hardware y software: **a.** Haga clic en **Inicio**. **b.** Haga clic en **Todos los programas**. **c.** Haga clic en **HP ProtectTools Security Manager**. **d.** Seleccione **Embedded Security** en el menú del árbol. **e.** Haga clic en **Más detalles**. El sistema debería tener la siguiente configuración: • Versión del producto = V4.0.1 • Estado de Embedded Security: Estado del chip = Activado, Estado del propietario = Inicializado, Estado del usuario = Inicializado • Información del componente: Versión de TCG Spec. = 1.2 • Proveedor = Broadcom Corporation

Software afectado: breve descripción	Detalles	Solución
		• Versión del firmware = 2.18 (o superior) • Versión de la biblioteca del controlador del dispositivo TPM 2.0.0.9 (o superior) 5. Si la versión de firmware no coincide con 2.18, descargue y actualice el firmware de TPM. El SoftPaq de firmware de TPM es un recurso que se puede descargar del sitio web de HP en http://www.hp.com.
HP ProtectTools Security Manager: intermitentemente, se devuelve un error cuando se cierra la interfaz de Security Manager.	Intermitentemente (1 en 12 casos), se crea un error al utilizar el botón Cerrar en el ángulo superior derecho de la pantalla para cerrar Security Manager antes de que todas las aplicaciones complementarias hayan completado la carga.	Esto responde a una dependencia del tiempo en el tiempo de carga de los servicios complementarios cuando se cierra y reinicia Security Manager. Debido a que PTHOST.exe es el shell que contiene a las otras aplicaciones (complementarias), depende de la capacidad del complemento para completar su tiempo de carga (servicios). El cierre del shell antes de que el complemento haya tenido tiempo de completar la carga es la causa fundamental. Permita que Security Manager complete el mensaje de carga de los servicios (que se ve en la parte superior de la ventana de Security Manager) y todos los complementos enumerados en la columna izquierda. Para evitar una falla, permita un tiempo razonable para que se carguen estos complementos.
HP ProtectTools: el acceso irrestricto o privilegios de administrador no controlados plantean un riesgo de seguridad.	Son posibles numerosos riesgos con el acceso irrestricto al equipo cliente, incluidos los siguientes: • Eliminación de la PSD • Modificación malintencionada de la configuración del usuario • Desactivación de las políticas y funciones de seguridad	Se alienta a los administradores a seguir las "mejores prácticas" en la restricción de los privilegios de usuario final y acceso de usuarios. A los usuarios no autorizados no se les debe otorgar privilegios administrativos.
Las contraseñas del BIOS y de Embedded Security del SO no están sincronizadas.	Si un usuario no valida una contraseña nueva como contraseña de Embedded Security del BIOS, la contraseña de Embedded Security del BIOS se revierte a la contraseña original de Embedded Security a través del BIOS de **f10** BIOS.	Esto funciona según el diseño; estas contraseñas puede volver a sincronizarse al cambiar la contraseña del usuario básico del SO y autenticarla en el indicador de la contraseña de Embedded Security del BIOS.
Sólo un usuario puede iniciar sesión en el sistema después de activar la autenticación de preinicio del TPM en el BIOS.	El PIN del BIOS del TPM está asociado con el primer usuario que inicializa la configuración del usuario. Si un equipo tiene múltiples usuarios, el primer usuario es, en esencia, el administrador. El primer usuario tendrá que dar su PIN del usuario del TPM a otros usuarios para que la utilicen para iniciar la sesión.	Esto funciona según el diseño; HP recomienda que el departamento de TI del usuario siga las buenas prácticas de seguridad para implementar su solución de seguridad y garantizar que la contraseña del administrador del BIOS esté configurada por los administradores de TI para la protección a nivel del sistema.
El usuario tiene que cambiar su PIN para hacer que el reinicio del TPM funcione después de una reconfiguración de fábrica del TPM.	El usuario tiene que cambiar su PIN o crear otro usuario para inicializar su configuración de usuario para que la autenticación del BIOS del TPM funcione después de la reconfiguración. No existe opción para que funcione la autenticación del BIOS del TPM.	Esto es según el diseño; la reconfiguración de fábrica elimina la Clave de usuario básica. El usuario debe cambiar su PIN de usuario o crear un nuevo usuario para reinicializar la Clave de usuario básico.

Software afectado: breve descripción	Detalles	Solución
Soporte de autenticación de inicio no está configurado en forma predeterminada utilizando **Reset to Factory Settings** (Reconfigurar de fábrica) de Embedded Security.	En la utilidad de configuración, la opción **Power-on authentication support** (Soporte de autenticación de inicio) no está reconfigurada de fábrica cuando se utiliza la opción de Embedded Security **Reset to Factory Settings** (Reconfigurar de fábrica). En forma predeterminada, **Power-on authentication support (Soporte de autenticación de inicio)** está configurado en **Desactivar**.	La opción **Reset to Factory Settings (Reconfigurar de fábrica)** desactiva Embedded Security Device, que oculta las otras opciones de Embedded Security (incluso **Power-on authentication support (Soporte de autenticación de inicio)**. Sin embargo, después de reactivar Embedded Security Device, **Soporte de autenticación de inicio** permanece activado. HP está trabajando en una solución, que se proporcionará en ofertas futuras de SoftPaq de ROM basado en la Web.
La autenticación de inicio de seguridad se superpone a la contraseña del BIOS durante la secuencia de inicio.	Autenticación de inicio solicita al usuario que inicie la sesión en el sistema utilizando la contraseña del TPM pero, si el usuario presiona **f10** para acceder al BIOS, se otorga al usuario acceso a derechos de Lectura únicamente.	Para poder escribir en el BIOS, el usuario debe ingresar la contraseña del BIOS en lugar de la contraseña del TPM en la ventana de autenticación de inicio.
El BIOS solicita tanto la contraseña anterior como la nueva a través de la utilidad de configuración después de que se cambia la contraseña del Propietario.	El BIOS solicita tanto la contraseña anterior como la nueva a través de Configuración del equipo después de que se cambia la contraseña del Propietario en el software de Windows Embedded Security.	Esto es según el diseño. Esto se debe a la incapacidad del BIOS de comunicarse con el TPM, después de que el sistema operativo se esté ejecutando y de verificar la contraseña del TPM.

Glosario

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

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

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

Administrador. Ver administrador de Windows.

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

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

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

Automatic Technology Manager (ATM). Permite que los administradores de red administren sistemas de forma remota a nivel del BIOS.

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

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

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

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

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

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

Chip de seguridad integrado de Trusted Platform Module (TPM) (sólo en algunos modelos) El témino genérico del chip de HP ProtectTools Embedded Security. Un TPM autentica un equipo, en lugar de un usuario, almacenando información específica en el sistema anfitrión, como claves de encriptación certificados digitales y contraseñas. Un TPM minimiza el riesgo de que la información del equipo se comprometa debido a un robo físico o a un ataque por parte de un hacker externo.

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

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

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

Contraseña de administrador de BIOS. Contraseña de *configuración* de la utilidad de configuración.

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

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

Criptografía. Acción de encriptar y desencriptar datos para que sólo puedan decodificarlos determinadas personas.

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

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

Desencriptación. Procedimiento utilizado en criptografía para convertir datos encriptados en texto común.

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

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

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

DriveLock automático. Recurso de seguridad que hace que el chip TPM Embedded Security genere y proteja las contraseñas de DriveLock. Cuando el usuario es autenticado por el chip TPM embedded security durante el inicio, ingresando la contraseña de clave de usuario básica TPM correcta, el BIOS desbloquea el disco duro para el usuario.

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

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

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

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

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

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

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

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

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

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

Infraestructura de clave pública (PKI) Norma que define las interfaces para crear, utilizar y administrar certificados y claves criptográficas.

Inicio de sesión único. Recurso que almacena información de autenticación y permite utilizar Credential Manager para acceder a Internet y a aplicaciones de Windows que requieren autenticación de contraseña.

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

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

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

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

Lista de contactos confiables. Una lista de los contactos confiables.

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

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

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

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

Modo de seguridad de BIOS. Configuración de Java Card Security que, al activarse, requiere el uso de una Java Card y un PIN válido para la autenticación del usuario.

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

Perfil de BIOS. Grupo de valores de la configuración del BIOS que puede guardarse y aplicarse a otras cuentas.

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

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

Reinicio. Proceso de reinicio del equipo.

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

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

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

Seguridad estricta. Recurso de seguridad de BIOS Configuration que brinda mejor protección para las contraseñas de inicio y de administrador y otras formas de autenticación de inicio.

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

Servicio de recuperación de claves de Drive Encryption. El Servicio de recuperación de arranque seguro. Almacena una copia de la clave de encriptación, lo que le permitirá acceder a su equipo si se le olvida la contraseña y no tiene acceso a su copia de seguridad local de la clave. Debe crear una cuenta en el servicio para configurar el acceso en línea a la copia de seguridad de su contraseña.

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

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

Token. Ver método de inicio de sesión seguro.

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

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

TXT. Trusted Execution Technology (Tecnología de ejecución confiable).

Unidad segura personal (PSD). Brinda un área de almacenamiento protegida para información importante.

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

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

Índice