Guía de HP ProtectTools Security Manager

Ordenadores de escritorio para empresas de HP Compaq

Guía de HP ProtectTools Security Manager

Ordenadores de escritorio para empresas de HP Compaq

Primera edición (agosto de 2006)

Referencia: 431330-071

Acerca de esta guía

En esta guía se proporcionan instrucciones para configurar y utilizar HP ProtectTools Security Manager.

ADVERTENCIA El texto señalado de esta forma significa que si no se siguen las indicaciones, se podrían producir lesiones personales e incluso la muerte.

PRECAUCIÓN El texto señalado de esta forma significa que si no se siguen las indicaciones, podrían producirse daños en el equipo o pérdida de información.

Nota El texto señalado de esta forma proporciona información complementaria importante.

Tabla de contenido

1 Introducción

HP ProtectTools Security Manager

El software ProtectTools Security Manager ofrece funciones de seguridad que facilitan la protección contra el acceso no autorizado a los ordenadores, redes y datos importantes. Los siguientes módulos proporcionan funciones de seguridad mejoradas:

- HP BIOS Configuration for ProtectTools
- HP Embedded Security for ProtectTools
- HP Credential Manager for ProtectTools
- HP Java Card Security for ProtectTools

Los módulos disponibles para el ordenador pueden variar dependiendo del modelo. Los módulos de ProtectTools pueden estar preinstalados, suministrados en el CD que acompaña al ordenador, o disponibles para su compra en la página Web de HP. Para obtener más información, visite la página http://www.hp.com.

Nota Para obtener instrucciones específicas sobre los módulos de ProtectTools, consulte las pantallas de ayuda de ProtectTools.

Para utilizar el Trusted Platform Module (TPM) (módulo de plataforma de confianza), las plataformas que incorporan un TPM requieren tanto un TCG Software Stack (TSS) como un software de seguridad integrado. Algunos modelos proporcionan el TSS; si no fuera el caso, puede adquirirse en HP. Además, el software que activa el TPM debe adquirirse por separado en el caso de algunos modelos. Para obtener más información, consulte Soluciones de terceros.

Acceso a HP ProtectTools Security Manager

Para acceder a ProtectTools Security Manager desde el panel de control de Microsoft Windows:

- Windows XP: Haga clic en **Inicio** > **Panel de control** > **Security Center** (Centro de seguridad) > **ProtectTools Security Manager**.
- Windows 2000: Haga clic en **Inicio** > **Todos los programas** > **HP ProtectTools Security Manager**.

Nota Una vez que haya configurado el módulo Credential Manager, podrá acceder a este módulo directamente desde la pantalla de acceso de Windows. Para obtener más información, consulte HP Credential Manager for ProtectTools.

Fundamentos de los roles de seguridad

En la gestión de la seguridad informática (particularmente en el caso de organizaciones extensas), una práctica importante consiste en asignar responsabilidades y derechos entre los diversos tipos de administradores y usuarios.

Nota En una organización pequeña o en el caso de uso individual, estos roles pueden estar asignados a la misma persona.

En el caso de ProtectTools, las obligaciones y los privilegios de seguridad pueden asignarse a los roles siguientes:

- Responsable de seguridad: define el nivel de seguridad de la empresa o de la red, y determina las funciones de seguridad que hay que implantar, como por ejemplo Tarjetas Java, lectores biométricos, o tokens USB.

  Nota En cooperación con HP, el responsable de seguridad puede personalizar una gran parte de las funciones de ProtectTools. Para obtener más información, visite la página http://www.hp.com.

- Administrador TI: aplica y gestiona las funciones de seguridad definidas por el responsable de seguridad. Puede asimismo activar y desactivar algunas funciones. Por ejemplo, si el responsable de seguridad ha decidido implantar Tarjetas Java, el administrador TI puede activar el modo de seguridad Java Card BIOS.
- Usuario: utiliza las funciones de seguridad. Por ejemplo, si el responsable de seguridad y el administrador TI han activado las Tarjetas Java en el sistema, el usuario puede definir el PIN de la Tarjeta Java y utilizar la tarjeta para autentificación.

De los administradores se espera que implementen las “prácticas recomendadas” en la restricción de los privilegios de los usuarios finales y en el acceso restrictivo a los usuarios.

Gestión de contraseñas de ProtectTools

La mayor parte de las funciones de ProtectTools Security Manager están protegidas con contraseña. En la tabla siguiente, figuran las contraseñas más comúnmente usadas, el módulo de software donde se incorpora la contraseña y la función de la contraseña.

Las contraseñas que únicamente configuran y utilizan los administradores TI se indican asimismo en la tabla. El resto de contraseñas pueden establecerlas los usuarios habituales o los administradores.

Tabla 1-1 Gestión de contraseñas

Contraseña de ProtectTools	Configurada en este módulo de ProtectTools	Función
Contraseña del administrador de Computer Setup **Nota** También se conoce como contraseña del administrador del BIOS, de configuración de F10, o de configuración de la seguridad	Configuración del BIOS, por el administrador TI	Protege el acceso a la utilidad y a la configuración de seguridad de BIOS Computer Setup.

Tabla 1-1 Gestión de contraseñas (continúa)

Contraseña de arranque	BIOS Configuration (Configuración del BIOS)	HP ProtectTools Power-On Authentication Support (Soporte de autentificación de arranque de HP ProtectTools) es una herramienta de seguridad basada en TPM, diseñada para evitar el acceso no autorizado al ordenador durante la operación de arranque. Power-On Authentication Support (Soporte de autentificación de arranque) utiliza la contraseña de usuario básico de HP ProtectTools Embedded Security. Una vez que se activa la Autentificación de arranque en Computer Setup, la contraseña queda establecida cuando se inicializa la primera/siguiente clave de usuario básico de Embedded Security (Seguridad integrada). El chip TPM de Embedded Security protege la contraseña de Autentificación de arranque.
contraseña del administrador de la Tarjeta Java **Nota** También se conoce como contraseña de la tarjeta del administrador del BIOS	Seguridad de la Tarjeta Java, por el administrador TI	Asocia la Tarjeta Java al ordenador con fines de identificación. Permite que un administrador informático active o desactive las contraseñas de Computer Setup, genere una nueva tarjeta de administrador y cree archivos de recuperación para restaurar las tarjetas de usuario o de administrador.
PIN de la Tarjeta Java	Seguridad de la Tarjeta Java	Protege el acceso al contenido de la Tarjeta Java y el acceso al ordenador cuando se utilizan una Tarjeta Java y un lector opcionales. Verifica si la contraseña de usuario de la Tarjeta Java se ha duplicado; se utiliza para registrar la autentificación de la Tarjeta Java
Contraseña de archivo de recuperación de la Tarjeta Java (si estuviera disponible)	Seguridad de la Tarjeta Java	Protege el acceso al archivo de recuperación que contiene las contraseñas del BIOS.
Contraseña de usuario de la Tarjeta Java (si estuviera disponible) **Nota** También se conoce como contraseña de la tarjeta de usuario del BIOS	Seguridad de la Tarjeta Java	Asocia la Tarjeta Java al ordenador con fines de identificación. Permite que un usuario cree un archivo de recuperación para restaurar una tarjeta de usuario.
contraseña de usuario básico **Nota** También se conoce como: Contraseña de Seguridad Integrada, contraseña TPM de arranque previo	Embedded Security (Seguridad integrada)	Se utiliza para tener acceso a funciones de Seguridad Integrada, como cifrado seguro de correos electrónicos, archivos y carpetas. Cuando se activa como contraseña de soporte de autentificación de arranque del BIOS, protege el acceso al contenido del ordenador cuando se enciende, reinicia o restaura de la hibernación. También se utiliza para autentificar la unidad Personal Secure Drive (PSD) (Unidad personal segura) y para registrar la autentificación TPM.

Tabla 1-1 Gestión de contraseñas (continúa)

Contraseña token de recuperación de emergencia **Nota** También se conoce como: Clave token de recuperación de emergencia	Seguridad integrada, por el administrador TI	Protege el acceso al token de recuperación de emergencia, que es un archivo de copia de seguridad del chip TPM de seguridad integrada
Contraseña de propietario	Seguridad integrada, por el administrador TI	Protege el sistema y el chip TPM del acceso no autorizado a todas las funciones de propietario de Embedded Security.
Contraseña de acceso a Credential Manager	Credential Manager	Esta contraseña ofrece 2 opciones: • Puede utilizarse para sustituir el proceso de acceso a Windows, permitiendo el acceso simultáneo a Windows y a Credential Manager. • Puede utilizarse en un acceso aparte para acceder a Credential Manager una vez se haya accedido a Microsoft Windows.
Contraseña de archivo de recuperación de Credential Manager	Credential Manager, por el administrador TI	Protege el acceso al archivo de recuperación de Credential Manager.
contraseña de acceso a Windows	Panel de control de Windows	Puede utilizarse en el acceso manual o guardarse en la Tarjeta Java.
Contraseña del programador de copias de seguridad **Nota** Se utiliza una contraseña de usuario de Windows para configurar el programador de copias de seguridad de la seguridad integrada.	Seguridad integrada, por el administrador TI	Establece el programador de copias de seguridad de la seguridad integrada
Contraseña de PKCS #12 Import **Nota** Cada certificado importado tiene su propia contraseña específica.	Seguridad integrada, por el administrador TI	Contraseña utilizada para la clave de cifrado de otros certificados, en el caso de ser importados **Nota** No se requiere en el funcionamiento de software normal; el usuario puede optar por establecer esta contraseña cuando utiliza la seguridad integrada para enviar certificados importantes
Token de restablecimiento de contraseña	Seguridad integrada, por el administrador TI	Herramienta suministrada al cliente, que permite que el propietario restablezca la contraseña de usuario básico en el caso de perderla; la contraseña se utiliza para realizar esta operación de restablecimiento
Contraseña de administrador del agente de recuperación de Microsoft	Microsoft, por el administrador TI de seguridad	Garantiza que los datos cifrados de la unidad personal segura (PSD) puedan recuperarse. Para obtener más información, consulte http://www.microsoft.com/technet/

Tabla 1-1 Gestión de contraseñas (continúa)

Nota El agente de recuperación puede ser cualquier administrador local de equipos. Si se crea el agente de recuperación, será necesario conectarse como ese administrador en cuestión y se requerirá contraseña. El agente de recuperación puede descifrar los datos cifrados de todos los usuarios con tan sólo abrirlos (no se requiere Asistente).		prodtechnol/winxppro/support/dataprot.mspx **Nota** No se requiere en el funcionamiento de software normal; el usuario puede optar por establecer esta contraseña cuando utilice la seguridad integrada para enviar certificados importantes
PIN maestro del token virtual	Credential Manager	Opción del cliente de almacenar las credenciales de propietario con Credential Manager
PIN de usuario del token virtual	Credential Manager	Opción del cliente de almacenar las credenciales de propietario con Credential Manager
Contraseña del asistente de copia de seguridad de la identidad	Credential Manager, por el administrador TI	Sirve para proteger el acceso a la copia de seguridad de la identidad cuando se utiliza Credential Manager
Contraseña de autentificación del token virtual	Credential Manager	Utilizado para registrar la autentificación del token virtual por el Credential Manager
Alias de autentificación del TPM.	Credential Manager	Credential Manager lo utiliza en sustitución de la contraseña de usuario básico, en la opción de administrador o usuario
Acceso de huella digital	Credential Manager	Credential Manager permite que el usuario sustituya el acceso de contraseña de Windows por un acceso de huella digital conveniente y seguro. A diferencia de las contraseñas, las credenciales de huella digital no pueden ser compartidas, entregadas, robadas o adivinadas. Utilización por Credential Manager
Autentificación de token USB	Credential Manager	Utilizado por Credential Manager como una autentificación token en lugar de una contraseña

Acceso a autentificación de multifactor de Credential Manager

Credential Manager Logon permite que la tecnología de autentificación de multifactor acceda al sistema operativo Windows. Incrementa la seguridad de acceso de la contraseña estándar de Windows, al requerir una autentificación de multifactor. También hace más fácil la experiencia de acceso cotidiana, al eliminar la necesidad de recordar contraseñas de usuario. Una función singular de Credential Manager Logon es la capacidad de agregar credenciales de cuentas múltiples en una sola identidad de usuario, lo que hace posible el empleo de la autentificación de multifactor sólo una vez y el acceso múltiple a diferentes cuentas de Windows con el mismo conjunto de credenciales.

La autentificación multifactor de usuario admite cualquier combinación de contraseñas de usuario, contraseñas dinámicas o de un sólo uso, TPM, Tarjetas Java, tokens USB, tokens virtuales y

biométricos. Credential Manager admite también métodos de autentificación alternativos, facilitando la posibilidad de múltiples privilegios de acceso de usuario para la misma aplicación o servicio. Un usuario puede consolidar todas las credenciales, contraseña de aplicación, y cuentas de red en una sola unidad de datos denominada Identidad de usuario. La identidad de usuario siempre está cifrada y protegida con la autentificación de multifactor.

Creación de una contraseña segura

A la hora de crear contraseñas, se deben seguir las especificaciones que el programa establezca. En general, sin embargo, considere las directrices siguientes que le servirán para crear contraseñas fiables y reducir sus posibilidades de riesgo:

- Utilice contraseñas con más de 6 caracteres, preferentemente con más de 8.
- Combine mayúsculas y minúsculas en el conjunto de la contraseña.
- Siempre que sea posible, combine caracteres alfanuméricos e incluya caracteres especiales y signos de puntuación.
- Substituya caracteres especiales o números por letras en una palabra clave. Por ejemplo, se podría utilizar el número 1 en lugar de las letras I o L.
- Combine palabras de 2 o más idiomas.
- Intercale en una palabra o frase números o caracteres especiales; por ejemplo, “Mary22Cat45”.
- No utilice una contraseña que aparecería en un diccionario.
- No utilice su nombre para la contraseña, o ninguna otra información personal, como la fecha de nacimiento, su diminutivo, o el apellido de su madre, incluso si lo escribe al revés.
- Cambie las contraseñas periódicamente. Podría cambiar únicamente un par de caracteres.
- Si anota su contraseña, no la guarde en un lugar visible y próximo al ordenador.
- No guarde la contraseña en un archivo, como por ejemplo un correo electrónico, del ordenador.
- No comparta cuentas ni transmita a nadie su contraseña.

Tareas avanzadas

Gestión de la configuración de ProtectTools

Algunas de las funciones de ProtectTools Security Manager pueden gestionarse en la Configuración del BIOS.

Activar y desactivar ayuda de autentificación de arranque de la Tarjeta Java.

Si esta opción está disponible, su activación le permitirá utilizar la Tarjeta Java para la autentificación de usuario cuando encienda el ordenador.

Nota Para activar plenamente la función de autentificación de arranque, se debe configurar la Tarjeta Java, utilizando el módulo Java Card Security for ProtectTools.

Para activar la ayuda de autentificación de arranque de la Tarjeta Java:

1. Seleccione **Inicio** > **Todos los programas** > **HP ProtectTools Security Manager**.
2. En el panel izquierdo, seleccione **BIOS Configuration**.
3. Introduzca su contraseña de administrador de Computer Setup en la pantalla de contraseña de administrador del BIOS, y haga clic en **OK** (Aceptar).
4. En el panel izquierdo, seleccione **Security** (Seguridad).
5. En **Java Card Security** (Seguridad de la Tarjeta Java), seleccione **Enable** (Activar).

   Nota Para desactivar la autentificación de arranque de la Tarjeta Java, seleccione **Disable** (Desactivar).

6. Haga clic en **Apply** (Aplicar), y a continuación **OK** (Aceptar) en la ventana de **ProtectTools** para guardar los cambios.

Activar y desactivar la ayuda de autentificación de arranque para seguridad integrada.

Si esta opción está disponible, su activación permitirá al sistema utilizar el chip de seguridad integrada TPM para la autentificación de usuario cuando encienda el ordenador.

Nota Para activar plenamente la función de autentificación de arranque, se debe configurar el chip de seguridad integrada TPM, utilizando el módulo Embedded Security for ProtectTools.

Para activar la ayuda de autentificación de arranque para seguridad integrada:

1. Seleccione **Inicio** > **Todos los programas** > **HP ProtectTools Security Manager**.
2. En el panel izquierdo, seleccione **BIOS Configuration**.
3. Introduzca su contraseña de administrador de Computer Setup en la pantalla de contraseña de administrador del BIOS, y haga clic en **OK** (Aceptar).
4. En el panel izquierdo, seleccione **Security** (Seguridad).
5. En **Embedded Security** (Seguridad integrada), seleccione **Enable Power-On Authentication Support** (Activar ayuda de autentificación de arranque).

Nota Para desactivar la autentificación de arranque para seguridad integrada, seleccione **Disable** (Desactivar).

6. Haga clic en **Apply** (Aplicar), y a continuación **OK** (Aceptar) en la ventana de **ProtectTools** para guardar los cambios.

Gestión de las contraseñas de Computer Setup

Se puede utilizar BIOS Configuration (Configuración del BIOS) para establecer y modificar las contraseñas de arranque y de configuración en Computer Setup, y gestionar asimismo diversas configuraciones de contraseñas.

PRECAUCIÓN Las contraseñas que se establezcan en la página **Passwords** (Contraseñas) en BIOS Configuration (configuración del BIOS) se guardan inmediatamente haciendo clic en **Apply** (Aplicar) o en el botón de **OK** (Aceptar) en la ventana **ProtectTools**. Asegúrese de recordar la contraseña establecida, ya que no podrá eliminar la configuración de una contraseña sin suministrar la contraseña previa.

La contraseña de arranque puede proteger el ordenador de un empleo no autorizado.

Nota Una vez que haya establecido una contraseña de arranque, el botón **Set** (Establecer) de la página de **Passwords** (Contraseñas) es sustituido por el botón **Change** (Cambiar).

La contraseña de administrador de Computer Setup protege los parámetros de configuración y la información de identificación del sistema en Computer Setup. Una vez establecida la contraseña, debe introducirse para acceder a Computer Setup.

Si ha establecido una contraseña de administrador, se le requerirá esta contraseña antes de que se abra la parte de BIOS Configuration de ProtectTools.

Nota Una vez que haya establecido una contraseña de administrador, el botón **Set** (Establecer) de la página **Passwords** (Contraseñas) es sustituido por el botón **Change** (Cambiar).

Configuración de la contraseña de arranque (si estuviera disponible)

Para configurar la contraseña de arranque:

1. Seleccione **Inicio** > **Todos los programas** > **HP ProtectTools Security Manager**.
2. En el panel izquierdo, seleccione **BIOS Configuration** (Configuración del BIOS), y a continuación seleccione **Security** (Seguridad).
3. En el panel derecho, junto a **Power-On Password** (Contraseña de arranque), haga clic en **Set** (Configurar).
4. Escriba y confirme la contraseña en los cuadros **Enter Password** (Introducir contraseña) y **Verify Password** (Verificar contraseña).
5. Haga clic en **OK** (Aceptar) en el cuadro de diálogo **Passwords**(Contraseñas).
6. Haga clic en **Apply** (Aplicar), y a continuación en **OK** (Aceptar) en la ventana de **ProtectTools** para guardar los cambios.

Cambio de contraseña de arranque (si estuviera disponible)

Para modificar la contraseña de arranque:

1. Seleccione **Inicio** > **Todos los programas** > **HP ProtectTools Security Manager**.
2. En el panel izquierdo, seleccione **BIOS Configuration** (Configuración del BIOS), y a continuación seleccione **Security** (Seguridad).
3. En el panel derecho, junto a **Power-On Password** (Contraseña de arranque), haga clic en **Change** (Cambiar).
4. Introduzca la contraseña actual en el cuadro **Old Password** (Contraseña antigua).
5. Introduzca y confirme la nueva contraseña en los cuadros **Enter New Password** (Introducir nueva contraseña) y **Verify New Password** (Verificar nueva contraseña).
6. Haga clic en **OK** (Aceptar) en el cuadro de diálogo **Passwords** (Contraseñas).
7. Haga clic en **Apply** (Aplicar), y a continuación en **OK** (Aceptar) en la ventana de **ProtectTools** para guardar los cambios.

Configuración del sistema

1. Inicializar HP ProtectTools Embedded Security.
2. Inicializar la clave de usuario básico.

Power-On Authentication Support (Ayuda de autentificación de arranque) se inicia tan pronto como se establecen la clave de usuario básico y la contraseña de usuario básico de arranque. Después de un nuevo arranque, se inicia HP ProtectTools Power-On Authentication Support (Ayuda de autentificación de arranque de HP ProtectTools) y se debe utilizar la contraseña de usuario básico para iniciar el ordenador. Una vez que esté operativa la ayuda de autentificación de arranque, dejará de verse la opción de entrar en BIOS Setup. Si el usuario introduce la contraseña de Setup (Configuración) en la ventana de la ayuda de autentificación de arranque, el usuario entrará en BIOS.

Una vez configurada la contraseña de usuario básico de seguridad integrada, debe cambiarse la contraseña para configurar la protección de contraseña, utilizando la autentificación de arranque.

Cambio de la ayuda de autentificación de arranque

La contraseña de Power-On Authentication Support (Soporte de autentificación de arranque) utiliza la contraseña de usuario básico de seguridad integrada. Para cambiar la contraseña:

1. Entre en la configuración de BIOS de F10 (debe tener una contraseña de configuración tal como se ha descrito en los pasos de configuración anteriores) y localice **Security** (Seguridad) > **Embedded Security Device** (Dispositivo de seguridad integrada) > **Reset authentication credential** (Restablecer credencial de autentificación).
2. Pulse las teclas de flecha para cambiar la configuración de **Do not reset** (No restablecer) por **Reset** (Restablecer)
3. Localice **Security Manager** (Gestor de seguridad) > **Embedded Security** (Seguridad integrada) > **User Settings** (Configuración de usuario) > **Basic User Password** (Contraseña de usuario básico) > **Change** (Cambiar).
4. Introduzca la contraseña antigua y, a continuación, confirme la contraseña nueva.

5. Vuelva a arrancar en el modo de ayuda de autentificación de arranque.

   La ventana de contraseña solicita que el usuario introduzca en primer lugar la contraseña antigua.

6. Introduzca la contraseña antigua y la contraseña nueva. (Si se introduce una contraseña nueva incorrecta tres veces seguidas, aparecerá una ventana donde se indicará que la contraseña no es válida y la autentificación de arranque volverá a la contraseña de seguridad integrada original F1 = Boot (arranque).

   Llegado este punto, las contraseñas no estarán sincronizadas y el usuario deberá cambiar de nuevo la contraseña de seguridad integrada para volver a sincronizarlas.)

Cambio de cuentas de usuario

La autentificación de arranque sólo admite un único usuario por vez. Para cambiar las cuentas de usuario que controlan la autentificación de arranque, se indican los siguientes pasos:

1. Localice **F10 BIOS** > **Security** (Seguridad) > **Embedded Security Device** (Dispositivo de seguridad integrada) > **Reset authentication credential** (Restablecer credencial de autentificación).
2. Utilice las teclas de flecha para desplazar el cursor lateralmente y, a continuación, pulse cualquier tecla para continuar.
3. Pulse F10 dos veces y, a continuación, Enter (Intro) para **Save Changes and Exit** (Guardar cambios y salir).
4. Crear/acceder a un usuario determinado de Microsoft Windows.
5. Abra Embedded Security (Seguridad integrada) e inicie Basic User Key (Clave de usuario básico) para la nueva cuenta de usuario de Windows. Si ya existiera una clave de usuario básico, cambie la contraseña de usuario básico para adquirir propiedad de la autentificación de arranque.

La autentificación de arranque aceptará únicamente la nueva contraseña de usuario básico.

PRECAUCIÓN Existen numerosos productos disponibles para la protección de datos, mediante cifrado de software, cifrado de hardware y hardware. La mayor parte se gestionan utilizando contraseñas. El fallo en la gestión de estas herramientas y contraseñas puede dar lugar a la pérdida de datos y de hardware, incluido el reemplazo de equipos. Revise con detenimiento todos los archivos de ayuda correspondientes antes de intentar utilizar estas herramientas.

Configuración de la contraseña del administrador de Computer Setup

Para configurar la contraseña del administrador de Computer Setup:

1. Seleccione **Inicio** > **Todos los programas** > **HP ProtectTools Security Manager**.
2. En el panel izquierdo, seleccione **BIOS Configuration** (Configuración del BIOS), y a continuación seleccione **Security** (Seguridad).
3. En el panel derecho, junto a **Setup Password** (Configurar contraseña, haga clic en **Set** (Configurar).
4. Escriba y confirme la contraseña en los cuadros **Enter Password** (Introducir contraseña) y **Confirm Password** (Confirmar contraseña).

5. Haga clic en **OK** (Aceptar) en el cuadro de diálogo **Passwords** (Contraseñas).
6. Haga clic en **Apply** (Aplicar), y a continuación en **OK** (Aceptar) en la ventana de **ProtectTools** para guardar los cambios.

Cambio de la contraseña del administrador de Computer Setup

Para cambiar la contraseña del administrador de Computer Setup:

1. Seleccione **Inicio** > **Todos los programas** > **HP ProtectTools Security Manager**.
2. En el panel izquierdo, seleccione **BIOS Configuration** (Configuración del BIOS), y a continuación seleccione **Security** (Seguridad).
3. En el panel derecho, junto a **Setup Password** (Configurar contraseña, haga clic en **Change** (Cambiar).
4. Introduzca la contraseña actual en el cuadro **Old Password** (Contraseña antigua).
5. Introduzca y confirme la nueva contraseña en los cuadros **Enter New Password** (Introducir nueva contraseña)y **Verify New Password** (Verificar nueva contraseña).
6. Haga clic en **OK** (Aceptar) en el cuadro de diálogo **Passwords** (Contraseñas).
7. Haga clic en **Apply** (Aplicar), y a continuación en **OK** (Aceptar) en la ventana de **ProtectTools** para guardar los cambios.

Ataque de diccionario con autentificación de arranque

Un ataque de diccionario es un método empleado para entrar en los sistemas de seguridad mediante la comprobación sistemática de todas las contraseñas posibles. Un ataque de diccionario contra la seguridad integrada podría tratar de descubrir la contraseña de propietario, la contraseña de usuario básico, o claves protegidas por contraseña. Embedded Security ofrece una defensa optimizada frente a los ataques de diccionario.

Defensa frente a los ataques de diccionario

La defensa de la seguridad integrada frente a los ataques de contraseña de diccionario consiste en detectar los intentos fallidos de autentificación y desactivar temporalmente el módulo TPM cuando se alcanza un determinado umbral de intentos fallidos. Una vez alcanzado el umbral de intentos fallidos, no sólo se desactiva el módulo TPM y se requiere un nuevo arranque, sino que se implementan tiempos en espera por bloqueo que van en aumento. En el transcurso del tiempo en espera, se ignorará la introducción de la contraseña correcta. La introducción de una contraseña incorrecta duplicará el último tiempo en espera.

En Embedded Security Help (Ayuda de seguridad integrada), se puede encontrar documentación adicional sobre este proceso. Haga clic en **Welcome to the HP Embedded Security for ProtectTools Solution** (Bienvenido a la solución HP Embedded Security for ProtectTools) > **Advanced Embedded Security Operation** (Operación avanzada de seguridad integrada) > **Dictionary Attack Defense** (Defensa frente a los ataques de diccionario).

Nota Normalmente, un usuario recibe advertencias de que su contraseña es incorrecta. Las advertencias informan del número de intentos que le quedan al usuario antes de que el módulo TPM se desactive.

El proceso de autentificación de arranque tiene lugar en la ROM antes de que se cargue el sistema operativo. La defensa frente a los ataques de diccionario está operativa, pero la única advertencia que obtiene el usuario es el símbolo clave X.

2 HP BIOS Configuration for ProtectTools

Conceptos básicos

BIOS Configuration for ProtectTools facilita el acceso a los parámetros de seguridad y configuración de la utilidad Computer Setup. Esto da a los usuarios acceso de Windows a las funciones de seguridad del sistema que gestiona Computer Setup.

Con BIOS Configuration, es posible:

- Gestionar contraseñas de arranque y de administrador.
- Configurar otras funciones disponibles de autentificación de arranque, como son la activación de contraseñas de Tarjeta Java, y ayuda de autentificación de seguridad integrada.
- Activar y desactivar funciones de hardware, como arranque de CD-ROM o puertos de hardware diferentes.
- Configurar las opciones de arranque, incluida la activación de MultiBoot (multiarranque) y modificar el orden de arranque.

Nota Gran parte de las funciones de BIOS Configuration for ProtectTools están también disponibles en Computer Setup.

Modificación de la configuración del BIOS

BIOS Configuration permite gestionar diversas configuraciones del ordenador que de otra forma estarían sólo disponibles pulsando F10 durante el arranque y entrando en la utilidad Computer Setup. Para obtener más información sobre la configuración y las funciones, consulte la *Guía sobre la utilidad Computer Setup (F10)* en el *Documentation and Diagnostics CD* que se suministró con el ordenador. Para acceder a los archivos de Ayuda para la configuración del BIOS, haga clic en **Security Manager** (Gestor de seguridad) > **BIOS Configuration** (Configuración del BIOS) > **Help** (Ayuda).

Nota Para obtener instrucciones específicas sobre la configuración de ProtectTools BIOS, consulte las pantallas de ayuda de ProtectTools.

3 HP Embedded Security for ProtectTools

Conceptos básicos

Si está disponible, Embedded Security for ProtectTools protege frente al acceso no autorizado a datos o credenciales de usuario. Este módulo proporciona las funciones de seguridad siguientes:

- Cifrado mejorado de archivos y carpetas de Microsoft Encrypting File System (EFS)
- Creación de una unidad personal segura (PSD) para cifrar datos de usuario
- Funciones de gestión de datos, como copias de seguridad y restauración de la jerarquía de claves
- Soporte para aplicaciones de terceros que utilicen MSCAPI (como Microsoft Outlook y Microsoft Internet Explorer) y aplicaciones que utilicen PKCS#11 (como Netscape) para operaciones protegidas de certificados digitales cuando se utilice el software Embedded Security

El chip de seguridad integrada de Trusted Platform Module (TPM) mejora y permite otras funciones de seguridad de ProtectTools Security Manager. Por ejemplo, Credential Manager for ProtectTools puede utilizar el chip integrado TPM como factor de autentificación cuando el usuario acceda a Windows. En algunos modelos, el chip de seguridad integrada TPM también potencia las funciones de seguridad del BIOS, a las que se accede por medio de BIOS Configuration for ProtectTools.

El hardware consiste en un TPM que cumple los estándares TPM 1.2 del Trusted Computing Group. El chip está integrado en la placa del sistema. Algunas implementaciones del TPM (dependiendo del modelo adquirido) integran el TPM como parte del NIC. En estas configuraciones NIC y TPM, la memoria on-chip y memoria off-chip, las funciones y el software de fábrica se localizan en un flash externo, integrado en la placa del sistema. Todas las funciones del TPM están cifradas o protegidas para asegurar un flash o unas comunicaciones seguras.

El software también facilita una función llamada PSD. La PSD es una función adicional al cifrado de archivos/carpetas basado en EFS, que utiliza el algoritmo de cifrado Advanced Encryption Standard (AES). Es importante destacar que HP ProtectTools Personal Secure Drive no funcionará a no ser que el TPM no esté oculto, habilitado con el software apropiado instalado con propiedad, e iniciada la configuración de usuario.

Procedimientos de configuración

PRECAUCIÓN Para reducir el riesgo de seguridad, se recomienda especialmente que el administrador TI inicie inmediatamente el chip de seguridad integrada TPM. Si el chip de seguridad integrada TPM no se ha inicializado, un usuario no autorizado o un gusano informático podría acceder al ordenador, o un virus podría iniciar el chip de seguridad TPM y restringir el acceso al ordenador.

El chip de seguridad integrada TPM puede activarse en la utilidad BIOS Computer Setup, en BIOS Configuration for ProtectTools, o en HP 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. Selecione **Embedded Security Device** (dispositivo de seguridad integrada).
4. Utilice las teclas de flecha para seleccionar **Embedded Security Device—Disable** (Dispositivo de seguridad integrada – Desactivar). Utilice las teclas de flecha para seleccionar **Embedded Security Device—Disable** (Dispositivo de seguridad integrada – Desactivar).
5. Seleccione **Enable** (Activar) > **Save changes and exit** (Guardar cambios y salir).

Nota Para obtener instrucciones específicas de ProtectTools Embedded Security, consulte las pantallas de ayuda de ProtectTools.

4 HP Credential Manager for ProtectTools

Conceptos básicos

Credential Manager for ProtectTools dispone de funciones de seguridad que proporcionan un entorno informático seguro y apropiado. Estas funciones incluyen las siguientes:

- Alternativas a las contraseñas cuando se accede a Microsoft Windows, como la utilización de una Tarjeta Java o un lector biométrico.
- Función de Single Sign On que recuerda de manera automática las credenciales (identificadores y contraseñas de usuarios) para sitios Web, aplicaciones y recursos de red.
- Soporte para dispositivos de seguridad opcionales, como Tarjetas Java y lectores biométricos.
- Soporte para configuraciones de seguridad adicionales, como la solicitud de autentificación con un dispositivo de seguridad opcional para desbloquear y las aplicaciones de acceso.
- Cifrado mejorado para contraseñas guardadas, cuando se implementa un chip de seguridad integrada TPM.

Procedimiento de inicio

Para iniciar Credential Manager, si estuviera disponible:

1. Haga clic en **Inicio** > **Panel de control** > **Security Center** (Centro de seguridad) > **Credential Manager**.
2. Haga clic en **Log On** (Iniciar sesión) en la esquina superior derecha del panel.

Sería posible iniciar una sesión en Credential Manager de cualquiera de las maneras siguientes:

- Asistente de sesión de inicio de Credential Manager (preferible)
- ProtectTools Security Manager

Nota Si utiliza el mensaje de inicio de sesión de Credential Manager, en la pantalla de inicio de sesión de Windows, para iniciar la sesión en Credential Manager, se inicia la sesión en Windows al mismo tiempo.

Acceso por primera vez

La primera vez que abra el Credential Manager, acceda con su contraseña de acceso a Windows habitual. Automáticamente, se crea una cuenta de Credential Manager con sus credenciales de acceso a Windows.

Después de entrar en Credential Manager, podrá registrar credenciales adicionales, como una huella digital o una Tarjeta Java.

En la siguiente conexión, podrá seleccionar la política de acceso y usar cualquier combinación de las credenciales registradas.

Nota Para obtener instrucciones específicas de ProtectTools Security Manager, consulte las pantallas de ayuda de ProtectTools.

5 HP Java Card Security for ProtectTools

Conceptos básicos

Java Card Security for ProtectTools gestiona la configuración de la Tarjeta Java en ordenadores equipados con un lector de Tarjeta Java opcional.

Con HP Java Card Security for ProtectTools, es posible:

- Acceder a las funciones de Java Card Security.
- Inicializar una Tarjeta Java, de manera que pueda utilizarse con otros módulos de ProtectTools, como Credential Manager for ProtectTools.
- Si fuera posible, trabaje con la utilidad Computer Setup para activar la autentificación de la Tarjeta Java en un entorno de pre-arranque, y para configurar Tarjetas Java separadas de administrador y de usuario. Para ello, se requiere que el usuario inserte la Tarjeta Java e introduzca, opcionalmente, un PIN antes de que el sistema empiece a cargarse.
- Si fuera posible, configure y cambie la contraseña empleada para autentificar a los usuarios de la Tarjeta Java.
- Si fuera posible, haga una copia de seguridad y restaure las contraseñas de Java Card BIOS almacenadas en la Tarjeta Java.
- Si es posible, guarde la contraseña del BIOS en la Tarjeta Java.

Nota Para obtener instrucciones específicas de ProtectTools Security Manager, consulte las pantallas de ayuda de ProtectTools.

6 Soluciones de terceros

Las plataformas que incluyen un TPM requieren tanto un TCG Software Stack (TSS) como un software de seguridad integrada. Todos los modelos se suministran con el TSS; el software de seguridad integrado debe adquirirse por separado en algunos modelos. Para esos modelos, se suministra un NTRU TSS para dar soporte a la compra de productos de terceros de software de seguridad integrado. Recomendamos soluciones de terceros como Wave Embassy Trust Suite.

7 HP Client Manager for Remote Deployment

Antecedentes

Las plataformas HP Trustworthy equipadas con un Trusted Platform Module (TPM) se suministran con el TPM desactivado (estado predeterminado). La activación del TPM es una opción administrativa protegida por las políticas obligatorias de HP BIOS. El administrador debe estar presente para entrar en las opciones de configuración de BIOS (opciones F10) y activar el TPM. Asimismo, las especificaciones del Trusted Computing Group (TCG) obligan a que se establezca presencia humana explícita (física) para activar un TPM. Esta obligación garantiza que se respetan los derechos de privacidad de un usuario (al proporcionar un modelo optativo de uso) y que el TPM no se desactiva a causa de una aplicación maliciosa, un virus o un caballo de Troya, para uso malintencionado. El establecimiento de presencia física y el requisito de la presencia local de un administrador plantea un desafío interesante para los gestores TI que tratan de desplegar esta tecnología en el conjunto de una gran empresa.

Configuración inicial

HP Client Manager (HPCM) proporciona un método remoto de activación del TPM y de toma de propiedad del TPM en el entorno de la empresa. Este método no requiere la presencia física del administrador TI, y sin embargo cumple con el requisito del TCG.

HPCM permite que el administrador TI configure ciertas opciones del BIOS y, a continuación, reinicia el sistema para activar el TPM en el sistema remoto. En el transcurso de este reinicio, el BIOS, de manera predeterminada, muestra una pantalla; para responder, el usuario final debe pulsar un tecla como prueba de presencia física, tal como lo especifica el TCG. El sistema remoto continuará con el reinicio, y se completa el script al tomar propiedad del TPM en el sistema. Durante este procedimiento, se crean un archivo de recuperación de emergencia y un token de recuperación de emergencia en la ubicación designada por el administrador TI.

HPCM no ejecuta la inicialización de usuario del TPM en el sistema remoto, ya que se debe permitir que el usuario elija la contraseña. La inicialización de usuario del TPM debe realizarla el usuario final de ese sistema.

Mantenimiento

El HP Client Manager puede utilizarse para restablecer la contraseña de usuario en modo remoto sin que el Administrador TI llegue a conocer la contraseña de usuario. HPCM puede incluso recuperar en modo remoto las credenciales de usuario. Deben suministrarse las contraseñas de administrador correspondientes para ambas funciones.

8 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, un símbolo de **!** en un triángulo amarillo aparece en Internet Explorer, 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.
No hay opción de **Browse for Virtual Token** (Examinar token virtual) 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.

Descripción breve	Detalles	Solución
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 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 usuario del dominio no tiene una cuenta física en el ordenador local, Credential Manager sólo puede cambiar la contraseña habitual de conexión.
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, entre 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) se salta la opción de elegir otro método de autentificación.	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), permitiendo que el sistema entre en S3	Si no se ha configurado una contraseña de administrador, el usuario no puede conectarse a Windows a través de Credential Manager, debido a las

Descripción breve	Detalles	Solución
	‘suspender’ y a continuación active el sistema, provoca que Credential Manager se conecte a Windows para abrirse.	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).
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.

Descripción breve	Detalles	Solución
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 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 flecha para seleccionar **Embedded Security Device—Disable** (Dispositivo de seguridad integrada – Desactivar). Utilice las teclas de flecha 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**	Cuando el usuario restaura la identidad, Credential Manager puede perder la	Esto sucede según el diseño actual.

Descripción breve	Detalles	Solución
(Restaurar identidad) pierde su asociación con el token virtual.	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.	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 se admite solamente en NTFS y no funciona en FAT32. Se trata de una función de EFS de Microsoft y no tiene relación con el software de 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	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 de “prácticas recomendadas” e instruir a los usuarios para

Descripción breve	Detalles	Solución
	eliminado, nadie podrá usar el software TPM.	que nunca cifren o eliminen los archivos del archivo de recuperación.
La interacción de HP ProtectTools Embedded Security EFS con Symantec Antivirus o Norton Antivirus da lugar a plazos de tiempo mayores en cifrado/descifrado y escaneado.	Los archivos cifrados interfieren con el escaneado de virus de Symantec 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.	Para reducir el tiempo necesario para escanear los archivos HP ProtectTools Embedded Security EFS, el 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 selección de **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), la selección **Encrypt** (Cifrar) aparecerá. Para solucionar el problema, cifre el archivo de la manera siguiente: haga doble clic 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: **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: **La seguridad integrada no se ha inicializado. Para utilizar el asistente, debe inicializarse antes la seguridad integrada.**	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** (Configurar) aparezca en pantalla (o tan pronto como 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**. 6. Configure la opción **Embedded Security Device** (Dispositivo de seguridad integrada) en **Enable** (Activar).

Descripción breve	Detalles	Solución
		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 salvar los cambios y salir de la utilidad de configuración de F10.
La contraseña de la utilidad Computer Setup (F10) puede eliminarse una vez que se haya activado el Módulo TPM.	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 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.	Así es como se ha diseñado. La contraseña de la utilidad Computer Setup (F10) sólo puede ser eliminada por un usuario que conozca la 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.

Descripción breve	Detalles	Solución
Errores intermitentes en el cifrado y descifrado tienen lugar: **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 esté presente, se muestra un mensaje de error avisando que **the device is not ready** (el dispositivo no está listo).
Durante la desinstalación, si el usuario no ha inicializado el usuario 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.	El usuario tiene la opción de desinstalar, bien sin desactivar el TPM, o desactivando primero el TPM (por medio de la herramienta Admin.), y desinstalando a continuación. El acceso a la herramienta Admin requier 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 la pantalla del cuadro de diálogo **Yes** (Sí) en **Click Yes to open Embedded Security Administration tool** (Haga clic en Sí para abrir la herramienta de administración de seguridad integrada), la desinstalación esperará a que se cierre la herramienta de 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.	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 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 autentificación de usuario EFS (se requiere contraseña) se interrumpe	La contraseña de autentificación de usuario EFS se vuelve a abrir después de hacer clic en **OK** (Aceptar) o de	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.

Descripción breve	Detalles	Solución
con **access denied** (acceso denegado).	retornar del estado en espera después de la interrupción.	
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.
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 **Yes** (Sí), la ubicación de SPEmRecToken aparecerá automáticamente en el cuadro de diálogo. Aunque esta ubicación sea correcta, se mostrará el mensaje de error siguiente:	Haga clic en el botón **Browse** (Examinar) de la pantalla para seleccionar la ubicación y los procedimientos del proceso de restauración.

Descripción breve	Detalles	Solución
	No se suministra token de recuperación de emergencia.. Seleccionar la ubicación del token; debe recuperarse el token de recuperación de emergencia	
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 hace algún intento de utilización del 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 seha configurado de nuevo para que utilice otra 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: **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.	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.
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: **El archivo de copias de seguridad seleccionado no coincide con el motivo de la restauración. Por favor seleccione otro archivo y continúe.**	Si el usuairo selecciona **SpSystemBackup.xml** cuando se requiera el SpBackupArchive.xml, el asistente de Embedded Security emitirá 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** (falló el 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.

Descripción breve	Detalles	Solución
		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. Si la copia automática de seguridad está programada para ocurrir después de la conexión, el icono de Embedded Security TNA muestra el siguiente mensaje: **La ubicación del archivo de copias 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 copias de seguridad esté de nuevo accesible.** 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.	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.
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 1.1B, 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 el 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 Broadcom-enabled TPMs —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 actualziación 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.** Aségurese 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. **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: Especificaciones TCG. Versión = 1.2 • Vendedor = Broadcom Corporation

Software impactado—Descripción breve	Detalles	Solución
		• 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 es un soporte descargable y disponible en http://www.hp.com.
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 usuairo 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 recomienta que el departamento TI del cliente siga buenas políticas de seguridad para desplegar su solución de seguridad y asegurarse de que la contraseña de administrador del BIOS es configurada por 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	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.

Software impactado—Descripción breve	Detalles	Solución
	que la autentificación de TPM BIOS funcione.	
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 de 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, **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.
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 operativoo 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 que se vuelvan a cifrar las claves de usuario básico desde una clave de propietario de plataforma a otra.

Autentificación Proceso de verificación de la autorización de un usuario para realizar una tarea, como por ejemplo acceder al ordenador, modificar la configuración de un programa determinado o ver datos seguros.

Autentificación de arranque Función de seguridad que requiere alguna forma de autentificación, como una Tarjeta Java, un chip de seguridad o una contraseña, cuando se enciende el ordenador.

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

Biométrico Categoría de credenciales de autentificación que utiliza una característica física, como una huella digital, para identificar a un usuario.

Certificado digital Credenciales electrónicas que confirman la identidad de un individuo o de una empresa, mediante la asociación de la identidad del propietario del certificado digital con un par de claves electrónicas que se utilizan para firmar la información digital.

Chip de seguridad integrada del Trusted Platform Module (TPM) (sólo en algunos modelos) Chip de seguridad integrada que permite proteger información de usuario sumamente sensible frente a atacantes malintencionados. Se trata de la “raíz de confianza” en una plataforma determinada. El TPM proporciona algoritmos y operaciones criptográficos que cumplen las especificaciones del Trusted Computing Group (TCG). El hardware y el software del TPM optimizan la seguridad del EFS y de la unidad segura personal al proteger las claves que utilizan. En sistemas sin TPM, las claves que utilizan el EFS y la PSD se almacenan normalmente en el disco duro. Lo que supone que las claves sean vulnerables potencialmente. En sistemas con la tarjeta TPM, las claves de origen del almacenamiento del TPM, que nunca abandonan el chip TPM, se utilizan para "envolver" o proteger las claves utilizadas por el EFS y la PSD. Irrumpir en el TPM para extraer las claves privadas es mucho más difícil que entrar ilegalmente en el disco duro del sistema para conseguir las claves. El TPM también potencia la seguridad del correo electrónico seguro a través de S/MIME en Microsoft Outlook y Outlook Express. El TPM funciona como un proveedor de servicios criptográficos (CSP). Las claves y certificados se generan y/o soportan por el hardware TPM, proporcionando una seguridad considerablemente mayor que las implementaciones únicamente de software.

Cifrado Procedimiento, como por ejemplo la utilización de un algoritmo, empleado en criptografía para convertir texto simple en texto cifrado para impedir que receptores no autorizados lean los datos. Existen numerosos tipos de cifrado de datos y son la base de la seguridad de red. Los tipos más comunes incluyen Data Encryption Standard (Estándar de cifrado de datos) y el cifrado de claves-públicas.

Contraseña del administrador de la Tarjeta Java Contraseña que asocia una Tarjeta Java de administrador con el ordenador en Computer Setup para la identificación durante el arranque o el reinicio. Esta contraseña puede ser configurada manualmente por el administrador o generarse al azar.

Contraseña de usuario de la Tarjeta Java Contraseña que asocia una Tarjeta Java de usuario con el ordenador en Computer Setup para la identificación durante el arranque o el reinicio. Esta contraseña puede ser configurada manualmente por el administrador o generarse al azar.

Credentiales Método mediante el cual un usuario muestra su autorización para realizar una tarea determinada en el proceso de autentificación.

Criptografía Práctica de cifrado y descifrado de datos, que sólo pueden ser descodificados por determinadas personas.

Cuenta de red Cuenta de usuario o de administrador de Windows, en un ordenador local, en un grupo de trabajo o en un dominio.

Cuenta de usuario de Windows Perfil de un individuo autorizado a conectarse a una red o a un ordenador individual.

Descifrado Procedimiento utilizado en criptografía para convertir datos cifrados en texto simple.

Dominio Grupo de ordenadores que forman parte de una red y que comparten una base de datos de directorios común. Los dominios tienen un nombre propio y cada dominio tiene un conjunto de reglas y procedimientos comunes.

Estándar avanzado de cifrado (AES) Técnica de cifrado simétrica de datos en bloques de 128 bits.

Estándares de cifrado de claves públicas (PKCS) Estándares generados que controlan la definición y la utilización de los medios de cifrado y descifrado de claves públicas/claves privadas.

Extensiones seguras multipropósito de correo Internet (S/MIME) Especificación para mensajería electrónica segura que utiliza PKCS. S/MIME ofrece autenticación a través de firmas digitales y privacidad a través del cifrado.

Firma digital Datos enviados con un archivo que verifica al remitente del material y que el archivo no haya sido modificado después de su firma.

Identidad En ProtectTools Credential Manager, significa un grupo de credenciales y configuraciones que se gestiona como una cuenta o perfil de un usuario particular.

Infraestructura de claves públicas (PKI) Término general que define la implementación de los sistemas de seguridad que utilizan el cifrado y descifrado de claves públicas/claves privadas.

Interfaz de Programación de Aplicaciones (API) Una serie de funciones del sistema operativo interno que pueden utilizar las aplicaciones para realizar diferentes tareas.

Interfaz LPC (Low Pin Count) Define una interfaz empleada por el dispostivio HP ProtectTools Embedded Security para conectarse con el conjunto de chips de la plataforma. El bus consiste en 4 bits de pins de Dirección/ Datos, junto con un reloj de 33Mhz y varios pins de control/estado.

Microsoft Cryptographic API, o CryptoAPI (MSCAPI) API de Microsoft que proporciona una interfaz al sistema operativo Windows para aplicaciones criptográficas.

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

Modo de seguridad del BIOS Configuración en Java Card Security for ProtectTools que, una vez activada, requiere el uso de una Tarjeta Java y un PIN válido para la autentificación de usuario.

Perfil del BIOS Grupo de parámetros de configuración del BIOS que se pueden guardar y aplicar a otras cuentas.

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

Reiniciar Proceso de reinicio del ordenador.

Seguridad rigurosa Función de seguridad en BIOS Configuration que proporciona una protección optimizada en contraseñas de arranque y de administrador, y en otras formas de autentificación de arranque.

Single Sign On Función que almacena datos de autentificación y permite utilizar Credential Manager para acceder a Internet y a las aplicaciones de Windows que requieran autentificación de contraseña.

Sistema de cifrado de datos (EFS) Sistema que cifra todos los archivos y subcarpetas dentro de una carpeta seleccionada. Un servicio transparente de cifrado de archivos proporcionado por Microsoft para Windows 2000 o posteriores

Tarjeta Java Componente pequeño de hardware, similar en el tamaño y la forma a una tarjeta de crédito, que almacena los datos de identificación del propietario. Se utiliza para autentificar al propietario de un ordenador.

TCG Software Stack (TSS) Proporciona servicios para optimizar la utilización del TPM, pero no requiere las mismas protecciones. Proporciona una interfaz de software estándar para tener acceso a las funciones del TPM. Para hacer pleno uso de las capacidades del TPM, como copia de seguridad de claves, autentificación y atestiguación de plataformas, las aplicaciones escriben directamente en el TSS.

Token USB Dispositivo de seguridad que almacena información de identificación de un usuario. Al igual que una Tarjeta Java o un lector biométrico, se utiliza para autentificar al propietario de un ordenador.

Token virtual Función de seguridad que funciona de manera similar a una Tarjeta Java y a un lector. El token se guarda en el disco duro del ordenador o en la base de registros de Windows. Cuando se conecta con un token virtual, se solicita un PIN de usuario para completar la autentificación.

Trusted Computing Group (TCG) Asociación empresarial establecida para promocionar el concepto de “Ordenador fiable”. TCG reemplaza a la TCPA

Trusted Computing Platform Alliance (TCPA) Asociación de empresas informáticas; reemplazada por el TCG

Unidad personal segura (PSD) Proporciona un área de almacenamiento protegida para datos sensibles. Una función facilitada por HP ProtectTools Embedded Security. Esta aplicación crea una unidad virtual en el ordenador del usuario que cifra automáticamente los archivos/carpetas que se desplazan a esta unidad virtual.

Índice