ProtectTools
Guía del usuario

Primera edición: julio de 2007

Referencia: 451271-071

Tabla de contenido

1 Introducción a la seguridad

El software HP ProtectTools Security Manager proporciona recursos de seguridad que sirven de protección contra al 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 para HP ProtectTools
- Embedded Security para HP ProtectTools
- Java Card Security para HP ProtectTools
- BIOS Configuration para HP ProtectTools
- Drive Encryption para HP ProtectTools

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

Los módulos de software HP ProtectTools puede que estén preinstalados, precargados o disponibles para su descarga en la página Web de HP. Para obtener más información, visite http://www.hp.com.

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

Recursos de HP ProtectTools

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

Módulo	Recursos clave
Credential Manager para HP ProtectTools	• Credential Manager actúa como una bóveda de la contraseña personal. • Single Sign On (Inicio de sesión único) recuerda múltiples contraseñas para distintos sitios Web, aplicaciones y recursos de red protegidos con contraseña. • Single Sign On (Inicio de sesión único) ofrece protección adicional al requerir combinaciones de distintas tecnologías de seguridad, por ejemplo, Java™ Card y biométrica, para la autenticación del usuario. • El almacenamiento de la contraseña se protege a través de la encriptación y se puede consolidar a través del uso de un chip TPM de Embedded Security y/o de la autenticación del dispositivo de seguridad, por ejemplo Java Card o biométrica.
Embedded Security para HP ProtectTools	• 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) para proteger los datos del usuario. • Embedded Security admite aplicaciones de otros fabricantes (como Microsoft Outlook e Internet Explorer) para operaciones de certificados digitales protegidos.
Java Card Security para HP ProtectTools	• Java Card Security configura la Java Card de HP ProtectTools para autenticar el usuario antes de que se cargue el sistema operativo. • Java Card Security configura Java Card separadas para un administrador y un usuario.
BIOS Configuration para HP ProtectTools	• BIOS Configuration proporciona el acceso a la administración de la contraseña del usuario y del administrador al inicio. • BIOS Configuration ofrece una alternativa a la utilidad de configuración del BIOS de pre-arranque conocida como configuración de F10. • DriveLock permite proteger una unidad de disco duro frente a un acceso no autorizado, aunque se extraiga del sistema, sin necesidad de que el usuario recuerde contraseñas adicionales.
Drive Encryption para HP ProtectTools	• Drive Encryption ofrece encriptación completa y de todo el volumen de la unidad de disco duro. • Drive Encryption fuerza a la autenticación preinicio a fin de desencriptar y acceder a los datos.

Acceso a HP ProtectTools Security

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

- Seleccione **Inicio** > **Todos los programas** > **HP ProtectTools Security Manager**.

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

Protección contra robo dirigido

Un ejemplo de este tipo de incidente sería el robo planeado de un ordenador que contenga datos confidenciales e información sobre clientes en un espacio cerrado o abierto. Las siguientes características protegen el ordenador frente a un robo planeado:

- El recurso de autenticación preinicio, si está activado, ayuda a evitar el acceso al sistema operativo. Vea los siguientes procedimientos:
  - “Activación y desactivación de soporte de autenticación de inicio de smart card en la página 46”
  - “Activación y desactivación del soporte de autenticación de inicio para Embedded Security en la página 47”
  - “Asignación de un nombre a una Java Card en la página 39”
  - “Drive Encryption para HP ProtectTools en la página 52”
- DriveLock ayuda a garantizar que no pueda accederse a los datos, incluso si se extrae una unidad de disco duro y se instala en un sistema no seguro. Consulte “Cómo activar y desactivar la protección de la unidad de disco duro DriveLock en la página 48.”
- El recurso Unidad personal segura, provisto por el módulo Embedded Security para 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 28”
  - “Uso de la unidad segura personal (PSD) en la página 31”

Restricción de acceso a datos sensibles

Imagine que un auditor está realizando una auditoría en una empresa y se le ha dado acceso a los equipos informáticos para que pueda revisar datos financieros confidenciales. Sin embargo, la empresa no desea que el auditor pueda imprimir archivos ni guardarlos en dispositivos de escritura como un CD. La siguiente característica permite restringir el acceso a los datos:

- DriveLock ayuda a garantizar que no pueda accederse a los datos, incluso si se extrae una unidad de disco duro y se instala en un sistema no seguro. Consulte “Cómo activar y desactivar la protección de la unidad de disco duro DriveLock en la página 48.”

Prevención de acceso no autorizado desde ubicaciones internas o externas

Si se accede a un equipo que contiene datos confidenciales e información del cliente desde una ubicación interna o externa, los usuarios no autorizados pueden ingresar a los recursos de red o datos corporativos de servicios financieros, de un equipo ejecutivo o de I&D o a información privada, por

ejemplo registros de pacientes o datos financieros personales. Los recursos siguientes 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:
  - "Activación y desactivación de soporte de autenticación de inicio de smart card en la página 46"
  - "Activación y desactivación del soporte de autenticación de inicio para Embedded Security en la página 47"
  - "Asignación de un nombre a una Java Card en la página 39"
  - "Drive Encryption para HP ProtectTools en la página 52"
- Embedded Security para 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 28"
  - "Uso de la unidad segura personal (PSD) en la página 31"
- Con los siguientes procedimientos, Credential Manager para 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"
- 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 28"
  - "Uso de la unidad segura personal (PSD) en la página 31"

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 para HP ProtectTools proporciona un repositorio protegido para las contraseñas y 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 para 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 28."

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: En cooperación con HP, el responsable de seguridad puede personalizar una gran parte de las funciones de HP ProtectTools. Para obtener más información, consulte la página 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 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

Contraseña de HP ProtectTools	Definida en este módulo de HP ProtectTools	Función
		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 se conoce como contraseña de administrador del BIOS, de configuración de F10 o de configuración de la 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 guardada 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 ningún 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.

HP ProtectTools Backup and Restore

HP ProtectTools Backup and Restore ofrece una forma cómoda y rápida de crear copias de seguridad y restaurar credenciales desde todos los módulos compatibles de HP ProtectTools.

Creación de copias de seguridad de credenciales y configuración

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

- Utilice el asistente de HP ProtectTools Backup para seleccionar y crear una copia de seguridad de los módulos de HP ProtectTools
- Copia de seguridad de módulos preseleccionados de HP ProtectTools

NOTA: Debe configurar las opciones de copia de seguridad antes de poder utilizar este método.

- Programar copias de seguridad

NOTA: Debe configurar las opciones de copia de seguridad antes de poder utilizar este método.

Uso del asistente de HP ProtectTools Backup para seleccionar y crear una copia de seguridad de los módulos de HP ProtectTools

1. Seleccione **Inicio** > **Todos los programas** > **HP ProtectTools Security Manager**.
2. En el panel izquierdo, haga clic en **HP ProtectTools**, y luego haga clic en **Backup and Restore**.
3. En el panel derecho, haga clic en **Backup Options** (Opciones de copia de seguridad). Aparece la ventana del asistente de HP ProtectTools Backup. Siga las instrucciones que aparecen en pantalla para crear una copia de seguridad de las credenciales.

Configuración de opciones de copia de seguridad

1. Seleccione **Inicio** > **Todos los programas** > **HP ProtectTools Security Manager**.
2. En el panel izquierdo, haga clic en **HP ProtectTools**, y luego haga clic en **Backup and Restore**.
3. En el panel derecho, haga clic en **Backup Options** (Opciones de copia de seguridad). Aparece la ventana del asistente de HP ProtectTools Backup.
4. Siga las instrucciones que aparecen en pantalla.
5. Después de configurar y confirmar **Storage File Password** (Contraseña del archivo de almacenamiento), seleccione **Remember all passwords and authentication values for future automated backups** (Recordar todas las contraseñas y valores de autenticación para futuras copias de seguridad automáticas).
6. Haga clic en **Save Settings** (Guardar configuración), y a continuación haga clic en **Finalizar**.

Copia de seguridad de módulos preseleccionados de HP ProtectTools

NOTA: Debe configurar las opciones de copia de seguridad antes de poder utilizar este método.

1. Seleccione **Inicio** > **Todos los programas** > **HP ProtectTools Security Manager**.
2. En el panel izquierdo, haga clic en **HP ProtectTools**, y luego haga clic en **Backup and Restore**.
3. En el panel derecho, haga clic en **Backup** (Copia de seguridad).

Programación de copias de seguridad

NOTA: Debe configurar las opciones de copia de seguridad antes de poder utilizar este método.

1. Seleccione **Inicio** > **Todos los programas** > **HP ProtectTools Security Manager**.
2. En el panel izquierdo, haga clic en **HP ProtectTools**, y luego haga clic en **Backup and Restore**.
3. En el panel derecho, haga clic en **Schedule Backups** (Programar copias de seguridad).
4. En la ficha **Task** (Tarea), seleccione la casilla de verificación **Enabled** (Activado) para activar las copias de seguridad programadas.
5. Haga clic en **Set Password** (Configurar contraseña) escriba y confirme su contraseña en el cuadro de diálogo **Set Password**. Haga clic en **Aceptar**.
6. Haga clic en **Apply** (Aplicar). Seleccione la ficha **Schedule** (Programar). Haga clic en la flecha **Schedule Task** (Programar tarea) y seleccione la frecuencia de copia de seguridad automática.
7. En **Start time** (Hora de inicio) utilice las flechas de **Start time** para seleccionar la hora exacta para que comience la copia de seguridad.
8. Haga clic en **Advanced** (Avanzadas) para seleccionar una fecha de inicio y fecha de finalización y configuración de tarea recurrente. Haga clic en **Apply** (Aplicar).
9. Haga clic en **Settings** (Configuración) y seleccione configuración para **Scheduled Task Completed** (Tarea programada completada), **Idle Time** (Tiempo ocioso), y **Power Management** (Administración de energía).
10. Haga clic en **Aplicar**, y a continuación haga clic en **OK** para cerrar el cuadro de diálogo.

Restauración de credenciales

1. Seleccione **Inicio** > **Todos los programas** > **HP ProtectTools Security Manager**.
2. En el panel izquierdo, haga clic en **HP ProtectTools**, y luego haga clic en **Backup and Restore**.
3. En el panel derecho, haga clic en **Restore** (Restaurar). Aparece la ventana del asistente de HP ProtectTools Restore. Siga las instrucciones que aparecen en pantalla.

Configuración de valores

1. Seleccione **Inicio** > **Todos los programas** > **HP ProtectTools Security Manager**.
2. En el panel izquierdo, haga clic en **HP ProtectTools**, y luego haga clic en **Settings** (Configuración).
3. En el panel derecho, seleccione su configuración, y luego haga clic en **Aceptar**.

2 Credential Manager para 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 13.”
- 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:

- El asistente de inicio de sesión Credential Manager (preferido)
- El icono de HP ProtectTools Security Manager en el área de notificación
- HP ProtectTools Security Manager

NOTA: Si utiliza la solicitud de inicio de sesión de Credential Manager en la pantalla de Inicio de sesión de Windows para iniciar la sesión en Credential Manager, iniciará la sesión en Windows simultáneamente.

La primera vez que abra Credential Manager, inicie la sesión con una contraseña normal de Windows. Se creará automáticamente una cuenta de Credential Manager con sus credenciales de inicio de sesión de Windows.

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 13.”

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 ProtectTools Security Manager, al hacer clic en el enlace **Iniciar sesión** en la parte superior derecha de la ventana.
2. Siga las instrucciones en la pantalla para ingresar a Credential Manager.

Primer inicio de sesión

Antes de comenzar, se debe iniciar la sesión en Windows con una cuenta de administrador, pero no iniciar la sesión en Credential Manager.

1. Abra HP ProtectTools Security Manager haciendo doble clic en el icono HP ProtectTools Security Manager del área de notificación. Aparece la ventana de HP ProtectTools Security Manager.
2. En el panel izquierdo, haga clic en **Credential Manager**, y luego haga clic en **Iniciar sesión** en la esquina superior derecha del panel. El asistente de inicio de sesión de Credential Manager se abrirá.
3. Escriba su contraseña de Windows en la casilla **Contraseña** y haga clic en **Siguiente**.

Registro de credenciales

Es posible utilizar la página “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. Después de iniciar sesión en Credential Manager, coloque su dedo sobre el lector de huellas digitales. El asistente de inicio de sesión de Credential Manager se abrirá.
2. Siga las instrucciones en pantalla para completar el registro de sus huellas digitales y configurar el lector de huellas digitales.
3. Si desea configurar el lector de huellas digitales para otro usuario de Windows, inicie sesión en Windows con las credenciales de dicho usuario y repita los pasos 1 y 2.

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 Java Card, USB eToken, o token virtual

NOTA: Deberá tener configurado un lector de tarjetas o un teclado de tarjeta inteligente para poder efectuar este procedimiento. Si decide no utilizar una tarjeta inteligente, puede registrar un token virtual según se describe en “Crear un token virtual en la página 15”.

1. Seleccione **Inicio** > **Todos los programas** > **HP ProtectTools Security Manager**.
2. En el panel izquierdo, haga clic en **Credential Manager**.
3. En el panel derecho, haga clic en **Registrar tarjeta inteligente o símbolo**. El asistente de inicio de sesión de Credential Manager se abrirá.
4. Siga las instrucciones que aparecen en pantalla.

Registro de un eToken USB

1. Asegúrese que los controladores del eToken USB estén instalados.

   NOTA: Consulte la guía del usuario del eToken USB para obtener información adicional.

2. Seleccione **Inicio** > **Todos los programas** > **HP ProtectTools Security Manager**.
3. En el panel izquierdo, haga clic en **Credential Manager**.
4. En el panel derecho, haga clic en **Registrar tarjeta inteligente o símbolo**. El asistente de inicio de sesión de Credential Manager se abrirá.
5. Siga las instrucciones que aparecen en pantalla.

Registro de otras credenciales

1. Seleccione **Inicio** > **Todos los programas** > **HP ProtectTools Security Manager**.
2. En el panel izquierdo, haga clic en **Credential Manager**.
3. En el panel derecho, haga clic en **Registrar credenciales**. El asistente de inicio de sesión de Credential Manager se abrirá.
4. Siga las instrucciones que aparecen en pantalla.

Tareas generales

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

- Crear un token virtual
- Cambiar la contraseña de inicio de sesión de Windows
- Administrar el PIN de un token
- Administración de identidad
- Bloqueo del equipo

NOTA: Esta opción está disponible sólo si la solicitud de inicio clásico de Credential Manager está activado. Consulte “Ejemplo 1: Utilizando la página “configuración avanzada” para permitir inicio de sesión en Windows desde Credential Manager en la página 25.”

Crear un token virtual

Un token virtual funciona de manera muy similar a una Java Card o un USB eToken. El token se guarda en la unidad de 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.

Para crear un nuevo token virtual:

1. Seleccione **Inicio** > **Todos los programas** > **HP ProtectTools Security Manager**.
2. En el panel izquierdo, haga clic en **Credential Manager**.
3. En el panel derecho, haga clic en **Virtual token**. El asistente de inicio de sesión de Credential Manager se abrirá.

NOTA: Si **Virtual token** no es una opción, utilice el procedimiento para “Registro de otras credenciales en la página 14.”

4. Siga las instrucciones que aparecen en pantalla.

Cambiar la contraseña de inicio de sesión de Windows

1. Seleccione **Inicio** > **Todos los programas** > **HP ProtectTools Security Manager**.
2. En el panel izquierdo, haga clic en **Credential Manager**.
3. En el panel derecho, haga clic en **Cambiar contraseña de Windows**.
4. Ingrese su contraseña antigua en la casilla **Contraseña anterior**.
5. Escriba la nueva contraseña en las casillas **Nueva contraseña** y **Confirmar contraseña**.
6. Haga clic en **Finalizar**.

Cambio del PIN de un token

1. Seleccione **Inicio** > **Todos los programas** > **HP ProtectTools Security Manager**.
2. En el panel izquierdo, haga clic en **Credential Manager**.
3. En el panel derecho, haga clic en **Cambiar PIN del token**.

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.

Administración de identidad

Eliminación de una identidad del sistema

NOTA: Esto no afecta la cuenta de usuario de Windows.

1. Seleccione **Inicio** > **Todos los programas** > **HP ProtectTools Security Manager**.
2. En el panel izquierdo, haga clic en **Credential Manager**.
3. En el panel derecho, haga clic en **Borrar identidad para esta cuenta**.
4. Haga clic en **Sí** en el cuadro de diálogo de confirmación. La identidad saldrá de la sesión y será eliminada del sistema.

Bloqueo del equipo

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 activado. Consulte “Ejemplo 1: Utilizando la página “configuración avanzada” para permitir inicio de sesión en Windows desde Credential Manager en la página 25.”

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 25.”

Para bloquear el equipo:

1. Seleccione **Inicio** > **Todos los programas** > **HP ProtectTools Security Manager**.
2. En el panel izquierdo, haga clic en **Credential Manager**.
3. En el panel derecho, haga clic en **Lock Workstation** (Bloquear estación de trabajo). Aparecerá la pantalla de inicio de sesión de Windows. Para desbloquear el equipo se 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. Si no registró su huella digital para iniciar la sesión en Windows, haga clic en el icono de teclado en la esquina superior izquierda de la pantalla junto al icono de huella digital. 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) > **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.

Adición de una cuenta

1. Seleccione **Inicio** > **Todos los programas** > **HP ProtectTools Security Manager**.
2. En el panel izquierdo, haga clic en **Credential Manager**, y luego haga clic en **Servicios y aplicaciones**.
3. En el panel derecho, haga clic en **Inicio de sesión en red de Windows**, y luego haga clic en **Añadir una cuenta de red**. Se abre el asistente de agregar una cuenta de red.
4. Siga las instrucciones que aparecen en pantalla.

Eliminación de una cuenta

1. Seleccione **Inicio** > **Todos los programas** > **HP ProtectTools Security Manager**.
2. En el panel izquierdo, haga clic en **Credential Manager**, y luego haga clic en **Servicios y aplicaciones**.
3. En el panel derecho, haga clic en **Inicio de sesión en red de Windows**, y luego haga clic en **Administrar cuentas de red**. Aparece el cuadro de diálogo **Administrar cuentas de red**.
4. Seleccione la cuenta que desee eliminar, y luego haga clic en **Quitar**.
5. En el cuadro de diálogo de confirmación, haga clic en **Sí**.
6. Haga clic en **Aceptar**.

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 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 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 25.”

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. Seleccione **Inicio** > **Todos los programas** > **HP ProtectTools Security Manager**.
2. En el panel izquierdo, haga clic en **Credential Manager**, y luego haga clic en **Servicios y aplicaciones**.
3. En el panel derecho, haga clic en **Single Sign On** (Inicio de sesión único), y luego haga clic en **Registrar nueva aplicación**. Se abre el asistente de aplicación de SSO.
4. Siga las instrucciones que aparecen en pantalla.

Administración de aplicaciones y credenciales

Modificación de propiedades de aplicación

1. Seleccione **Inicio** > **Todos los programas** > **HP ProtectTools Security Manager**.
2. En el panel izquierdo, haga clic en **Credential Manager**, y luego haga clic en **Servicios y aplicaciones**.
3. En el panel derecho, en **Single Sign On** (Inicio de sesión único), haga clic en **Administrar aplicaciones y credenciales**.
4. Seleccione la aplicación que desee modificar, y haga clic en **Propiedades**.
5. 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.
6. Haga clic en la ficha **Script** para ver y editar el script de la aplicación SSO.
7. Haga clic en **Aceptar**.

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

1. Seleccione **Inicio** > **Todos los programas** > **HP ProtectTools Security Manager**.
2. En el panel izquierdo, haga clic en **Credential Manager**, y luego haga clic en **Servicios y aplicaciones**.
3. En el panel derecho, en **Single Sign On** (Inicio de sesión único), haga clic en **Administrar aplicaciones y credenciales**.
4. Seleccione la aplicación que desee eliminar, y haga clic en **Quitar**.
5. Haga clic en **Sí** en el cuadro de diálogo de confirmación.
6. 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. Seleccione **Inicio** > **Todos los programas** > **HP ProtectTools Security Manager**.
2. En el panel izquierdo, haga clic en **Credential Manager**, y luego haga clic en **Servicios y aplicaciones**.
3. En el panel derecho, en **Single Sign On** (Inicio de sesión único), haga clic en **Administrar aplicaciones y credenciales**.
4. Haga clic en el registro de la aplicación que desea exportar. A continuación, haga clic en **More** (Más) > **Applications** (Aplicaciones) > **Export Script** (Exportar script).
5. Siga las instrucciones en pantalla para completar la exportación.
6. Haga clic en **Aceptar**.

Importación de aplicaciones

1. Seleccione **Inicio** > **Todos los programas** > **HP ProtectTools Security Manager**.
2. En el panel izquierdo, haga clic en **Credential Manager**, y luego haga clic en **Servicios y aplicaciones**.
3. En el panel derecho, en **Single Sign On** (Inicio de sesión único), haga clic en **Administrar aplicaciones y credenciales**.
4. Haga clic en el registro de la aplicación que desea importar. A continuación, haga clic en **More** (Más) > **Applications** (Aplicaciones) > **Import Script** (Importar script).
5. Siga las instrucciones en pantalla para completar la importación.
6. Haga clic en **Aceptar**.

Modificación de credenciales

1. Seleccione **Inicio** > **Todos los programas** > **HP ProtectTools Security Manager**.
2. En el panel izquierdo, haga clic en **Credential Manager**, y luego haga clic en **Servicios y aplicaciones**.
3. En el panel derecho, en **Single Sign On** (Inicio de sesión único), haga clic en **Administrar aplicaciones y credenciales**.
4. Seleccione la aplicación que desee modificar, y luego haga clic en **Más**.
5. 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.

6. Siga las instrucciones que aparecen en pantalla.
7. 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. Seleccione **Inicio** > **Todos los programas** > **HP ProtectTools Security Manager**.
2. En el panel izquierdo, haga clic en **Credential Manager**, y luego haga clic en **Servicios y aplicaciones**.
3. En el panel derecho, en **Protección de aplicación**, haga clic en **Administrar aplicaciones protegidas**. Aparece el cuadro de diálogo **Servicio de protección de aplicaciones**.
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. Haga clic en **Añadir**. Se abre el asistente de agregar programas.
6. Siga las instrucciones que aparecen en pantalla.

Eliminación de protección de una aplicación

Para eliminar restricciones de una aplicación:

1. Seleccione **Inicio** > **Todos los programas** > **HP ProtectTools Security Manager**.
2. En el panel izquierdo, haga clic en **Credential Manager**, y luego haga clic en **Servicios y aplicaciones**.
3. En el panel derecho, en **Protección de aplicación**, haga clic en **Administrar aplicaciones protegidas**. Aparece el cuadro de diálogo **Servicio de protección de aplicaciones**.
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. Seleccione **Inicio** > **Todos los programas** > **HP ProtectTools Security Manager**.
2. En el panel izquierdo, haga clic en **Credential Manager**, y luego haga clic en **Servicios y aplicaciones**.
3. En el panel derecho, en **Protección de aplicación**, haga clic en **Administrar aplicaciones protegidas**. Aparece el cuadro de diálogo **Servicio de protección de aplicaciones**.
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 modificar, y luego haga clic en **Propiedades**. Aparece el cuadro de diálogo **Propiedades** para la aplicación.
6. 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)
7. 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.
8. Haga clic en **Aceptar** para cerrar el cuadro de diálogo de **Propiedades** de aplicaciones.
9. 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. Seleccione **Inicio** > **Todos los programas** > **HP ProtectTools Security Manager**.
2. En el panel izquierdo, haga clic en **Credential Manager**, y luego haga clic en **Autenticación y credenciales**.
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. Seleccione **Inicio** > **Todos los programas** > **HP ProtectTools Security Manager**.
2. En el panel izquierdo, haga clic en **Credential Manager**, y luego haga clic en **Autenticación y credenciales**.
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. Seleccione **Inicio** > **Todos los programas** > **HP ProtectTools Security Manager**.
2. En el panel izquierdo, haga clic en **Credential Manager**, y luego haga clic en **Autenticación y credenciales**.
3. En el panel derecho, haga clic en la ficha **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

Desde la página “Configuración avanzada”, es posible acceder y modificar varias configuraciones utilizando las siguientes fichas:

- General—Permite modificar la definición para configuración básica.
- Single Sign On (Inicio de seseión 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. Seleccione **Inicio** > **Todos los programas** > **HP ProtectTools Security Manager**.
2. En el panel izquierdo, haga clic en **Credential Manager**, y luego haga clic en **Configuración avanzada**.
3. En el panel derecho, haga clic en la ficha apropiada de 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: Utilizando la página “configuración avanzada” para permitir inicio de sesión en Windows desde Credential Manager

1. Seleccione **Inicio** > **Todos los programas** > **HP ProtectTools Security Manager**.
2. En el panel izquierdo, haga clic en **Credential Manager**, y luego haga clic en **Configuración avanzada**.
3. En el panel derecho, 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 en la página 17.”

Ejemplo 2: Utilizando la página “Configuración avanzada” para solicitar verificación del usuario antes del inicio único de sesión

1. Seleccione **Inicio** > **Todos los programas** > **HP ProtectTools Security Manager**.
2. En el panel izquierdo, haga clic en **Credential Manager**, y luego haga clic en **Configuración avanzada**.
3. En el panel derecho, haga clic en la ficha **Single Sign On** (Inicio de sesión único).
4. 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**.
5. Haga clic en **Aplicar** y, a continuación, haga clic en **Aceptar**.
6. Reinicie el equipo.

3 Embedded Security para HP ProtectTools

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

Embedded Security para 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 Computer Setup encendiendo o reiniciando el ordenador y, a continuación, pulse F10 cuando el mensaje “F10 = ROM Based Setup” se muestre en la esquina inferior izquierda de la pantalla.
2. Si no ha definido una contraseña de administrador, utilice las teclas de dirección para seleccionar **Security** (Seguridad) > **Setup password** (Contraseña de configuración) y, a continuación, pulse Intro.
3. Escriba la contraseña en los cuadros **New password** (Nueva contraseña) y **Verify new password** (Verificar nueva contraseña) y, a continuación, pulse 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. Pulse F10 para aceptar los cambios en la configuración de Embedded Security.
8. Para guardar sus preferencias y salir de Computer Setup, utilice las teclas de dirección para seleccionar **File** (Archivo) > **Save Changes and Exit** (Guardar cambios y salir). A continuación, siga las instrucciones 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 del usuario de Embedded Security no se abre, seleccione **Inicio** > **Todos los programas** > **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 certificados digitales, consulte la Ayuda en línea para 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 en línea de Embedded Security y la Ayuda en línea de su correo electrónico.

Cambio de la contraseña de la clave de usuario básico

Para cambiar la contraseña clave de usuario básico:

1. Seleccione **Inicio** > **Todos los programas** > **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. Seleccione **Inicio** > **Todos los programas** > **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 **Backup** (Copia de seguridad). El asistente de copias de seguridad de Embedded Security se abrirá.
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. Seleccione **Inicio** > **Todos los programas** > **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 **Restore** (Restaurar). El asistente de copias de seguridad de Embedded Security se abrirá.
4. Siga las instrucciones que aparecen en pantalla.

Cambio de la contraseña de propietario

Para cambiar la contraseña de propietario:

1. Seleccione **Inicio** > **Todos los programas** > **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

Si un usuario olvidó su contraseña, un administrador le ayudará a redefinirla. Para obtener más información, consulte la Ayuda en línea.

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. Seleccione **Inicio** > **Todos los programas** > **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. Seleccione **Inicio** > **Todos los programas** > **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 más información acerca de la migración, consulte la Ayuda en línea de Embedded Security.

4 Java Card Security para HP ProtectTools

Java Card Security para HP ProtectTools administra la instalación y la configuración de las Java Card para equipos que poseen un lector de tarjeta opcional.

Con Java Card Security, puede realizar las siguientes tareas:

- Acceder a recursos de Java Card Security
- Trabajar con la utilidad de configuración del equipo para permitir la autenticación de Java Card en un entorno de inicio
- Configurar Java Card separadas para un administrador y un usuario. Un usuario debe insertar la Java Card y escribir un PIN antes de que cargue el sistema operativo
- Definir y cambiar el PIN utilizado para autenticar a los usuarios de la Java Card

Tareas generales

La página “General” permite realizar las siguientes tareas:

- Cambiar un PIN de Java Card
- Seleccione el lector de tarjetas o el teclado de tarjeta inteligente

NOTA: El lector de tarjeta utiliza tanto Java Card como Smart Card. Este recurso está disponible si cuenta con más de un lector de tarjeta en el equipo.

Cambio de un PIN de Java Card

Para cambiar el PIN de una Java Card:

NOTA: El PIN de la Java Card debe tener entre 4 y 8 caracteres numéricos.

1. Seleccione **Inicio** > **Todos los programas** > **HP ProtectTools Security Manager**.
2. En el panel izquierdo, haga clic en **Java Card Security**, y luego haga clic en **General**.
3. Inserte una Java Card (con un PIN existente) en el lector de tarjeta.
4. En el panel derecho, haga clic en **Cambiar**.
5. En el cuadro de diálogo **Cambiar PIN**, escriba el PIN actual en la casilla **PIN actual**.
6. Escriba un nuevo PIN en la casilla **Nuevo PIN**, y luego escriba el PIN nuevamente en la casilla **Confirmar nuevo PIN**.
7. Haga clic en **Aceptar**.

Selección del lector de tarjeta

Asegúrese de seleccionar el lector de tarjeta correcto en Java Card Security antes de utilizar la Java Card. Si no se selecciona el lector correcto, puede ser que algunos de los recursos no estén disponibles o no se muestren correctamente. Además, los controladores del lector de tarjeta deben estar instalados correctamente, como se muestra en el Administrador de dispositivos de Windows.

Para seleccionar el lector de tarjeta:

1. Seleccione **Inicio** > **Todos los programas** > **HP ProtectTools Security Manager**.
2. En el panel izquierdo, haga clic en **Java Card Security**, y luego haga clic en **General**.
3. Inserte la Java Card en el lector de tarjeta.
4. En el panel derecho, en **Lector de tarjeta seleccionado**, haga clic en el lector correcto.

Tareas avanzadas (sólo para administradores)

La página “Avanzado” permite realizar las siguientes tareas:

- Asignar un PIN de Java Card
- Asignar un nombre a una Java Card
- Configurar la autenticación de inicio
- Crear y restaurar copias de seguridad de Java Card

NOTA: Usted debe tener privilegios de administrador de Windows a fin de mostrar la página “Avanzado”.

Asignación de un PIN de Java Card

Debe asignar un nombre y un PIN a una Java Card antes de poder utilizarla en Java Card Security.

Para asignar un PIN de Java Card:

NOTA: El PIN de la Java Card debe tener entre 4 y 8 caracteres numéricos.

1. Seleccione **Inicio** > **Todos los programas** > **HP ProtectTools Security Manager**.
2. En el panel izquierdo, haga clic en **Java Card Security**, y luego haga clic en **Avanzadas**.
3. Inserte una nueva Java Card en el lector de tarjeta.
4. Cuando se abra el cuadro de diálogo **Nueva tarjeta**, escriba un nuevo nombre en la casilla, **Nuevo nombre exhibido**, escriba un nuevo PIN en la casilla **Nuevo PIN**, y luego escriba el nuevo PIN otra vez en la casilla **Confirmar nuevo PIN**.
5. Haga clic en **Aceptar**.

Asignación de un nombre a una Java Card

Debe asignar un nombre a una Java Card antes de poder utilizarla para la autenticación de inicio.

Para asignar un nombre a una Java Card:

1. Seleccione **Inicio** > **Todos los programas** > **HP ProtectTools Security Manager**.
2. En el panel izquierdo, haga clic en **Java Card Security**, y entonces haga clic en **Avanzadas**.
3. Inserte la Java Card en el lector de tarjeta.

NOTA: Si no asignó un PIN a esta tarjeta, se abrirá el cuadro de diálogo **Nueva tarjeta** permitiéndole escribir un nombre y un PIN nuevos.

4. En el panel derecho, en **Nombre exhibido**, haga clic en **Cambiar**.
5. Escriba un nombre para la Java Card en la casilla **Nombre**.
6. Escriba el PIN actual de la Java Card en la casilla **PIN**.
7. Haga clic en **Aceptar**.

Configuración de la autenticación de inicio

Cuando está activada, la autenticación de inicio requiere utilizar una Java Card para iniciar el equipo.

El proceso de activación de la autenticación de inicio de Java Card abarca los siguientes pasos:

1. Activación del soporte de autenticación de inicio de Java Card en BIOS Configuration o en la utilidad de configuración. Para obtener más información, consulte “Activación y desactivación de soporte de autenticación de inicio de smart card en la página 46.”
2. Activación de la autenticación de inicio de Java Card en Java Card Security.
3. Creación y activación de una Java Card de administrador.

Activación de la autenticación de inicio de Java Card y creación de una Java Card de administrador

Para activar la autenticación de inicio de Java Card:

1. Seleccione **Inicio** > **Todos los programas** > **HP ProtectTools Security Manager**.
2. En el panel izquierdo, haga clic en **Java Card Security**, y entonces haga clic en **Avanzadas**.
3. Inserte la Java Card en el lector de tarjeta.

NOTA: Si no asignó un nombre y un PIN a esta tarjeta, se abrirá el cuadro de diálogo **Nueva tarjeta** permitiéndole escribir un nombre y un PIN nuevos.

4. En el panel derecho, en **Autenticación de inicio**, haga clic en la casilla de verificación **Activar**.
5. Escriba su contraseña de la utilidad de configuración en el cuadro de diálogo **Contraseña de Computer Setup**, y a continuación haga clic en **Aceptar**.
6. Si DriveLock no está activado, escriba el PIN de la Java Card y luego haga clic en **Aceptar**.

   – o –

   Si DriveLock no está activado:

   a. Haga clic en **Hacer que la identidad de Java Card sea única**.

      – o –

      Haga clic en **Hacer que la identidad de la Java Card sea igual a la contraseña de DriveLock**.

      NOTA: Si DriveLock está activado en el equipo, es posible configurar la identidad de la Java Card para que sea la misma que la contraseña de usuario de DriveLock, lo que le permite validar tanto DriveLock como la Java Card utilizando sólo la Java Card cuando inicie el equipo.

   b. Si corresponde, escriba su contraseña de usuario de DriveLock en la casilla **Contraseña de DriveLock**, y entonces escríbala nuevamente en la casilla **Confirmar contraseña**.

   c. Escriba el PIN de la Java Card.

   d. Haga clic en **Aceptar**.

7. Cuando se le solicite crear un archivo de recuperación, haga clic en **Cancelar** para crear un archivo de recuperación posteriormente o haga clic en **Aceptar** y siga las instrucciones en la pantalla del asistente de copia de seguridad de HP ProtectTools para crear un archivo de recuperación ahora.

NOTA: Para obtener más información, consulte “HP ProtectTools Backup and Restore en la página 8.”

Creación de una Java Card de usuario

NOTA: Para crear una Java Card de usuario deben configurarse una autenticación de inicio y una tarjeta de administrador.

Para crear una Java Card de usuario:

1. Seleccione **Inicio** > **Todos los programas** > **HP ProtectTools Security Manager**.
2. En el panel izquierdo, haga clic en **Java Card Security**, y a continuación haga clic en **Avanzadas**.
3. Inserte una Java Card que se utilizará como tarjeta de usuario.
4. En el panel derecho, en **Autenticación de inicio**, haga clic en **Crear** junto a **Identidad de la tarjeta de usuario**.
5. Escriba un PIN para la Java Card de usuario y haga clic en **Aceptar**.

Desactivación de la autenticación de inicio de Java Card

Cuando desactive la autenticación de inicio de Java Card, no precisará utilizar más la Java Card para acceder al equipo.

1. Seleccione **Inicio** > **Todos los programas** > **HP ProtectTools Security Manager**.
2. En el panel izquierdo, haga clic en **Java Card Security**, y entonces haga clic en **Avanzadas**.
3. Inserte la Java Card del administrador.
4. En el panel derecho, en **Autenticación de inicio**, desmarque la casilla de verificación **Activar**.
5. Escriba un PIN para la Java Card y haga clic en **Aceptar**.

5 BIOS Configuration para 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 inicio y de administrador.
- Configurar otros recursos de autenticación de inicio, como activación del soporte de autenticación de embedded security.
- Activar y desactivar recursos de hardware, como inicio por CD-ROM o diferentes 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 permite gestionar diversas configuraciones del ordenador que de otra forma estarían sólo disponibles pulsando F10 durante el arranque y entrando en Computer Setup.

Administración de opciones de arranque

Se puede utilizar BIOS Configuration para administrar varias configuraciones de tareas ejecutadas al encender o reiniciar el equipo.

Para administrar opciones de arranque:

1. Seleccione **Inicio** > **Todos los programas** > **HP ProtectTools Security Manager**.
2. En el panel izquierdo, haga clic en **Configuración de la BIOS**.
3. Escriba la contraseña de administrador de la utilidad de configuración cuando se le solicite la contraseña de administrador de BIOS, y a continuación haga clic en **Aceptar**.

   NOTA: Sólo se le solicitará la contraseña de administrador de BIOS si ya ha definido la contraseña de usuario de la utilidad de configuración. Para obtener más información sobre la configuración de la contraseña de la utilidad de configuración, consulte “Definición de la contraseña de configuración en la página 50”.
4. En el panel izquierdo, haga clic en **Configuración del sistema**.
5. En el panel derecho, seleccione la demora (en segundos) para F9, F10 y F12, y **Express Boot Popup Delay (Sec)** (Demora de solicitud de arranque exprés [seg.]).
6. Active o desactive **MultiBoot**.
7. Si ha activado MultiBoot, seleccione el orden de inicio eligiendo un dispositivo de inicio y luego haciendo clic en flecha arriba o flecha abajo para ajustar su orden en la lista.
8. Haga clic en **Aplicar**, y a continuación haga clic en **Aceptar** en la ventana de HP ProtectTools.

Activación y desactivación de opciones de configuración del sistema

NOTA: Algunos de los elementos listados a continuación podrían no ser admitidos por su equipo.

Para activar o desactivar dispositivos u opciones de seguridad:

1. Seleccione **Inicio** > **Todos los programas** > **HP ProtectTools Security Manager**.
2. En el panel izquierdo, haga clic en **Configuración de la BIOS**.
3. Escriba la contraseña de administrador de la utilidad de configuración cuando se le solicite la contraseña de administrador de BIOS y a continuación haga clic en **Aceptar**.
4. En el panel izquierdo, haga clic en **Configuración del sistema**, y luego active o desactive una opción de configuración del sistema o configure cualquiera de las siguientes opciones de configuración del sistema en el panel derecho:
   - Opciones de puerto
     - Puerto en serie
     - Puerto de infrarrojos
     - Puerto paralelo
     - Ranura SD
     - Puerto USB
     - Puerto 1394
     - Ranura para Cardbus
     - Ranura para ExpressCard
   - Opciones de arranque
     - Demora en F9, F10 y F12 (seg.)
     - MultiBoot
     - Express Boot Popup Delay (Sec) (Demora emergente de inicio rápido (seg))
     - Arranque a partir de CD-ROM
     - Arranque a partir de disquete
     - Arranque a partir del adaptador interno de red
     - Modo de Arranque a partir del adaptador interno de red (PXE o RPL)
     - Orden de arranque
   - Configuración del dispositivo
     - Activar bloq num al iniciar
     - Intercambiar teclas fn/ctrl
     - Activar dispositivo de puntero múltiple
     - Activar soporte legado para USB
     - Modo de puerto paralelo (estándar, bidireccional, EPP o ECP)
     - Prevención de ejecución de datos

- Modo nativo SATA
- CPU de núcleo doble
- Soporte de funcionalidad automática Intel® SpeedStep
- Ventilador siempre encendido mientras se utiliza alimentación de CA
- Transferencias de datos BIOS DMA
- Desactivación de ejecución Intel o AMD PSAE

- Opciones de dispositivo integrado
  - Radio de dispositivo de WLAN incorporada
  - Radio de dispositivo WWAN icorporado
  - Radio de dispositivo Bluetooth® icorporado
  - Alternancia LAN/WLAN
  - Encendido a través de Wake on LAN

5. Haga clic en **Aplicar** y luego haga clic en **Aceptar** en la ventana HP ProtectTools para guardar los cambios y salir.

Tareas avanzadas

Administración de configuración del módulo complementario de HP ProtectTools

Algunos de los recursos de HP ProtectTools Security Manager pueden ser administrados en BIOS Configuration.

Activación y desactivación de soporte de autenticación de inicio de smart card

La activación de esta opción permite utilizar una smart card para la autenticación del usuario cuando enciende el equipo.

NOTA: Para activar completamente el recurso de autenticación de inicio, también debe configurar una smart card utilizando el módulo Java Card Security para HP ProtectTools.

Para activar el soporte de autenticación de inicio con smart card:

1. Seleccione **Inicio** > **Todos los programas** > **HP ProtectTools Security Manager**.
2. En el panel izquierdo, haga clic en **Configuración de la BIOS**.
3. Escriba la contraseña de administrador de la utilidad de configuración cuando se le solicite la contraseña de administrador de BIOS y a continuación haga clic en **Aceptar**.
4. En el panel izquierdo, haga clic en **Seguridad**.
5. En **Smart Card Security**, haga clic en **Activar**.

   NOTA: Para desactivar la autenticación de inicio con smart card, haga clic en **Desactivar**.

6. Haga clic en **Aplicar**, y a continuación haga clic en **Aceptar** en la ventana HP ProtectTools.

Activación y desactivación del soporte de autenticación de inicio para Embedded Security

La activación de esta opción posibilita que el sistema utilice el chip TPM embedded security (si está disponible) para la autenticación del usuario cuando enciende el equipo.

NOTA: Para activar completamente el recurso de autenticación de inicio, también debe configurar el chip TPM embedded security utilizando el módulo Embedded Security para HP ProtectTools.

Para activar el soporte de autenticación de inicio para Embedded Security:

1. Seleccione **Inicio** > **Todos los programas** > **HP ProtectTools Security Manager**.
2. En el panel izquierdo, haga clic en **Configuración de la BIOS**.
3. Escriba la contraseña de administrador de la utilidad de configuración cuando se le solicite la contraseña de administrador de BIOS y a continuación haga clic en **Aceptar**.
4. En el panel izquierdo, haga clic en **Seguridad**.
5. En **Embedded Security**, haga clic en **Activar la compatibilidad con la autenticación de encendido**.

   NOTA: Para desactivar la autenticación de inicio para Embedded Security, haga clic en **Desactivar**.

6. Haga clic en **Aplicar**, y a continuación haga clic en **Aceptar** en la ventana HP ProtectTools.

Cómo activar y desactivar la protección de la unidad de disco duro DriveLock

DriveLock (Bloqueo de la unidad) es una característica de seguridad estándar de la industria que impide el acceso no autorizado a los datos de unidades de disco duro ATA. Esta función se ha implementado como una extensión de Computer Setup. Sólo está disponible cuando se detectan unidades de disco duro que admiten el conjunto de comandos de seguridad ATA. La función de DriveLock (Bloqueo de la unidad) ha sido ideada para los clientes de HP cuya preocupación principal es la seguridad de los datos. Para dichos clientes, el coste de la unidad de disco duro y la pérdida de los datos almacenados en ésta es irrelevante en comparación con los daños que pueden resultar del acceso no autorizado al contenido. A fin de equilibrar este nivel de seguridad con la necesidad práctica de facilitar una contraseña olvidada, la implementación de HP de DriveLock (Bloqueo de la unidad) utiliza un esquema de seguridad de dos contraseñas. El administrador del sistema establece y utiliza una de las contraseñas, mientras que la otra, la establece y utiliza normalmente el usuario final. La unidad no puede desbloquearse si se han perdido ambas contraseñas. Por lo tanto, la forma más segura de utilizar DriveLock (Bloqueo de la unidad) es duplicar los datos de la unidad de disco duro en un sistema de información corporativo o hacer una copia de seguridad periódicamente. En el caso de que se pierdan ambas contraseñas de bloqueo, la unidad de disco duro queda inutilizada. Para los usuarios que no se ajustan al perfil de cliente anteriormente definido, esto puede suponer un riesgo inaceptable. Para los usuarios que se ajustan al perfil del cliente, puede constituir un riesgo tolerable dada la naturaleza de los datos almacenados en la unidad de disco duro.

Utilización de la opción de DriveLock (Bloqueo de la unidad)

Cuando se detectan unidades de disco duro que admiten el conjunto de comandos de seguridad ATA, la opción de DriveLock (Bloqueo de la unidad) aparece en el menú Security (Seguridad) de Computer Setup. El usuario tiene la posibilidad de establecer la contraseña maestra o de activar DriveLock (Bloqueo de la unidad). Debe proporcionarse una contraseña de usuario para activar DriveLock (Bloqueo de la unidad). Dado que la configuración inicial de DriveLock (Bloqueo de la unidad) la realiza normalmente un administrador del sistema, primero debe establecerse una contraseña maestra. HP recomienda a los administradores de sistemas que definan una contraseña maestra tanto si desean activar DriveLock (Bloqueo de la unidad) como si lo dejan desactivado. De esta manera, el administrador tiene la posibilidad de modificar los valores de DriveLock (Bloqueo de la unidad) en el caso de que, posteriormente, se active esta función. Una vez establecida la contraseña maestra, el administrador del sistema puede activar DriveLock (Bloqueo de la unidad) o dejarlo desactivado.

En el caso de una unidad de disco duro bloqueada, la POST solicitará una contraseña para desbloquear el dispositivo. Si se ha establecido una contraseña de arranque que coincide con la contraseña de usuario del dispositivo, la POST no solicitará que se vuelva a introducir la contraseña. De lo contrario, el usuario deberá introducir una contraseña de DriveLock (Bloqueo de la unidad). En un arranque en frío, puede utilizarse tanto la contraseña maestra como la contraseña de usuario. En un arranque en caliente, introduzca la misma contraseña utilizada para desbloquear la unidad durante el arranque en frío anterior. Los usuarios dispondrán de dos intentos para introducir una contraseña correcta. En el arranque en frío, si ninguno tiene éxito, la POST continuará pero no se podrá acceder a los datos de la unidad. En un arranque en caliente o reinicio desde Windows, si no funciona ningún intento, la POST se detendrá y se indicará al usuario mueva la fuente de alimentación.

Aplicaciones de DriveLock (Bloqueo de la unidad)

El uso más práctico de la característica de seguridad de DriveLock (Bloqueo de la unidad) es en entornos corporativos. El administrador del sistema será el responsable de configurar la unidad de disco duro para el compartimiento multiuso que implicará, entre otras cosas, definir la contraseña maestra de DriveLock (Bloqueo de la unidad) y una contraseña de usuario temporal. En el caso de que el usuario olvidara su contraseña o que otro empleado utilizara el equipo, siempre podría utilizarse la contraseña maestra para volver a establecer la contraseña de usuario y tener nuevamente acceso a la unidad de disco duro.

HP recomienda a los administradores de sistemas corporativos que optan por activar DriveLock (Bloqueo de la unidad) que establezcan también una política corporativa para establecer y mantener las contraseñas maestras. Esto debe realizarse para evitar una situación en la que un empleado modifique de forma intencionada, o no, ambas contraseñas de DriveLock (Bloqueo de la unidad) antes

de abandonar la compañía. En tal caso, la unidad de disco duro quedaría inutilizada y debería reemplazarse. Asimismo, si no se establece una contraseña maestra, los administradores del sistema pueden encontrarse con el acceso bloqueado a una unidad de disco duro, sin posibilidad de realizar comprobaciones rutinarias para detectar software no autorizado, ni otras funciones de control de activos y soporte técnico.

Para los usuarios con requisitos de seguridad menos estrictos, HP no recomienda que se active DriveLock (Bloqueo de la unidad). Entre los usuarios de esta categoría se incluyen los usuarios particulares o los usuarios que no mantienen datos sensibles en las unidades de disco duro de forma habitual. Para estos usuarios, la pérdida potencial de una unidad de disco duro consecuencia del olvido de ambas contraseñas es más importante que el valor de los datos para los que se ha diseñado la función de DriveLock (Bloqueo de la unidad). Puede restringirse el acceso a Computer Setup y a la función de DriveLock (Bloqueo de la unidad) mediante la contraseña de configuración. Al especificar una contraseña de configuración y no proporcionarla a los usuarios finales, los administradores del sistema restringen el número de usuarios que pueden activar DriveLock (Bloqueo de la unidad).

Administración de contraseñas de la utilidad de configuración

Es posible utilizar BIOS Configuration para definir y cambiar las contraseñas de inicio y definir la contraseña de la utilidad de configuración y también administrar varias configuraciones de contraseña.

△ **PRECAUCIÓN:** Las contraseñas definidas en la página de “Contraseñas” en BIOS Configuration son guardadas inmediatamente haciendo clic en el botón **Aplicar** o **Aceptar** en la ventana de HP ProtectTools. Asegúrese de recordar la contraseña que haya definido ya que no podrá alterar la configuración de la contraseña sin suministrar la contraseña anterior.

La contraseña de inicio puede proteger su PC portátil contra el uso no autorizado.

NOTA: Después de configurar una contraseña de inicio, el botón Definir en la página “Contraseñas” es reemplazado por el botón Cambiar.

Una contraseña de configuración del equipo protege los parámetros de configuración y la información de identificación del sistema en la utilidad de configuración. Una vez definida, esta contraseña se debe utilizar para acceder a la utilidad de configuración. Si ha definido una contraseña de configuración, ésta se le solicitará antes de abrir la parte BIOS Configuration para HP ProtectTools.

NOTA: Después de configurar una contraseña de configuración, el botón Configurar en la página “Contraseñas” es reemplazado por el botón Cambiar.

Configuración de la contraseña de inicio

Para configurar la contraseña de inicio:

1. Seleccione **Inicio** > **Todos los programas** > **HP ProtectTools Security Manager**.
2. En el panel izquierdo, haga clic en **Configuración de la BIOS** y luego haga clic en **Seguridad**.
3. En el panel derecho, junto a **Contraseña de arranque**, haga clic en **Configurar**.
4. Ingrese y confirme la contraseña en las casillas **Nueva contraseña** y **Confirmar contraseña**.
5. Haga clic en **Aceptar** en el cuadro de diálogo **Contraseñas**.
6. Haga clic en **Aplicar**, y a continuación haga clic en **Aceptar** en la ventana HP ProtectTools.

Cambio de la contraseña de inicio

Para cambiar la contraseña de inicio:

1. Seleccione **Inicio** > **Todos los programas** > **HP ProtectTools Security Manager**.
2. En el panel izquierdo, haga clic en **Configuración de la BIOS** y luego haga clic en **Seguridad**.

3. En el panel derecho, al lado de **Contraseña de arranque**, haga clic en **Cambiar**.
4. Ingrese su contraseña actual en la casilla **Contraseña actual**.
5. Defina y confirme la nueva contraseña en la casilla **Nueva contraseña**.
6. Haga clic en **Aceptar** en el cuadro de diálogo **Contraseñas**.
7. Haga clic en **Aplicar**, y a continuación haga clic en **Aceptar** en la ventana HP ProtectTools.

Definición de la contraseña de configuración

Para definir la contraseña de la utilidad de configuración:

1. Seleccione **Inicio** > **Todos los programas** > **HP ProtectTools Security Manager**.
2. En el panel izquierdo, haga clic en **Configuración de la BIOS** y luego haga clic en **Seguridad**.
3. En el panel derecho, al lado de **Contraseña de configuración**, haga clic en **Configurar**.
4. Ingrese y confirme la contraseña en las casillas **Nueva contraseña** y **Confirmar contraseña**.
5. Haga clic en **Aceptar** en el cuadro de diálogo **Contraseñas**.
6. Haga clic en **Aplicar**, y a continuación haga clic en **Aceptar** en la ventana HP ProtectTools.

Cambio de la contraseña de configuración

Para cambiar la contraseña de la utilidad de configuración:

1. Seleccione **Inicio** > **Todos los programas** > **HP ProtectTools Security Manager**.
2. En el panel izquierdo, haga clic en **Configuración de la BIOS** y luego haga clic en **Seguridad**.
3. En el panel derecho, al lado de **Contraseña de configuración**, haga clic en **Cambiar**.
4. Ingrese su contraseña actual en la casilla **Contraseña actual**.
5. Ingrese y confirme la nueva contraseña en las casillas **Nueva contraseña** y **Confirmar contraseña**.
6. Haga clic en **Aceptar** en el cuadro de diálogo **Contraseñas**.
7. Haga clic en **Aplicar**, y a continuación haga clic en **Aceptar** en la ventana HP ProtectTools.

Definición de opciones de contraseña

Es posible utilizar BIOS Configuration for ProtectTools para definir opciones de contraseña para optimizar la seguridad del sistema.

Activación y desactivación de seguridad estricta

△ **PRECAUCIÓN:** Para evitar que el equipo quede permanentemente inutilizable, anote la contraseña de configuración, la contraseña de inicio o el PIN de la smart card configurados y guárdelos en un lugar seguro y lejos del equipo. Sin estas contraseñas o sin el PIN, el equipo no se podrá desbloquear.

La activación de seguridad estricta brinda mejor protección para las contraseñas de inicio y de administrador y otras formas de autenticación de inicio.

Para activar o desactivar seguridad estricta:

1. Seleccione **Inicio** > **Todos los programas** > **HP ProtectTools Security Manager**.
2. En el panel izquierdo, haga clic en **Configuración de la BIOS** y luego haga clic en **Seguridad**.

3. En el panel derecho, bajo **Opciones de contraseña**, active o desactive **Seguridad estricta**.

NOTA: Si desea desactivar seguridad estricta, desactive la casilla de verificación **Activar seguridad estricta**.

4. Haga clic en **Aplicar**, y a continuación haga clic en **Aceptar** en la ventana HP ProtectTools.

Activación y desactivación de autenticación de inicio al reiniciar Windows

Esta opción posibilita optimizar la seguridad solicitando que los usuarios escriban una contraseña de inicio, TPM o smart card cuando se reinicia Windows.

Para activar o desactivar la autenticación de inicio en el reinicio de Windows:

1. Seleccione **Inicio** > **Todos los programas** > **HP ProtectTools Security Manager**.
2. En el panel izquierdo, haga clic en **Configuración de la BIOS** y luego haga clic en **Seguridad**.
3. En el panel derecho, en **Opciones de contraseña**, active o desactive **Solicitar contraseña al reiniciar**.
4. Haga clic en **Aplicar**, y a continuación haga clic en **Aceptar** en la ventana HP ProtectTools.

6 Drive Encryption para HP ProtectTools

△ **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 en las unidades encriptadas, a menos que se haya registrado en el servicio de recuperación de Drive Encryption (consulte "Recuperación en la página 56"). La reinstalación del módulo Drive Encryption no le permitirá acceder a las unidades encriptadas.

Administración de encriptación

Encriptación de una unidad

1. Seleccione **Inicio** > **Todos los programas** > **HP ProtectTools Security Manager**.
2. En el panel izquierdo, haga clic en **Drive Encryption**, y a continuación haga clic en **Administración de encriptación**.
3. En el panel derecho, haga clic en **Activar**. Se abre el asistente de Drive Encryption for ProtectTools.
4. Siga las instrucciones que aparecen en pantalla para activar la encriptación.

NOTA: Deberá especificar un disco flexible, un dispositivo de almacenamiento flash o algún otro medio de almacenamiento conectado con USB en el que se almacenará la información de recuperación.

Cambio de encriptación

1. Seleccione **Inicio** > **Todos los programas** > **HP ProtectTools Security Manager**.
2. En el panel izquierdo, haga clic en **Drive Encryption**, y a continuación haga clic en **Administración de encriptación**.
3. En el panel derecho, haga clic en **Cambiar encriptación**. Seleccione los discos que se encriptarán en el cuadro de diálogo **Cambiar encriptación**, y luego haga clic en **Aceptar**.
4. Haga clic nuevamente en **Aceptar** para comenzar la encriptación.

Desencriptación de una unidad

1. Seleccione **Inicio** > **Todos los programas** > **HP ProtectTools Security Manager**.
2. En el panel izquierdo, haga clic en **Drive Encryption**, y a continuación haga clic en **Administración de encriptación**.
3. En el panel derecho, haga clic en **Desactivar**.

Administración de usuarios

Añadir un usuario

1. Seleccione **Inicio** > **Todos los programas** > **HP ProtectTools Security Manager**.
2. En el panel izquierdo, haga clic en **Drive Encryption**, y a continuación haga clic en **Administración de usuarios**.
3. En el panel derecho, haga clic en **Añadir**. Haga clic en un nombre de usuario en la lista **Nombre de usuario**, o escriba un nombre de usuario en la casilla **Nombre de usuario**. Haga clic en **Siguiente**.
4. Escriba la contraseña de Windows para el usuario seleccionado y a continuación haga clic en **Siguiente**.
5. Seleccione un método de autenticación para el nuevo usuario y entonces haga clic en **Finalizar**.

Eliminar un usuario

1. Seleccione **Inicio** > **Todos los programas** > **HP ProtectTools Security Manager**.
2. En el panel izquierdo, haga clic en **Drive Encryption**, y a continuación haga clic en **Administración de usuarios**.
3. En el panel derecho, haga clic en un nombre de usuario para eliminarlo en la lista **Nombre de usuario**. Haga clic en **Quitar**.
4. Haga clic en **Sí** para confirmar que desea eliminar el usuario seleccionado.

Cambio de token

Cambie el método de autenticación para un usuario de la siguiente manera:

1. Seleccione **Inicio** > **Todos los programas** > **HP ProtectTools Security Manager**.
2. En el panel izquierdo, haga clic en **Drive Encryption**, y a continuación haga clic en **Administración de usuarios**.
3. En el panel derecho, seleccione un nombre de usuario de la lista **Nombre de usuario**, y a continuación haga clic en **Cambiar token**.
4. Escriba la contraseña de Windows del usuario y a continuación haga clic en **Siguiente**.
5. Seleccione un nuevo método de autenticación y entonces haga clic en **Finalizar**.
6. Si seleccionó una Java Card como método de autenticación, escriba la contraseña de Java Card cuando se le solicite, y a continuación haga clic en **Aceptar**.

Definir contraseña

Defina una contraseña o cambie el método de autenticación para un usuario de la siguiente manera:

1. Seleccione **Inicio** > **Todos los programas** > **HP ProtectTools Security Manager**.
2. En el panel izquierdo, haga clic en **Drive Encryption**, y a continuación haga clic en **Administración de usuarios**.
3. En el panel derecho, seleccione el usuario de la lista **Nombre de usuario**, y a continuación haga clic en **Set password** (Definir contraseña).
4. Escriba la contraseña de Windows del usuario y a continuación haga clic en **Siguiente**.

5. Seleccione el nuevo método de autenticación y entonces haga clic en **Finalizar**.

6. Si seleccionó una Java Card como método de autenticación, escriba la contraseña de Java Card cuando se le solicite, y entonces haga clic en **Aceptar**.

Recuperación

Se encuentran disponibles las siguientes dos medidas de seguridad:

- Si olvida su contraseña, no podrá acceder a sus unidades encriptadas. Sin embargo, puede registrarse en el servicio de recuperación de Drive Encryption para poder acceder a su equipo si olvida su contraseña.
- Puede crear una copia de seguridad de sus claves de Drive Encryption en un disco flexible, un dispositivo de almacenamiento flash o algún otro medio de almacenamiento conectado mediante USB.

Registro en el servicio de recuperación de Drive Encryption

1. Seleccione **Inicio** > **Todos los programas** > **HP ProtectTools Security Manager**.
2. En el panel izquierdo, haga clic en **Drive Encryption**, y a continuación haga clic en **Recovery (Recuperación)**.
3. En el panel derecho, haga clic en **Click here to register** (Haga clic aquí para registrarse). Escriba la información solicitada para completar el procedimiento de copia de seguridad.

Copia de seguridad de sus claves de Drive Encryption

1. Seleccione **Inicio** > **Todos los programas** > **HP ProtectTools Security Manager**.
2. En el panel izquierdo, haga clic en **Drive Encryption**, y a continuación haga clic en **Recovery (Recuperación)**.
3. En el panel derecho, haga clic en **Click here to register (Haga clic aquí para registrarse)**.
4. Seleccione un disco flexible, un dispositivo de almacenamiento flash o algún otro medio de almacenamiento conectado mediante USB en el que se guardará la información de recuperación y, a continuación, haga clic en **Siguiente**. Se abre el asistente de Drive Encryption for ProtectTools.
5. Siga las instrucciones que aparecen en la pantalla para crear una copia de seguridad de las claves de Drive Encryption.

NOTA: Deberá especificar un disco flexible, un dispositivo de almacenamiento flash o algún otro medio de almacenamiento conectado con USB en el que se almacenará la información de recuperación.

7 Solución de problemas

Credential Manager for ProtectTools

Descripción breve	Detalles	Solución
Utilizando la opción de Credential Manager Network Accounts, un usuario puede seleccionar la cuenta de dominio a la que acceder. Esta opción no está disponible cuando se utiliza la autentificación TPM. El resto de los métodos de autentificación funcionan correctamente.	Cuando se utiliza la autentificación TPM, el usuario sólo accede al ordenador local.	La utilización de las herramientas de Credential Manager Single Sign On permite al usuario autentificar otras cuentas.
La credencial del token USB no está disponible en las conexiones a Windows XP Service Pack 1.	Una vez instalado el software del token USB, registrada la credencial del token USB y configurado Credential Manager como conexión principal, el token USB no aparece como listado o disponible en el acceso a Credencial Manager. Cuando vuelva a entrar en Windows, cierre la sesión de Credential mamager, vuelva a entrar en Credential Manager y reseleccione el token como conexión primaria, la operación de conexión del token funcionará con normalidad.	Esto sucede únicamente con Windows XP Service Pack 1; se puede actualizar la versión con el Service Pack 2 utilizando la Actualización de Windows. Para trabajar con Service Pack 1, vuelva a registrarse en Windows utilizando otra credencial (contraseña de Windows) con el fin de cerrar la sesión y volver a registrarse en Credential Manager.
Algunas páginas Web de aplicaciones crean errores que impiden al usuario realizar o completar tareas.	Algunas aplicaciones basadas en la Web dejan de funcionar e informan de errores debido al modelo de funcionalidad de desactivación de Single Sign On. Por ejemplo, en Internet Explorer aparece un símbolo de **!** en un triángulo amarillo, indicando que se ha producido un error.	Credential Manager Single Sign On no admite todas las interfaces de software de Web. Desactive el soporte Single Sign On de una página Web específica desactivando el soporte de Single Sign On. Consulte toda la documentación en Single Sign On, que está disponible en los archivos de ayuda de Credential Manager. Si una Single Sign On en particular no pudiera desactivarse para una aplicación determinada, llame al Servicio y Asistencia de HP y solicite una ayuda de tercer nivel a través de su contacto de Servicio de HP.
La opción **Browse for Virtual Token** (Examinar token virtual) no está disponible durante el proceso de conexión.	El usuario no puede trasladar la ubicación del token virtual registrado en Credential Manager porque la opción de examinar se eliminó debido a los riesgos de seguridad.	La opción de examinar se eliminó de la oferta actual de productos, porque permitía a los no usuarios eliminar y renombrar archivos, tomando control de Windows.
La conexión con la autenticación TPM no ofrece la opción **Network Accounts** (Cuentas de red).	Utilizando la opción de **Network Accounts** (Cuentas de red), un usuario puede seleccionar la cuenta de dominio a la que desea acceder. Esta opción no está disponible cuando se utiliza la autentificación TPM.	HP está trabajando en un parche provisional para la mejora de futuros productos.
Los administradores de dominio no pueden cambiar la contraseña de Windows aunque dispongan de autorización.	Esto sucede una vez que un administrador de dominio se conecta a un dominio y registra la identidad de dominio con Credential Manager, utilizando una cuenta con derechos de administrador sobre el dominio y el ordenador local. Cuando el administrador del dominio intenta cambiar la contraseña de Windows en Credential Manager, el administrador incurre en un fallo de error de la conexión: **User account restriction** (Restricción de la cuenta de usuario).	Credential Manager no puede cambiar la contraseña de una cuenta de usuario del dominio a través de **Change Windows password** (Cambiar contraseña de Windows). Credential Manager sólo puede cambiar las contraseñas de cuenta de ordenadores locales. El usuario del dominio puede cambiar su contraseña en la opción **Windows security** (Seguridad de Windows) > **Change password** (Cambiar contraseña) pero, dado que el este usuario no tiene una cuenta física en el ordenador local, Credential Manager sólo puede cambiar la contraseña utilizada para la conexión.

Descripción breve	Detalles	Solución
Deberían configurarse los parámetros predeterminados de Credential Manager Single Sign On para presentación en pantalla y evitar bucles.	El valor predeterminado de Single Sign On está configurado para que los usuarios se registren automáticamente. Sin embargo, cuando se crea el segundo de dos documentos diferentes protegidos por contraseña, Credential Manager utiliza la última contraseña registrada, la del primer documento.	HP está trabajando en un parche provisional para la mejora de futuros productos.
Problemas de incompatiblidad con la contraseña “gina” de Corel WordPerfect 12	Si el usuario se conecta a Credential Manager, crea un documento en WordPerfect y lo guarda con protección de contraseña, Credential Manager no podrá detectar o reconocer, ni manual ni automáticamente, la contraseña “gina”.	HP está trabajando en un parche provisional para la mejora de futuros productos.
Credential Manager no reconoce el botón en pantalla **Connect** (Conectar).	Si las credenciales de Single Sign On para la conexión de escritorio remoto (RDP) están configuradas para **Connect** (Conectar), Single Sign On, una vez reiniciado, entrará siempre en **Save As** (Guardar como) en lugar de en **Connect** (Conectar).	HP está trabajando en un parche provisional para la mejora de futuros productos.
El asistente de configuración de ATI Catalyst no se puede utilizar con Credential Manager.	Credential Manager Single Sign On entra en conflicto con el asistente de configuración de ATI Catalyst.	Desactive Credential Manager Single Sign On.
Cuando se conecte utilizando la autentificación TPM, el botón en la pantalla **Back** (Atrás) ignora la opción de elegir otro método de autenticación.	Si el usuario que utiliza la autenticación de conexión TM para Credential Manager introduce su contraseña, el botón **Back** (Atrás) no funciona correctamente, ya que muestra de inmediato la pantalla de conexión de Windows.	HP está trabajando en un parche provisional para la mejora de futuros productos.
Credential Manager se abre en el modo en espera cuando está configurado para no hacerlo.	Cuando no está seleccionada la opción **use Credential Manager log on to Windows** (utilizar la conexión de Credential Manager a Windows), que permite que el sistema entre en S3 “suspender” y, a continuación, active el sistema, Credential Manager se conectará a Windows para abrirse.	Si no se ha configurado una contraseña de administrador, el usuario no puede conectarse a Windows a través de Credential Manager, debido a las restricciones de cuenta invocadas por Credential Manager. • Sin una tarjeta Java/token, el usuario puede cancelar la conexión de Credential Manager, lo que dará lugar a la aparición de la conexión de Microsoft Windows. Llegado este punto, el usuario puede conectarse. • Con la tarjeta Java/token, el siguiente parche provisional permite que el usuario active/desactive la apertura de Credential Manager una vez insertada la tarjeta Java. 1. Haga clic en **Advanced Settings** (Configuración avanzada). 2. Haga clic en **Service & Applications** (Servicio y aplicaciones). 3. Haga clic en **Java Cards and Tokens** (Tarjetas Java y tokens). 4. Haga clic una vez que haya insertado la tarjeta Java/token. 5. Seleccione la casilla de verificación **Advise to log-on** (Avisar para conectar).

Descripción breve	Detalles	Solución
Los usuarios pierden todas las credenciales de Credential Manager protegidas por el TPM, si el módulo TPM se elimina o daña.	Si el módulo TPM se elimina o daña, los usuarios perderán todas las credenciales protegidas por el TPM.	Así es como se ha diseñado. El Módulo TPM está diseñado para proteger las credenciales de Credential Manager. HP recomienda al usuario que haga una copia de seguridad de la identidad en Credential Manager antes de retirar el módulo TPM.
Credential Manager no se configura como conexión principal de Windows 2000.	Durante la instalación de Windows 2000, la política de conexión se configura para administración de conexión manual o automática. Si se elige la conexión automática, la configuración de registro predeterminada de Windows establece el valor predeterminado de conexión automática en 1, y Credential Manager no lo anula.	Así es como se ha diseñado. Si el usuario desea modificar la configuración del sistema operativo, con el fin de ignorar los valores de conexión automáticos, la ruta de edición es `HKEY_LOCAL_MACHINE/Software/Microsoft/WindowsNT/CurrentVersion/WinLogon` **PRECAUCIÓN:** ¡Utilice el Editor de registro bajo su riesgo! La utilización del Editor de registro (regedit) de manera incorrecta puede causar problemas serios que pueden requerir una reinstalación del sistema operativo. No hay ninguna garantía de que los problemas causados por el empleo incorrecto del Editor de registro puedan solucionarse.
El mensaje de conexión de huella digital aparece tanto si el lector de huella digital está o no instalado o registrado.	Si el usuario selecciona la conexión de Windows, aparece la siguiente alarma de escritorio en la barra de tareas de Credential Manager: **Es posible colocar el dedo en el lector de huella digital para conectarse al Credential Manager.**	El objetivo de la alarma de escritorio es notificar al usuario la disponibilidad de la autentificación de huella digital, si estuviera configurada.
La ventana de conexión de Credential Manager para Windows 2000 indica **insert card** (insertar tarjeta) cuando no hay ningún lector asociado.	La pantalla de Windows Credential Manager Welcome sugiere al usuario que se puede conectar con **insert card** (insertar tarjeta) cuando no está asociado ningún lector de tarjeta Java Card.	El objetivo de la alarma es notificar al usuario la disponibilidad de la autentificación de tarjeta Java, si estuviera configurada.
No es posible acceder a Credential Manager después de pasar del modo de suspensión a hibernación únicamente en Windows XP Service Pack 1.	Después de permitir que el sistema pase del modo de suspensión al de hibernación, el administrador o usuario no podrá acceder a Credential Manager y la pantalla de conexión de Windows se mostrará independientemente de la credencial de conexión seleccionada (contraseña, huella digital o tarjeta Java).	Esta cuestión parece haberse solucionado en Service Pack 2 de Microsoft. Para obtener más información sobre esta cuestión, consulte el artículo básico informativo 813301 de Microsoft, en http://www.microsoft.com. Para conectarse, el usuario debe seleccionar Credential Manager e iniciar la sesión. Después de entrar en Credential Manager, se solicita que el usuario se conecte a Windows (el usuario deberá probablemente seleccionar la opción de conexión de Windows) para completar el proceso de conexión. Si el usuario se registra primero en Windows, deberá entonces registrarse manualmente en Credential Manager.
La restauración de la seguridad integrada provoca el fallo de Credential Manager.	Credential Manager no puede registrar credenciales después de que se haya restaurado la configuración de fábrica de la ROM.	HP Credential Manager for ProtectTools no puede acceder al TPM si se restauró la configuración de fábrica de la ROM después de la instalación de Credential Manager. El chip de seguridad integrada TPM puede activarse en la utilidad BIOS Computer Setup, en BIOS Configuration for ProtectTools, o en HP

Descripción breve	Detalles	Solución
		Client Manager. Para activar el chip de seguridad integrada TPM: 1. Abra Computer Setup encendiendo o reiniciando el ordenador y, a continuación, pulse F10 cuando el mensaje **F10 = ROM Based Setup** se muestre en la esquina izquierda inferior de la pantalla. 2. Utilice las teclas de flecha para seleccionar **Security** (Seguridad) > **Setup Password** (Configurar contraseña). Configurar una contraseña. 3. Seleccione **Embedded Security Device** (Dispositivo de seguridad integrada). 4. Utilice las teclas de dirección para seleccionar **Embedded Security Device—Disable** (Dispositivo de seguridad integrada: desactivar). Utilice las teclas de dirección para seleccionar **Embedded Security Device—Disable** (Dispositivo de seguridad integrada: desactivar). 5. Seleccione **Enable** (Activar) > **Save changes and exit** (Guardar cambios y salir). HP está trabajando en opciones de solución para futuras versiones de software de clientes.
El proceso de seguridad **Restore Identity** (Restaurar identidad) pierde su 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 conexión. Incluso aún cuando Credential Manager tenga registrado el token virtual, el usuario deberá registrar de nuevo el token para restaurar la asociación.	Esto sucede según el diseño actual. Cuando se desinstala Credential Manager sin guardar las identidades, la parte del sistema (servidor) del token se destruye, y por lo tanto ya no puede usarse el token para conexión, incluso si la parte de cliente del token se restaura a través de la restauración de la identidad. HP está trabajando en las opciones de solución a largo plazo.

Embedded Security for ProtectTools

Descripción breve	Detalles	Solución
El cifrado de carpetas, subcarpetas, y archivos en PSD provoca mensajes de error.	Si el usuario copia archivos y carpetas en la PSD y trata de cifrar carpetas/archivos o carpetas/subcarpetas, aparece el mensaje **Error Applying Attributes** (Error al aplicar atributos). El usuario puede cifrar los mismos archivos en la unidad C:\ en una unidad de disco duro adicional instalada.	Así es como se ha diseñado. Cuando se desplazan archivos/carpetas a la PSD, automáticamente se cifran. No hay ninguna necesidad de “duplicar el cifrado” de archivos/carpetas. El intento de duplicar su cifrado en la PSD, mediante el EFS, causará este mensaje de error.
No se pude tomar propiedad con otro sistema operativo en la plataforma de multiarranque.	Si se configura una unidad para arranque múltiple del sistema operativo, sólo se podrá adquirir propiedad con el asistente de inicialización de la plataforma en un sistema operativo.	Así se ha diseñado, por motivos de seguridad.
Un administrador no autorizado puede ver, suprimir, renombrar, o mover el contenido de carpetas cifradas EFS.	El cifrado de una carpeta no impide que un usuario no autorizado con derechos administrativos vea, suprima, o mueva el contenido de la carpeta.	Así es como se ha diseñado. Es una función del EFS, no del Embedded Security TPM. La seguridad integrada utiliza el software Microsoft EFS, y EFS conserva los derechos de acceso a archivos/carpetas de todos los administradores.
Las carpetas cifradas con EFS en Windows 2000 no se muestran resaltadas en verde.	Las carpetas cifradas con EFS se resaltan en verde en Windows XP, pero no en Windows 2000.	Así es como se ha diseñado. Es una función de EFS la que no resalta las carpetas cifradas en Windows 2000, pero sí lo hace en Windows XP. Esto ocurre independientemente de que esté o no instalada Embedded Security TPM.
EFS no requiere una contraseña para ver archivos cifrados en Windows 2000.	Si un usuario configura Embedded Security, se conecta como un administrador, luego se desconecta y se vuelve a conectar como el administrador, podrá ver los archivos/carpetas en Windows 2000 sin necesidad de contraseña. Sólo ocurre en la primera cuenta de administrador en Windows 2000. Si se registra una cuenta de administrador secundaria, esto no sucede.	Así es como se ha diseñado. Se trata de una función de EFS en Windows 2000. EFS en Windows XP, de manera predeterminada, no dejará que el usuario abra archivos/carpetas sin una contraseña.
No debería instalarse software en una restauración con partición FAT32.	Si el usuario intenta restaurar el disco duro utilizando FAT32, no habrá opciones de cifrado para ninguno de los archivos/carpetas que utilicen EFS.	Así es como se ha diseñado. Microsoft EFS es compatible solamente con NTFS y no funcionará con FAT32. Se trata de una función de Microsoft EFS y no está relacionada con el software HP ProtectTools.
El usuario de Windows 2000 puede compartir con la red cualquier PSD con la parte ($) oculta.	El usuario de Windows 2000 puede compartir con la red cualquier PSD con la parte ($) oculta. Se puede acceder a la parte oculta en la red utilizando la parte ($) oculta.	La PSD no se comparte normalmente en la red, pero puede hacerse a través de la parte ($) oculta en Windows 2000 únicamente. HP recomienda siempre tener protegida con contraseña la cuenta de administrador incorporada.
El usuario puede cifrar o eliminar el archivo XML del archivo de recuperación.	Según su diseño, las ACL de esta carpeta no están configuradas; por lo tanto, un usuario podría deliberadamente o no cifrar o eliminar el archivo, haciéndolo inaccesible. Una vez que este archivo haya sido cifrado o eliminado, nadie podrá usar el software TPM.	Así es como se ha diseñado. Los usuarios tienen derechos de acceso a un archivo de emergencia para guardar/actualizar su copia de seguridad de la clave de usuario básico. Los clientes deberían adoptar un enfoque de seguridad basado en “prácticas recomendadas” e instruir a los usuarios para que nunca cifren o eliminen los datos del archivo de recuperación.
La interacción de HP ProtectTools Embedded	Los archivos cifrados interfieren con el escaneado de virus de Symantec	Para reducir el tiempo necesario para escanear los archivos HP ProtectTools Embedded Security EFS, el

Descripción breve	Detalles	Solución
Security EFS con Symantec Antivirus o Norton Antivirus da lugar a plazos de tiempo mayores en cifrado/descifrado y escaneado.	Antivirus o Norton Antivirus 2005. Durante este proceso de escaneado, la pantalla de contraseña de usuario básico solicita al usuario una contraseña cada 10 archivos aproximadamente. Si el usuario no introduce una contraseña, la pantalla de contraseña de usuario básico se desconecta, permitiendo que NAV2005 continúe con el escaneado. El cifrado de archivos con HP ProtectTools Embedded Security EFS lleva más tiempo cuando se ejecutan Symantec Antivirus o Norton Antivirus.	usuario debe introducir la contraseña de cifrado antes del escaneado o descifrar antes del escaneado. Para reducir el tiempo requerido para cifrar/descifrar datos utilizando HP ProtectTools Embedded Security EFS, el usuario debe desactivar la Protección automática en Symantec Antivirus o Norton Antivirus.
No se puede guardar el archivo de recuperación de emergencia en medios extraíbles.	Si el usuario inserta una tarjeta MMC o SD en el momento de crear la ruta del archivo de recuperación de emergencia durante la inicialización de Embedded Security, aparecerá un mensaje de error.	Así es como se ha diseñado. 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.
No se pueden cifrar datos en el entorno de Windows 2000 francés (Francia).	No existe la opción **Encrypt** (Cifrar) cuando se hace clic con el botón derecho en el icono de un archivo.	Se trata de una limitación del sistema operativo de Microsoft. Si se cambia la configuración regional (Francés [Canadá], por ejemplo), aparecerá la opción **Encrypt** (Cifrar). Para solucionar el problema, cifre el archivo de la manera siguiente: haga clic con el botón derecho del ratón en el icono del archivo y seleccione **Properties** (Propiedades) > **Advanced** (Avanzadas) > **Encrypt Contents** (Cifrar contenido).
Pueden ocurrir errores después de experimentar una pérdida de alimentación mientras tiene lugar la toma de propiedad, durante la inicialización de Embedded Security.	Si hay una pérdida de alimentación mientras se inicializa el chip de la seguridad integrada, pueden darse las siguientes circunstancias: • Cuando se intenta iniciar el asistente de inicialización de la seguridad integrada, se muestra el error siguiente: **The Embedded security cannot be initialized since the Embedded Security chip has already an Embedded Security owner.** (La seguridad integrada no puede inicializarse debido a que el chip de la seguridad integrada ya tiene un propietario.) • Cuando se intenta iniciar el asistente de inicialización de usuario, se muestra el error siguiente: **The Embedded security is not initialized. To use the wizard, the Embedded Security must be initialized first.** (Embedded Security no se ha inicializado. Para utilizar el asistente, debe inicializarse antes Embedded Security.)	Realice el procedimiento siguiente para la recuperación de la pérdida de alimentación: **NOTA:** Utilice las teclas de flecha para seleccionar distintos menús, artículos de menú y para cambiar valores (a no ser que se indique lo contrario). 1. Inicie o reinicie el ordenador. 2. Pulse F10 cuando el mensaje **F10=Setup** aparezca en pantalla (o cuando el indicador luminoso del monitor se muestre en verde). 3. Seleccione la opción de idioma apropiada. 4. Pulse Intro. 5. Seleccione **Security** (Seguridad) > **Embedded Security** (Embedded Security). 6. Configure la opción **Embedded Security Device** (Dispositivo de seguridad integrada) en **Enable** (Activar). 7. Pulse F10 para aceptar el cambio. 8. Seleccione **File** (Archivo) > **Save Changes and Exit** (Guardar cambios y salir). 9. Pulse INTRO. 10. Pulse F10 para guardar los cambios y salir de la utilidad de configuración de F10.
La contraseña de la utilidad Computer Setup (F10) puede eliminarse	La activación del módulo TPM requiere una contraseña de la utilidad Computer Setup (F10). Una vez que el módulo haya sido activado, el usuario puede	Así es como se ha diseñado. La contraseña de la utilidad Computer Setup (F10) sólo puede ser eliminada por un usuario que conozca la

Descripción breve	Detalles	Solución
una vez que se haya activado el Módulo TPM.	eliminar la contraseña. Esto permite que cualquier persona con acceso directo al sistema pueda reconfigurar el módulo TPM y provocar una posible pérdida de datos.	contraseña. No obstante, HP recomienda encarecidamente que se tenga la contraseña de la utilidad Computer Setup (F10) protegida en todo momento.
La casilla de contraseña de la PSD deja de mostrarse cuando el sistema se vuelve activo después del estado En espera.	Cuando un usuario se conecta al sistema después de crear una PSD, el TPM le solicita la contraseña de usuario básico. Si el usuario no introduce la contraseña y el sistema entra en En espera, el cuadro de diálogo de la contraseña no estará disponible cuando el usuario desee reanudar.	Así es como se ha diseñado. El usuario tiene que finalizar una sesión y retroceder para ver de nuevo el cuadro de contraseña de la PSD.
No se requiere contraseña para cambiar las directrices de la plataforma de seguridad.	El acceso a las directrices de la plataforma de seguridad (en el caso del equipo y del usuario) no requiere una contraseña TPM por parte de los usuarios que tengan derechos administrativos en el sistema.	Así es como se ha diseñado. Cualquier administrador puede modificar las directrices de la plataforma de seguridad con o sin la inicialización de usuario TPM.
Microsoft EFS no funciona plenamente en Windows 2000.	Un administrador puede tener acceso a la información cifrada en el sistema sin conocer la contraseña correcta. Si el administrador introduce una contraseña incorrecta o cancela el diálogo de contraseña, el archivo cifrado se abrirá como si el administrador hubiera introducido la contraseña correcta. Esto sucede independientemente de la configuración de seguridad utilizada cuando se cifraron los datos. Esto ocurre solamente en la primera cuenta de administrador en Windows 2000.	La política de recuperación de datos se configura automáticamente para designar a un administrador como agente de recuperación. Cuando una clave de usuario no se puede recuperar (como en el caso de introducir la contraseña incorrecta o cancelar el diálogo de Introducir contraseña), el archivo se descifra automáticamente con una clave de recuperación. Esto es debido a Microsoft EFS. Para obtener más información, consulte el artículo técnico informativo Q257705 en http://www.microsoft.com. Los documentos no los podrá abrir un usuario no-administrador
Cuando se visualiza un certificado, se muestra como no-fiable.	Después de configurar HP ProtectTools y ejecutar el asistente de inicialización de usuario, el usario podrá ver el certificado emitido; no obstante, cuando se visualiza, se muestra como no-fiable. Si bien el certificado puede instalarse en ese momento haciendo clic en el botón de instalar, su instalación no lo convierte en fiable.	Los certificados autofirmados no son fiables. En un entorno empresarial correctamente configurado, los certificados EFS son emitidos en línea por Autoridades de certificación y son fiables.
Se producen errores intermitentes en el cifrado y descifrado: **El proceso no puede acceder al archivo porque está siendo utilizado por otro proceso.**	Un error intermitente en extremo durante el cifrado o descifrado de archivos se debe a que el archivo está siendo utilizado por otro proceso, aún cuando el archivo o carpeta no estén siendo procesados por el sistema operativo u otras aplicaciones.	Para solucionar el fallo: 1. Reinicie el ordenador. 2. Salga de la sesión. 3. Inicie la sesión de nuevo.
La pérdida de datos en almacenamiento extraíble ocurre si el almacenamiento se extrae antes de la generación o transferencia de nuevos datos.	Si se extraen medios de almacenamiento como MultiBay, la unidad de disco duro sigue mostrando la disponibilidad de la PSD y no genera errores mientras se añaden/modifican datos en la PSD. Después del reinicio del sistema, la PSD no refleja los cambios de archivo que ocurrieron mientras el almacenamiento extraíble no estaba disponible.	El hecho sólo se percibe si el usuario accede a la PSD, y extrae la unidad de disco duro antes de que finalice la generación o transferencia de nuevos datos. Si el usuario intenta acceder a la PSD cuando la unidad de disco duro extraíble no está presente, se muestra el mensaje de error **the device is not ready** (el dispositivo no está listo).
Durante la desinstalación, si el usuario no ha inicializado Usuario	El usuario tiene la opción de desinstalar, bien sin desactivar el TPM, o desactivando primero el TPM (por medio	La herramienta Admin. se utiliza para desactivar el chip TPM, pero esta opción no estará disponible a no ser que la clave de usuario básico se haya inicializado. Si

Descripción breve	Detalles	Solución
básico y abre la herramienta Administración, la opción **Disable** (Desactivar) no estará disponible y el desinstalador no continuará hasta que se cierre la herramienta Administración.	de la herramienta Admin.), y desinstalando a continuación. El acceso a la herramienta Admin. requiere la inicialización de la clave de usuario básico. Si la inicialización básica no ha tenido lugar, todas las opciones serán inaccesibles para el usuario. Dado que el usuario ha decidido expresamente abrir la herramienta Admin. (haciendo clic en **Sí**) en el mensaje del cuadro de diálogo **Click Yes to open Embedded Security Administration tool** (Haga clic en Sí para abrir la herramienta de administración de Embedded Security), la desinstalación esperará a que se cierre la herramienta Admin. Si el usuario hace clic en **No** en el cuadro de diálogo, la herramienta Admin. no se abrirá y el proceso de desinstalación continuará.	no se ha inicializado, seleccione **OK** (Aceptar) o **Cancel** (Cancelar) para seguir con el proceso de desinstalación.
Ocurrirá un bloqueo intermitente del sistema después de crear la PSD en 2 cuentas de usuario y de utilizar el conmutador de usuario rápido en las configuraciones de sistemas de 128 MB.	El sistema puede bloquearse con una pantalla negra y el teclado y el ratón no responderán, en lugar de mostrarse la pantalla de bienvenida (conexión), si se utiliza la conmutación rápida con una RAM mínima.	La sospecha de causa de origen es una cuestión de programación en configuraciones de memoria baja. Los gráficos integrados utilizan la arquitectura UMA que emplea 8 MB de memoria, dejando solamente disponibles para el usuario 120 MB. Estos 120 MB son compartidos por los dos usuarios conectados y con conmutación de usuario rápido cuando se genera este error. El parche provisional es arrancar de nuevo el sistema y que el usuario incremente la configuración de memoria (HP no suministra configuraciones de 128 MB de manera predeterminada en los módulos de seguridad).
La autenticación de usuario EFS (requiere contraseña) se interrumpe con el mensaje **access denied** (acceso denegado).	La contraseña de autenticación de usuario EFS se vuelve a abrir después de hacer clic en **OK** (Aceptar) o de regresar del estado en espera después de la interrupción.	Se debe al diseño que trata de evitar problemas con Microsoft EFS; se creó un temporizador de guardia de 30 segundos para generar este mensaje de error.
Se observa un truncamiento menor en la descripción funcional durante la configuración en japonés	En la opción de configuración personalizada, en el asistente de instalación, se truncan las descripciones funcionales.	HP corregirá este problema en una próxima versión.
El cifrado EFS funciona sin introducir ninguna contraseña en la pantalla.	Al permitir que se interrumpa la pantalla de contraseña de usuario, es posible el cifrado de un archivo o una carpeta.	La capacidad de cifrado no requiere la autentificación de contraseña, ya que es una función del cifrado de Microsoft EFS. El descifrado requerirá el suministro de una contraseña de usuario.
Se da soporte al correo electrónico seguro, incluso si no está señalado en el asistente de inicialización de usuario, o si la configuración de correo electrónico está desactivada en las políticas de usuario.	El software de seguridad integrada y el asistente no controlan la configuración de un cliente de correo electrónico (Outlook, Outlook Express, o Netscape)	Así es como se ha diseñado. La configuración de los parámetros de correo electrónico del TPM no prohíbe la edición de la configuración de cifrado directamente en el cliente de correo electrónico. El uso de correo electrónico seguro se configura y controla por aplicaciones de terceros. El asistente de HP permite el enlace con las tres aplicaciones de referencia para personalización inmediata.

Descripción breve	Detalles	Solución
La ejecución de una distribución a gran escala por segunda vez en el mismo ordenador o en un ordenador inicializado previamente sobrescribe los archivos de recuperación de emergencia y los archivos de tokens de emergencia. Los nuevos archivos no son válidos para recuperación.	La ejecución de una distribución a gran escala en un sistema de seguridad inicializado previamente de HP ProtectTools Embedded Security inutilizará los archivos de recuperación y los tokens de recuperación existentes, al sobrescribir los archivos xml.	HP está trabajando para resolver el problema de sobrescritura de los archivos xml y suministrará una solución en un futuro SoftPaq.
Los scripts de conexión automatizados no funcionan durante la restauración del usuario en Embedded Security.	El error ocurre después de que el usuario • Inicialice al propietario y al usuario en Embedded Security (utilizando las ubicaciones predeterminadas: **Mis documentos**. • Restablezca la configuración de fábrica del chip en el BIOS. • Reinicie el ordenador. • Empieza a restaurar Embedded Security: durante el proceso de restauración, Credential Manager pregunta al usuario si el sistema puede automatizar la conexión en Infineon TPM User Authentication. Si el usuario selecciona **Sí**, la ubicación de SPEmRecToken aparecerá automáticamente en el cuadro de texto. Aunque esta ubicación sea correcta, se mostrará el mensaje de error siguiente: **No Emergency Recovery Token is provided. Select the token location the Emergency Recovery Token should be retrieved from.** (No se suministra token de recuperación de emergencia. Seleccione la ubicación de donde se recuperará el token de recuperación de emergencia.)	Haga clic en el botón **Browse** (Examinar) de la pantalla para seleccionar la ubicación y los procedimientos del proceso de restauración.
Las PSD de usuarios múltiples no funcionan en un entorno de conmutación de usuario rápido.	Este error ocurre cuando se crean usuarios múltiples y se les da una PSD con la misma letra de unidad. Si se intenta utilizar el conmutador de usuario rápido entre usuarios cuando la PSD está cargada, la PSD del segundo usuario no estará disponible.	La PSD del segundo usuario sólo estará disponible si se ha configurado de nuevo para que utilice otras letras de unidad o si el primer usuario finaliza la sesión.
La PSD se desactiva y no puede borrarse después de formatear la unidad de disco duro en la que se generó	La PSD se desactiva y no puede borrarse después de formatear la unidad de disco duro secundaria en la que se generó. El icono de la PSD es todavía visible, pero aparece el mensaje de error **drive is not accessible** (la unidad no es accesible) cuando el usuario intenta acceder a la PSD. El usuario no podrá borrar la PSD y aparecerá un mensaje informando que: **your PSD is still in use, please ensure that your PSD contains no open files**	Así es como se ha diseñado: si un cliente borra o desconecta la ubicación del almacenamiento de los datos de la PSD, la emulación de la unidad PSD de Embedded Security continuará funcionando, y causará errores basados en la falta de comunicación con los datos que faltan. Solución: después del siguiente reinicio, las emulaciones no cargan y el usuario puede borrar la antigua emulación de PSD y crear una nueva PSD.

Descripción breve	Detalles	Solución
	and is not accessed by another process. (Su PSD está todavía en uso, asegúrese de que no contiene archivos abiertos y que no está siendo utilizada por otro proceso). El usuario deberá reiniciar el sistema para borrar la PSD, que no estará cargada después del reinicio.	
Se ha detectado un error interno al restaurar del archivo automático de copias de seguridad.	Si el usuario • hace clic en la opción **Restore under Backup** (Restaurar a partir de copias de seguridad) de Embedded Security en HPPTSM para restaurar desde el archivo automático de copias de seguridad • selecciona **SPSystemBackup.xml** el asistente de restauración falla y se muestra el siguiente mensaje de error: **The selected Backup Archive does not match the restore reason. Please select another archive and continue.** (El archivo de copias de seguridad seleccionado no coincide con el motivo de la restauración. Por favor seleccione otro archivo y continúe).	Si el usuario selecciona **SpSystemBackup.xml** cuando se requiere el SpBackupArchive.xml, el asistente de Embedded Security mostrará el siguiente mensaje de error: **se ha detectado un error interno de Embedded Security.** El usuario debe seleccionar el archivo .xml correcto para que coincida con el motivo requerido. Los procesos funcionan tal como se diseñaron y adecuadamente; no obstante, el mensaje de error interno de Embedded Security no está claro y se debería configurar un mensaje más apropiado. HP está trabajando para mejorarlo en futuros productos.
El sistema de seguridad muestra un error de restauración con usuarios múltiples.	Durante el proceso de restauración, si el administrador selecciona usuarios para restaurar, los usuarios no seleccionados no podrán restaurar las claves cuando intenten restaurar en otra ocasión. Se muestra un mensaje de error **decryption process failed** (fallo del proceso de descifrado).	Los usuarios no seleccionados pueden restaurarse reconfigurando el TPM, ejecutando el proceso de restauración y seleccionando a todos los usuarios antes de que se ejecute la siguiente copia de seguridad diaria predeterminada. Si se ejecuta la copia de seguridad automática, sobrescribirá a los usuarios no restaurados y se perderán sus datos. Si se almacena una nueva copia de seguridad del sistema, los usuarios no seleccionados previamente no podrán restaurarse. Asimismo, el usuario debe restaurar la copia de seguridad de todo el sistema. Una copia de seguridad del archivo puede restaurarse individualmente.
El restablecimiento de los valores predeterminados de la ROM del sistema oculta el TPM.	El restablecimiento de los valores predeterminados de la ROM del sistema oculta el TPM a Windows. Esto no permite que el software de seguridad funcione correctamente y convierte en inaccesibles los datos cifrados del TPM.	Elimine la ocultación del TPM en el BIOS: Abra la utilidad Computer Setup (F10), localice **Security** (Seguridad) > **Device security** (Seguridad del dispositivo), modifique el campo de **Hidden** (Oculto) a **Available** (Disponible).
La copia de seguridad automática no funciona con unidades asignadas.	Cuando un administrador configura la copia de seguridad automática en Embedded Security, crea una entrada en **Windows** > **Tasks** (Tareas) > **Scheduled Task** (Tarea programada). Esta tarea programada de Windows está configurada para utilizar NT AUTHORITY\SYSTEM y ejecutar la copia de seguridad. Funciona correctamente en cualquier unidad local. Cuando el administrador configura la copia de seguridad para que se guarde en una unidad asignada, el proceso falla porque el NT AUTHORITY\SYSTEM no tiene los derechos para utilizar la unidad asignada.	La manera de solucionarlo es cambiar el NT AUTHORITY\SYSTEM por el (nombre del ordenador)\ (nombre del administrador). Esta es la configuración predeterminada si la Tarea programada se crea manualmente. HP está trabajando para suministrar futuras versiones de producto con configuraciones predeterminadas que incluyan el nombre del ordenador/nombre del administrador.

Descripción breve	Detalles	Solución
	Si la copia automática de seguridad está programada para ocurrir después de la conexión, el icono de Embedded Security TNA muestra el siguiente mensaje: **The Backup Archive location is currently not accessible. Click here if you want to backup to a temporary archive until the Backup Archive is accessible again.** (La ubicación del archivo de copia de seguridad no es actualmente accesible. Haga clic aquí si desea hacer una copia de seguridad en un archivo temporal hasta que el archivo de copia de seguridad sea accesible de nuevo.) No obstante, si la copia automática de seguridad está programada para una hora específica, la copia de seguridad falla sin que se muestre ningún aviso del fallo.	
No es posible desactivar Embedded Security State temporalmente en Embedded Security GUI.	El software 4.0 actual fue diseñado para las implementaciones del HP Notebook 1.1 B, así como para dar soporte a las implementaciones de HP Desktop 1.2. Esta opción de desactivación todavía se admite en la interfaz de software para plataformas TPM 1.1.	HP corregirá este problema en próximas versiones.

Otros

Software impactado: descripción breve	Detalles	Solución
HP ProtectTools Security Manager: advertencia recibida: **la aplicación de seguridad no puede instalarse hasta que HP Protect Tools Security Manager esté instalado**.	Todas las aplicaciones de seguridad como Embedded Security, tarjeta Java y biométricos son complementos extensibles para la interfaz de HP Security Manager. El Security Manager debe estar instalado antes de que pueda cargarse un complemento de seguridad autorizado por HP.	El software de HP ProtectTools Security Manager debe estar instalado antes de la instalación de cualquier complemento de seguridad.
Utilidad HP ProtectTools TPM Firmware Update para modelos dc7600 y modelos que incluyan TPM habilitadas para Broadcom. La herramienta suministrada a través del sitio Web de soporte de HP informa que **ownership required** (se requiere propiedad).	Se trata del comportamiento previsto de la utilidad TPM firmware para modelos dc7600 y modelos que incluyan Broadcom-enabled TPMs La herramienta de actualización del firmware permite al usuario actualizar el firmware, con o sin clave de autorización (EK). Cuando no existe ninguna EK, no se requiere autorización para realizar la actualización del firmware. Cuando existe una EK, debe existir un propietario TPM, ya que la actualización requiere la autorización del propietario. Una vez realizada la actualización, se debe reiniciar la plataforma para que el nuevo firmware surta efecto. Si el BIOS TPM ha sido restablecido en fábrica, la propiedad se elimina y se posterga la capacidad de actualización del firmware hasta que se hayan configurado la plataforma del software de Embedded Security y el asistente de inicialización de usuario. *Siempre que se realice una actualización de firmware, se recomienda reiniciar. La versión de firmware no se identifica correctamente hasta después del reinicio.	1. Reinstale el software de HP ProtectTools Embedded Security. 2. Ejecute la plataforma y el asistente de configuración de usuario. 3. Asegúrese de que el sistema incluye 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 **Microsoft .NET Framework 1.1** aparece en la lista. 4. Compruebe la configuración del software y el hardware: **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 de árbol. **e.** Haga clic en **More Details** (Más detalles). El sistema debería tener la configuración siguiente: • Versión de producto = V4.0.1 • Estado de Embedded Security: Estado del chip = Activado, Estado del propietario = Inicializado, Estado del usuario = Inicializado • Información de componentes: Versión espec. TCG = 1.2 • Vendedor = Broadcom Corporation • FW Versión = 2.18 (o superior) • TPM Device driver library versión 2.0.0.9 (o superior) 5. Si la versión FW no coincide con la 2.18, descargue y actualice el firmware del TPM. El TPM Firmware SoftPaq puede descargarse y está disponible en http://www.hp.com.

Software impactado: descripción breve	Detalles	Solución
HP ProtectTools Security Manager: intermitentemente, se muestra un error cuando se cierra la interfaz de Security Manager.	Intermitentemente (1 de cada 12 instancias), se crea un error al utilizar el botón de cierre, situado en la parte derecha superior de la pantalla, al cerrar el Security Manager antes de que las aplicaciones de complemento hayan terminado de cargarse.	Está relacionado con una dependencia de programación del tiempo de carga de los servicios de complemento al cerrar y reiniciar el Security Manager. Dado que PTHOST.exe es el alojamiento del resto de aplicaciones (complementos), depende de la capacidad del complemento en finalizar su tiempo de carga (servicios). La causa origen es el cierre del alojamiento antes de que el complemento haya tenido tiempo de completar su carga. Permita que el Security Manager finalice su mensaje de carga de servicios (mostrado en la parte superior de la ventana de Security Manager) y todos los complementos aparezcan en la columna izquierda. Para evitar fallos, asigne un tiempo razonable para la carga de estos complementos.
HP ProtectTools * General: el acceso sin restricción o los privilegios de administrador sin control suponen un riesgo para la seguridad.	Numerosos riesgos son posibles con un acceso sin restricción al ordenador cliente: • borrado de PSD • modificación malintencionada de la configuración de usuario • desactivación de las políticas y funciones de seguridad	De los administradores se espera que implementen las “prácticas recomendadas” en la restricción de los privilegios de usuarios finales y en la restricción del acceso a usuarios. No se deberían otorgar privilegios de administrador a usuarios no autorizados.
Las contraseñas del BIOS y del OS Embedded Security no están sincronizadas.	Si el usuario no valida una nueva contraseña como la contraseña de BIOS Embedded Security, esta contraseña retrocederá a la contraseña de seguridad integrada original, a través de F10 BIOS.	Su funcionamiento es el previsto; estas contraseñas pueden resincronizarse cambiando la contraseña de usuario básico del sistema operativo y autentificándolo en la pantalla de contraseña de BIOS Embedded Security.
Sólo un usuario puede conectarse al sistema después de que la autentificación de prearranque del TPM se active en el BIOS.	El PIN de TPM BIOS se asocia con el primer usuario que inicializa la configuración de usuario. Si un ordenador tiene usuarios múltiples, el primer usuario es, esencialmente, el administrador. El primer usuario tendrá que dar su PIN de usuario del TPM a otros usuarios para que puedan conectarse.	El funcionamiento es el previsto; HP recomienda que el departamento TI del cliente aplique una política de seguridad adecuada para desplegar su solución de seguridad y asegure que la contraseña de administrador del BIOS la configuren los administradores TI con el fin de proteger el sistema.
El usuario tiene que cambiar el PIN para conseguir que funcione el prearranque del TPM después de un restablecimiento de fábrica del TPM.	El usuario tiene que cambiar el PIN o crear otro usuario para inicializar su configuración de usuario, con el fin de que la autentificación del TPM BIOS funcione después del restablecimiento. No hay ninguna opción para conseguir que la autentificación de TPM BIOS funcione.	Así se ha diseñado, el restablecimiento de fábrica elimina la clave de usuario básico. El usuario debe cambiar su PIN de usuario o crear un nuevo usuario para reinicializar la clave de usuario básico.
Power-on authentication support (Ayuda de autentificación de arranque) no se configura en valores predeterminados cuando se utiliza Embedded Security **Reset to Factory Settings** (Restablecer configuración de fábrica)	En Computer Setup, la opción **Power-on authentication support** (Ayuda de autentificación de arranque) no se restablece en los valores de fábrica cuando se utiliza la opción Embedded Security Device **Reset to Factory Settings** (Restablecer valores de fábrica). De manera predeterminada, **Power-on authentication support** (Ayuda de autentificación de arranque) está configurada en **Disable** (Desactivar).	La opción **Reset to Factory Settings** (Restablecer valores de fábrica) desactiva el dispositivo Embedded Security, que oculta el resto de opciones de Embedded Security (incluida **Power-on authentication support** [Ayuda de autentificación de arranque]). No obstante, una vez reactivado el dispositivo Embedded Security, la opción **Power-on authentication support** (Ayuda de autentificación de arranque) permanece activada. HP está trabajando en una solución, que se suministrará en futuras ofertas SoftPaq de ROM basada en Web.

Software impactado: descripción breve	Detalles	Solución
La autentificación del arranque de seguridad solapa la contraseña del BIOS durante la secuencia de arranque.	La autentificación de arranque solicita al usuario que se conecte al sistema utilizando la contraseña TPM, pero si el usuario pulsa F10 para acceder al BIOS, sólo se otorga acceso de derechos de lectura.	Para poder escribir en el BIOS, el usuario debe introducir la contraseña del BIOS en vez de la contraseña TPM en la ventana de autentificación de arranque.
El BIOS solicita las contraseñas antigua y nueva a través de Computer Setup, después de cambiar la contraseña de Propietario en el software de Embedded Security Windows.	El BIOS solicita las contraseñas antigua y nueva a través de Computer Setup, después de cambiar la contraseña de Propietario en el software de Embedded Security Windows.	Así es como se ha diseñado. Se debe a la incapacidad del BIOS de comunicarse con el TPM, una vez que el sistema operativo está activo y en ejecución, y de comparar la frase de paso del TPM con el blob clave del TPM.

Glosario

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

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.

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.

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

Chip embedded security de Trusted Platform Module (TPM) (sólo en algunos modelos) Chip de seguridad integrado que protege la información más importante del usuario contra ataques maliciosos. Es la base de la confianza en una determinada plataforma. El TPM provee algoritmos criptográficos y operaciones que cumplen especificaciones del Trusted Computing Group (TCG).

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

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

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

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

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 con un usuario y requiere que el usuario escriba la contraseña correcta de DriveLock al encender el equipo.

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

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.

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.

Java 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.

Migración Tarea que permite la administración, restauración y transferencia de claves y certificados.

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.

Partición FAT Tabla de asignación de archivos (File Allocation Table), un método para indexar soportes de almacenamiento.

Partición NTFS Sistema de archivos NT (NT File System), un método para indexar soportes de almacenamiento. Este método cumple con las especificaciones de Windows Vista y Windows XP.

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

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

Reiniciar Proceso de reinicio del equipo.

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.

Single Sign On (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.

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 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 Java Card y un lector de tarjeta. El token se guarda en la unidad de 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.

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

Índice