Guía HP ProtectTools Embedded Security

Número de Parte del Documento: 364876-161

Mayo de 2004

Esta guía proporciona instrucciones para el uso del software que le permite definir las configuraciones para el chip HP ProtectTools Embedded Security.

ADVERTENCIA: El texto presentado de esta forma indica que, si no se siguen las instrucciones, se pueden producir lesiones corporales o pérdida de la vida.

PRECAUCIÓN: El texto presentado de esta forma indica que, si no se siguen las instrucciones, se pueden producir daños en el equipo o pérdida de información.

Guía HP ProtectTools Embedded Security

Primera Edición: Mayo de 2004

Número de Parte del Documento: 364876-161

Contenido

Guía HP ProtectTools Embedded Security

Guía HP ProtectTools Embedded Security

El HP ProtectTools Embedded Security Manager es un software que permite ajustar la configuración del HP ProtectTools Embedded Security. El Administrador es una interfaz (shell) que señala las diversas opciones que están disponibles en el software Embedded Security. El HP ProtectTools Embedded Security es un conjunto de software que incluye, la Unidad de Seguridad Personal (PSD), interfaz de chip de encriptación/TPM, migración de seguridad, creación de archivos y control de contraseña.

Requerimientos

Para utilizar los recursos de seguridad se requieren las siguientes herramientas:

- Software HP ProtectTools Embedded Security
- Software HP ProtectTools Security Manager
- El chip HP ProtectTools Embedded Security instalado en su computadora.

Para obtener más informaciones sobre cómo configurar la solución Embedded Security, consulte "Procedimientos de Configuración" en la página 8 más adelante en este capítulo.

Conceptos Básicos sobre ProtectTools Embedded Security

Esta sección contiene información de alto nivel sobre conceptos que debe comprender para utilizar el HP ProtectTools Embedded Security Manager.

Chip HP ProtectTools Embedded Security

El chip Embedded Security es un componente de hardware que ofrece recursos de seguridad y encriptación además de proporcionar un área de almacenamiento a prueba de manipulación indebida para la protección de claves públicas y privadas. El chip viene instalado de fábrica y no se debe tocar ni remover excepto por los proveedores de servicio autorizado de HP.

Unidad de Seguridad Personal (PSD)

Un recurso de Embedded Security es la Unidad de Seguridad Personal (PSD). La PSD es una unidad virtual que se crea durante el proceso de inicialización del Usuario de HP ProtectTools Embedded Security. Provee una área de almacenamiento protegida para datos importantes. La PSD le permite crear y acceder carpetas y archivos, como cualquier otra unidad.

Acceso a la PSD requiere acceso físico a la computadora en la cual reside y su contraseña. La PSD se visualiza al ingresar la contraseña y los archivos se tornan disponibles para uso. Los archivos permanecen accesibles hasta que cierra la sesión, en ese momento la PSD se oculta automáticamente. La PDS no se puede acceder desde una red.

La PDS guarda las claves utilizadas para cifrar los archivos en el chip HP ProtectTools Embedded Security, asegurando que los datos estén protegidos contra usuarios no autorizados bloqueándolos en la computadora. Esto significa que sólo se puede acceder a los datos protegidos en su computadora.

Correo electrónico

La seguridad de los correos electrónicos es otro recurso importante de Embedded Security. Permite a los usuarios compartir información en forma confidencial y cerciorarse de que la autenticidad de ésta se mantenga durante la transferencia. El correo electrónico seguro le permite:

- Seleccionar un certificado de clave pública emitido por una Autoridad Certificadora (CA).
- Firmar mensajes digitalmente.
- Encriptar mensajes.

El HP ProtectTools Embedded Security y el HP ProtectTools Embedded Security Manager mejoran la funcionalidad de seguridad del correo electrónico al proporcionar protección adicional a la clave utilizada para cifrar, descifrar y firmar mensajes digitalmente. Mejoran la seguridad del correo electrónico cuando se usan los siguientes programas de correo electrónico:

- Microsoft Outlook Express (versión 4 o superior)
- Microsoft Outlook 2000
- Microsoft Outlook 2002
- Netscape Messenger 4.79
- Netscape Messenger 7.0

Para obtener más instrucciones sobre el uso de los programas de correo electrónico, consulte Ayuda de Integración para Correo Electrónico de HP ProtectTools Embedded Security.

Sistema de Encriptación de Archivos Mejorado (EFS)

El EFS es un servicio de encriptación de archivos ofrecido por Microsoft Windows 2000 y Windows XP Professional. El EFS proporciona privacidad de los datos al ofrecer las siguientes funcionalidades:

- Encriptación de archivos cuando el usuario los almacena en un disco
- Acceso fácil y rápido a los archivos encriptados
- Encriptación automática (y transparente) de datos
- Capacidad del administrador del sistema de recuperar datos encriptados por otro usuario

El HP ProtectTools Embedded Security y el HP ProtectTools Embedded Security Manager mejoran el EFS al proporcionar protección adicional a la clave utilizada para cifrar y descifrar datos.

Para obtener más informaciones sobre el EFS, consulte la Ayuda en línea del sistema operativo.

Usuarios y Administradores

Usuarios

Los usuarios tienen acceso básico a Embedded Security y pueden:

- enviar y recibir correos electrónicos encriptados
- encriptar archivos y carpetas
- inicializar la clave de Usuario Básico personal
- crear, eliminar o modificar las cuentas personales del usuario dentro de embedded security
- configurar, crear, utilizar y eliminar PSD individuales

Administradores

Los administradores inicializan la solución Embedded Security en una computadora y pueden:

- configurar el equipo local y los criterios de usuario de Embedded Security
- preparar las claves de usuario y los certificados para migración
- cambiar la contraseña de propietario de Embedded Security
- activar y desactivar Embedded Security
- autorizar computadoras de destino para migración de clave de usuario y certificados
- recuperar datos que se almacenaron y encriptaron usando Embedded Security

Para obtener más informaciones sobre usuarios y administradores de Embedded Security, consulte la Ayuda en línea del sistema operativo. Para obtener más informaciones sobre propietarios de Embedded Security, consulte Ayuda del HP ProtectTools Embedded Security Manager.

Certificados Digitales

Los certificados digitales son “claves” electrónicas que confirman la identidad de un individuo o empresa. Las claves son números o cadenas de caracteres conocidos sólo por el remitente y/o por el destinatario. Un certificado digital autentica el propietario al proporcionarle una firma digital que se adjunta al correo electrónico enviado por el propietario del certificado digital.

Un certificado digital es emitido por una Autoridad Certificadora (CA) que contiene la siguiente información:

- Clave pública del propietario
- Nombre del propietario
- Fecha de vencimiento del certificado digital
- Número de serie del certificado digital
- Nombre de la Autoridad Certificadora (CA) que emitió el certificado digital

- Firma digital de la Autoridad Certificadora (CA) que emitió el certificado digital

Firma Digital

Una firma digital muestra el nombre de la Autoridad Certificadora (CA) que emite el certificado digital. Se utiliza para:

- verificar la identidad del remitente de un documento digital.
- certificar que el contenido no fue modificado después de que el remitente ingresó su firma digital en el documento.

Para obtener más informaciones sobre las firmas digitales, consulte la Ayuda en línea del sistema operativo.

Claves Públicas y Privadas

La criptografía asimétrica, es un método usado por Embedded Security para encriptar información, requiere el uso de dos claves, una pública y una privada.

Una clave pública puede ser distribuida gratuitamente a muchos usuarios, mientras que una clave privada pertenece sólo a un usuario.

Por ejemplo, para enviar un correo electrónico encriptado, el Usuario A usa la clave pública (disponible gratuitamente) del Usuario B para encriptar el contenido del correo electrónico enviado por el Usuario B. Puesto que el Usuario B tiene la posesión única de su clave privada, él es el único que puede descifrar el contenido del correo electrónico enviado por el Usuario A.

La tecnología que habilita claves públicas le permite transmitir información privada a través de redes públicas, utilizar firmas digitales para asegurar la autenticidad del correo electrónico y proporciona autenticación entre un servidor y un cliente.

Recuperación de Emergencia

El Archivo de Recuperación de Emergencia, creado por el administrador durante la configuración de Embedded Security, es un archivo que almacena información importante sobre la computadora, sus usuarios y las claves privadas que se usan para proteger datos encriptados o personales. En caso de una falla del sistema, esta información importante es necesaria para recuperar el acceso a los datos protegidos.

Señal de Recuperación de Emergencia, también creada por el administrador durante la configuración de Embedded Security, es un archivo que almacena las claves utilizadas para proteger los datos en el Archivo de Recuperación de Emergencia. La señal es necesaria para acceder al archivo. El acceso a la Señal de Recuperación de Emergencia está protegida por una contraseña. Esta contraseña es necesaria en caso de que el sistema Embedded Security necesite restauración.

Criterios

Los criterios son normas que rigen el comportamiento de una computadora o software. Por lo general, el administrador del sistema especifica los criterios de seguridad para asegurar el uso consistente de Embedded Security en una organización. Existen dos tipos de criterios de seguridad: los criterios del equipo y los criterios de usuario.

Criterios del Equipo

Los criterios del equipo son normas que rigen el comportamiento integral de Embedded Security puesto que se refiere a una computadora específica.

Criterios de usuario

Los criterios de usuario son normas que rigen los derechos del usuario de Embedded Security.

Para obtener más informaciones sobre los criterios del equipo y de usuario, consulte la Ayuda del HP ProtectTools Embedded Security Manager.

Procedimientos de Configuración

Siga estas etapas para activar y inicializar el chip Embedded Security a través de la utilidad Computer Setup en el sistema de la BIOS:

PRECAUCIÓN: Para evitar un riesgo de seguridad, HP recomienda que una persona autorizada por la organización inicialice inmediatamente el chip Embedded Security (consulte la etapa 4). Falla en la inicialización del chip Embedded Security, puede resultar que un usuario no autorizado, un gusano computacional o un virus tome posesión del sistema.

Debido a que las configuraciones del chip se activan y modifican a través de Computer Setup, la contraseña del administrador de la BIOS debe ser establecida en Computer Setup antes de que las configuraciones del chip puedan ser accedidas.

Activación del Chip

1. Encienda o reinicie la computadora. Si está en Microsoft Windows, haga clic en **Inicio > Apagar > Reiniciar**.
2. Así que se encienda la computadora, presione y mantenga presionada la tecla **F10** hasta que ingrese Computer Setup Presione **Intro** para saltar la pantalla de título, si necesario.

Si no presiona la tecla **F10** en el momento correcto, debe reiniciar la computadora, presione nuevamente y mantenga presionada la tecla F10 para acceder la utilidad.

Si está utilizando un teclado PS/2, puede ser que vea un mensaje de Error de Teclado—no le preste atención.

3. Utilice la tecla de flecha arriba o abajo para seleccionar el lenguaje. Presione **Intro** para ingresar Computer Setup.

   Para obtener instrucciones de navegación, presione **F1**.

4. Use la tecla de flecha izquierda o derecha para seleccionar el menú **Seguridad**, luego use la tecla de flecha arriba o abajo para seleccionar **Configuración de Contraseña**. Presione **Intro**, ingrese y confirme una contraseña de configuración nueva y presione **F10** para aceptarla.

Escriba cuidadosamente; por motivos de seguridad, los caracteres que escribe no aparecen en pantalla.

5. En el menú **Seguridad** utilice la tecla de flecha arriba o abajo para seleccionar **Dispositivo Embedded Security**, luego presione **Intro**.
6. Si la selección del cuadro de diálogo es **Dispositivo Embedded Security—Desactivar**, utilice la tecla de flecha izquierda o derecha para cambiarlo a **Dispositivo Embedded Security—Activar**.
7. Presione **F10** para aceptar los cambios en la configuración de Embedded Security.
8. Para guardar sus preferencias y salir de Computer Setup, presione **F10** y después en **Guardar cambios y Salir**. Presione **Intro**, luego presione **F10** para confirmar.

Inicialización del Chip Embedded Security

En la mayoría de los casos, el Administrador del sistema de TI inicializa el chip Embedded Security.

1. Haga clic con el botón derecho en el icono **HP ProtectTools** en la bandeja del sistema y haga clic con el botón izquierdo en **Inicialización de Embedded Security** .

   El Asistente de Inicialización **HP ProtectTools Embedded Security** aparece.
2. Haga clic en **Siguiente**.
3. Escriba y confirme la contraseña de Asunción de Propiedad, luego haga clic en **Siguiente**.

Escriba cuidadosamente; por motivos de seguridad, los caracteres que escribe no aparecen en pantalla.

4. Haga clic en **Siguiente** para aceptar la ubicación predefinida del archivo de Recuperación.
5. Escriba y confirme la contraseña de Señal de Recuperación de Emergencia, luego haga clic en **Siguiente**.
6. Haga clic en **Buscar** y seleccione el destino apropiado.

PRECAUCIÓN: La Clave de la Señal de Recuperación de Emergencia es utilizada para recuperar datos encriptados si falla una computadora o el chip de Embedded Security. Es imposible recuperar los datos sin la clave. (Los datos aún no pueden ser accedidos sin la contraseña de Usuario Básico). Almacene esta Clave en un lugar seguro.

7. Haga clic en **Guardar** para aceptar la ubicación y el nombre de archivo predefinido, luego haga clic en **Siguiente**.
8. Haga clic en **Siguiente** para confirmar las configuraciones antes inicializar la Plataforma de Seguridad.

PRECAUCIÓN: Un mensaje puede ser exhibido, informando que los recursos de Embedded Security no fueron inicializadas. No haga clic en el mensaje; se abordará esto más adelante en el procedimiento y el mensaje se cerrará después de algunos segundos.

9. Si va a configurar la cuenta del usuario, certfíquese de que la casilla del **Asistente de Inicialización Original del Usuario Embedded Security** sea seleccionada. Haga clic en **Terminar**.

Configuración de una Cuenta de Usuario:

Configuración de una cuenta de usuario:

- crea una cuenta de Usuario Básico que protege los datos encriptados.
- configura una PSD para almacenar archivos y carpetas encriptadas.

PRECAUCIÓN: Proteja la contraseña de Usuario Básico. No se puede acceder ni recuperar a los datos encriptados sin esta contraseña.

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

1. Si el Asistente de Inicialización del Usuario **Embedded Security** no se abre, haga clic con el botón derecho en el icono **HP ProtectTools** en la bandeja del sistema y haga clic con el botón izquierdo en **Inicialización del Usuario Embedded Security** .

   El Asistente de Inicialización del Usuario **Embedded Security** aparece.

2. Haga clic en **Siguiente**.
3. Escriba y confirme una contraseña de Clave de Usuario Básico, luego haga clic en **Siguiente**.

Escriba cuidadosamente; por motivos de seguridad, los caracteres que escribe no aparecen en pantalla.

4. Haga clic en **Siguiente** para confirmar las configuraciones.
5. Seleccione los Recursos de Seguridad apropiados y haga clic en **Siguiente**.
6. Haga clic en **Siguiente** para saltar los archivos de Ayuda.
7. Si existe más de un Certificado de Encriptación, haga clic en el certificado apropiado.

   Haga clic en **Siguiente** para aplicar el Certificado de Encriptación.

8. Configure la PSD con las configuraciones apropiadas y haga clic en **Siguiente**.

9. Configure la PSD nuevamente con las configuraciones apropiadas y haga clic en **Siguiente**.

El tamaño mínimo de la PSD es de 50 MB; el tamaño máximo es de 2.000 MB.

10. Haga clic en **Siguiente** para confirmar las configuraciones.

Dependiendo del tamaño de la PSD, la computadora puede tomar algunos minutos para procesar la confirmación.

11. Haga clic en **Terminar**.
12. Haga clic en **Si** para reiniciar la computadora.

Tareas Comúnmente Realizadas

En esta sección se analizan las tareas básicas realizadas comúnmente por un usuario y un propietario.

Tareas del Usuario

Las tareas básicas del usuario incluyen la configuración de la PSD, encriptación de archivos y carpetas, envío y recibimiento de correo electrónico cifrado y/o firmas digitales.

Uso de la PSD

Para usar la PSD, ingrese la contraseña PSD. La PSD se torna visible y los archivos son descifrados. La PSD puede ser utilizada como cualquier otra unidad.

Cuando finalice de utilizar la PSD, cierre la sesión correctamente. La PSD se oculta automaticamente.

Encriptación de Archivos y Carpetas

Al utilizar el EFS en Windows 2000 and Windows XP Professional, considere las siguientes pautas:

- Sólo los archivos y las carpetas con partición NTFS se pueden cifrar. (Archivos y las carpetas con partición FAT no pueden ser cifrados.)
- Los archivos del sistema y los archivos comprimidos no se pueden cifrar.
- Carpetas temporales deben ser cifradas, pues los archivos temporales son blanco potencial de interés para posibles ataques de intrusos.
- Cuando los usuarios cifran un archivo o una carpeta por primera vez, se configuran automáticamente los criterios de recuperación. Esto garantiza a los usuarios que han perdido sus certificados y claves privadas tener la posibilidad de usar un agente de recuperación para descifrar sus datos.

Para cifrar archivos y carpetas:

1. Seleccione el archivo o carpeta que desea cifrar.
2. Haga clic con el botón derecho del mouse o Touchpad.
3. Haga clic en **Cifrar**.
4. Haga clic en **Aplicar cambios sólo en esta carpeta** o **Aplicar cambios en esta carpeta, subcarpeta y archivos**.
5. Haga clic en **Aceptar**.

Envío y Recibimiento de Correos Electrónicos Encriptados y/o con Firmas Digitales

Para obtener instrucciones sobre correo electrónico encriptado y firmas digitales, consulte Ayuda en línea para clientes de correo electrónico.

Para utilizar correo electrónico seguro, primero debe configurar el proveedor de correo electrónico para que use un certificado digital que se crea con Embedded Security. Si no dispone de un certificado digital, debe obtener uno de una Autoridad Certificadora (CA). Para obtener instrucciones sobre cómo configurar su correo electrónico y obtener un certificado digital, consulte la Ayuda en línea del cliente de correo electrónico.

Para enviar un mensaje de correo electrónico encriptado, necesita una copia de la clave pública o un certificado encriptado del destinatario. (El certificado contiene una copia de la clave pública del destinatario.)

Micosoft Windows XP Outlook usa la clave pública del destinatario para encriptar su correo electrónico; por lo que no es necesario que inserte su clave privada. Sin embargo, necesita su clave privada para leer un correo electrónico encriptado ya que el descifrado necesita de una clave privada que corresponda a la clave pública usada para encriptar el correo electrónico.

Tareas del Administrador

El administrador puede ejecutar diversas tareas, algunas de las cuales se describen a continuación. Para obtener más informaciones, consulte la Ayuda en línea de HP ProtectTools Embedded Security.

Migración de Claves a través del Asistente de Migración de Seguridad de la Computadora

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

El primer paso de una migración es la autorización, configuración y administración del proceso de migración. Una vez que se complete la autorización, el usuario exporta e importa claves y certificados desde la computadora de origen a la computadora de destino.

Para obtener más informaciones sobre migración, consulte la Ayuda en línea de HP ProtectTools Embedded Security.

Recuperación de Información

En el evento de falla en el chip o restauración:

- El Asistente de Restauración de Emergencia puede ser usado para recuperar datos de la PSD.
- La PSD también soporta recuperación de archivos con el uso de un agente de recuperación, mecanismo parecido al Sistema de Encriptación de Archivos (EFS).

  Para determinar si tiene un agente de recuperación registrado en la computadora, haga clic en **Inicio > Todos los Programas > Herramientas del Administrador > Criterios de Seguridad Local > Criterios de Claves Públicas > Agente de Recuperación de Datos Encriptados**.

Para obtener más informaciones, consulte la Ayuda en línea del sistema operativo.

Windows XP Professional no crea en forma automática un agente de recuperación registrado. Siga las instrucciones del sistema operativo para configurar el agente de recuperación registrado.

Para recuperar datos, el agente de recuperación registrado debe tener el certificado digital y las claves. Exporte el certificado de recuperación de datos y la clave privada al disco, almacénelas en un lugar seguro y elimine la clave privada de recuperación de datos de la computadora. La única persona que puede recuperar los datos es aquélla que tiene acceso físico a la clave privada de recuperación de datos.

Restauración del Chip Embedded Security a la configuración original de fábrica a través de Computer Setup.

PRECAUCIÓN: Esta tarea libera la propiedad del chip Embedded Security. Una vez que la propiedad es liberada, cualquier persona puede inicializar el chip Embedded Security.

Al restaurar el chip Embedded Security a su configuración original de fábrica puede ocasionar pérdida de datos si tiene archivos encriptados.

Para restaurar el chip Embedded Security a la configuración original de fábrica:

1. Encienda o reinicie la computadora. Si está en Microsoft Windows, haga clic en **Inicio > Apagar > Reiniciar**.
2. Así que se encienda la computadora, presione y mantenga presionada la tecla **F10** hasta que ingrese Computer Setup Presione **Intro** para saltar la pantalla de título, si necesario.

Si no presiona la tecla **F10** en el momento correcto, debe reiniciar la computadora, presione nuevamente y mantenga presionada la tecla F10 para acceder la utilidad.

Si está utilizando un teclado PS/2, puede ser que vea un mensaje de Error de Teclado—no le preste atención.

3. Si es necesario, ingrese la contraseña de configuración y presione **Intro**.

4. Utilice la tecla de flecha arriba o abajo para seleccionar el lenguaje. Presione **Intro** para ingresar Computer Setup.

   Para obtener instrucciones de navegación, presione **F1**.

5. Si no se ha configurado una contraseña de Seguridad, debe establecer una ahora. Use la tecla de flecha izquierda o derecha para seleccionar el menú **Seguridad**, luego use la tecla de flecha arriba o abajo para seleccionar **Configuración de Contraseña**. Presione **Intro**, ingrese y confirme una contraseña de configuración nueva y presione **F10** para aceptarla.

Escriba cuidadosamente; por motivos de seguridad, los caracteres que escribe no aparecen en pantalla.

6. En el menú **Seguridad** utilice la tecla de flecha arriba o abajo para seleccionar **Dispositivo Embedded Security**, luego presione **Intro**.

7. Use la tecla de flecha arriba o abajo para pasar a **Restaurar las Configuraciones de Fábrica—No Restaurar**. Presione *una vez* la tecla de flecha izquierda o derecha.

   Se exhibe un mensaje que informa: **La ejecución de esta acción borrará todas las claves de seguridad. Puede ocurrir pérdida de datos. Presione cualquier tecla para continuar.**

   Presione **Intro**.

8. Ahora, la selección presentará **Restaurar las Configuraciones de Fábrica—Restaurar**. Presione **F10** para confirmar el cambio.

9. Para guardar los cambios y salir de Computer Setup, presione **F10** y después en **Guardar cambios y Salir**. Presione **Intro**, luego presione **F10** para confirmar.

10. Encienda y apague la computadora.

Las preferencias son definidas cuando sale de Computer Setup y entran en vigencia cuando la computadora es apagada y encendida; no se recomienda un reinicio, pues no es eficaz.

Procedimientos Recomendados

HP recomienda seguir las siguientes pautas al usar Embedded Security.

- Un administrador de seguridad de TI debe configurar la contraseña del administrador de la BIOS en Computer Setup e inicializar el chip Embedded Security antes de distribuir computadoras a usuarios.
- El administrador de seguridad de TI debe configurar el Archivo de Recuperación de Emergencia durante el proceso de configuración de la solución Embedded Security e incentivar a los usuarios para que guarden y hagan copias de seguridad de los datos en forma regular. En caso de falla en el sistema, esta es la única manera de recuperar datos encriptados. El Archivo de Recuperación de Emergencia y la Señal de Recuperación de Emergencia deben ser almacenadas por separado.
- Encripte carpetas en vez de archivos individuales de modo que los archivos temporales que se crearon durante la edición también se encripten.
- Encripte datos importantes en computadoras que son miembros de un dominio. Esto protege los datos que sufren ataques de tipo criptográfico fuera de línea.
- Haga copias de seguridad de todo el servidor regularmente, que almacena los datos encriptados almacenados en el servidor. Esto garantiza que en el caso de recuperación de datos, los perfiles que incluyen claves de descifrado se puedan restaurar también.
- Si está encriptando tipos de archivos que son monitoreados por System Restore, coloque los archivos en un volumen que no sea monitoreado por éste.
- El sistema no admite niveles múltiples de encriptación. Por ejemplo, un usuario no debe almacenar un archivo encriptado EFS en la PSD, ni tratar de encriptar un archivo que ya se almacenó en la PSD.

Preguntas Más Frecuentes (FAQ)

¿Cómo averiguo si la computadora tiene un chip HP ProtectTools Embedded Security?

El chip es un componente de hardware incorporado en el sistema. El componente es listado en el Administrador de Dispositivos.

¿Dónde obtengo el software HP ProtectTools Embedded Security?

Descargue el software, controladores y Ayuda en línea visitando el sitio Web de HP en http://www.hp.com/products/security.

¿Se puede desinstalar el software HP ProtectTools Embedded Security? ¿Cómo?

Sí. El software se desinstala al usar el proceso de desinstalación estándar de software de Windows. Antes de la desinstalación, se deben guardar los datos específicos protegidos por el usuario. Si no se guardan los datos, éstos se perderán. El último paso de la desinstalación es desactivar el chip en la BIOS de la computadora a través de la utilidad Computer Setup. Una vez que HP ProtectTools Embedded Security es desinstalado, la única manera de desactivar el chip es a través de Computer Setup (**F10**).

1. Encienda o reinicie la computadora. Si está en Microsoft Windows, haga clic en **Inicio > Apagar > Reiniciar**.
2. Así que se encienda la computadora, presione y mantenga presionada la tecla **F10** hasta que ingrese Computer Setup Presione **Intro** para saltar la pantalla de título, si necesario.

Si no presiona la tecla **F10** en el momento correcto, debe reiniciar la computadora, presione nuevamente y mantenga presionada la tecla F10 para acceder la utilidad.

Si está utilizando un teclado PS/2, puede ser que vea un mensaje de Error de Teclado—no le preste atención.

---

3. Si es necesario, ingrese la contraseña de configuración y presione **Intro**.
4. Utilice la tecla de flecha arriba o abajo para seleccionar el lenguaje. Presione **Intro** para ingresar Computer Setup.

Para obtener instrucciones de navegación, presione **F1**.

5. Si no se ha configurado una contraseña de **S**eguridad, debe establecer una ahora. Use la tecla de flecha izquierda o derecha para seleccionar el menú **Seguridad**, luego use la tecla de flecha arriba o abajo para seleccionar **Configuración de Contraseña**. Presione **Intro**, ingrese y confirme una contraseña de configuración nueva y presione **F10** para aceptarla.

Escriba cuidadosamente; por motivos de seguridad, los caracteres que escribe no aparecen en pantalla.

6. En el menú **Seguridad** utilice la tecla de flecha arriba o abajo para seleccionar **Dispositivo Embedded Security**, luego presione **Intro**.
7. Si la selección del cuadro de diálogo es **Dispositivo Embedded Security—Activar**, utilice la tecla de flecha izquierda o derecha para cambiarlo a **Dispositivo Embedded Security—Desactivar**.
8. Presione **F10** para aceptar los cambios en la configuración Embedded Security.
9. Para guardar los cambios y salir de Computer Setup, presione **F10** y después en **Guardar Cambios y Salir**. Presione **Intro**, luego presione **F10** para confirmar.

Solución de Problemas

Embedded Security no funciona. ¿Qué debo hacer?

1. Haga clic con el botón derecho en el icono **HP ProtectTools** en la bandeja del sistema y haga clic con el botón izquierdo en **Administrar Embedded Security**.
2. Haga clic en **Embedded Security > Información > Auto Prueba**.

También verifique en **Estado de Embedded Security, Chip, Propietario** y **Usuario**.

Restauré mi sistema después de un cuelgue. Qué debo hacer ahora?

PRECAUCIÓN: En la mayoria de los casos, el administrador del sistema ejecuta este procedimiento. Pérdida permanente de datos puede resultar si el procedimiento no se ejecuta correctamente.

Para recuperar datos después de reemplazar el chip de ProtectTools, debe tener lo siguiente:

- SPEmRecToken.xml-la Clave de Señal de Recuperación de Emergencia
- SPEmRecArchive.xml-carpeta oculta, ubicación predefinida: C:\Documents and Settings\All Users\Application Data\Infineon\TPM Software\Recovery Archive
- Contraseñas de ProtectTools
  - F10 Setup
  - Asumir Propiedad
  - Señal de Recuperación de Emergencia
  - Usuario Básico

1. Encienda o reinicie la computadora. Si está en Microsoft Windows, haga clic en **Inicio > Apagar > Reiniciar**.
2. Así que se encienda la computadora, presione y mantenga presionada la tecla **F10** hasta que ingrese Computer Setup. Presione **Intro** para saltar la pantalla de título, si necesario.

Si no presiona la tecla **F10** en el momento correcto, debe reiniciar la computadora, presione nuevamente y mantenga presionada la tecla F10 para acceder la utilidad.

Si está utilizando un teclado PS/2, puede ser que vea un mensaje de Error de Teclado—no le preste atención.

3. Si es necesario, ingrese la contraseña de configuración y presione **Intro**.
4. Utilice la tecla de flecha arriba o abajo para seleccionar el lenguaje. Presione **Intro** para ingresar Computer Setup.

   Para obtener instrucciones de navegación, presione **F1**.
5. Si no se ha configurado una contraseña de Seguridad, debe establecer una ahora. Use la tecla de flecha izquierda o derecha para seleccionar el menú **Seguridad**, luego use la tecla de flecha arriba o abajo para seleccionar **Configuración de Contraseña**. Presione **Intro**, ingrese y confirme una contraseña de configuración nueva y presione **F10** para aceptarla.

Escriba cuidadosamente; por motivos de seguridad, los caracteres que escribe no aparecen en pantalla.

6. En el menú **Seguridad** utilice la tecla de flecha arriba o abajo para seleccionar **Dispositivo Embedded Security**, luego presione **Intro**.
7. Si sólo una selección, **Dispositivo Embedded Security–Desactivar**, está disponible, salte al paso 13.
8. Si dos selecciones están disponibles:
   a. Use la tecla de flecha arriba o abajo para pasar a **Restaurar las Configuraciones de Fábrica—No Restaurar**. Presione *una vez* la tecla de flecha izquierda o derecha.

      Se exhibe un mensaje que informa: **La ejecución de esta acción borrará todas las claves de seguridad. Puede ocurrir pérdida de datos. Presione cualquier tecla para continuar.**

b. Presione **Intro**.

Ahora, la selección presentará **Restaurar las Configuraciones de Fábrica–Restaurar**.

9. Presione **F10** para confirmar el cambio.
10. Para guardar los cambios, presione **F10** y después **Guardar Cambios y Salir**. Presione **Intro**, luego presione **F10** para confirmar.
11. Apague la computadora.

Alimentación debe ser desconectada para que el chip se restaure.

12. Salte al paso 1.
13. Si la selección del cuadro de diálogo es **Dispositivo Embedded Security—Desactivar**, utilice la tecla de flecha izquierda o derecha para cambiarlo a **Dispositivo Embedded Security—Activar**.
14. Presione **F10** para aceptar los cambios en la configuración Embedded Security.
15. Para guardar los cambios, presione **F10** y después **Guardar Cambios y Salir**. Presione **Intro**, luego presione **F10** para confirmar.
16. Después de abrir Windows, haga clic con el botón derecho en el icono **HP ProtectTools Embedded Security** en la bandeja del sistema y haga clic con el botón izquierdo en **Inicialización de Embedded Security**.
17. Seleccione la casilla de verificación: **Quiero restaurar el Embedded Security existente**, luego haga clic en **Siguiente**.
18. Escriba y confirme la contraseña de Asunción de Propiedad. Haga clic en **Siguiente**.
19. Haga clic en **No crear un archivo de recuperación**, luego haga clic en **Siguiente**.

PRECAUCIÓN: La creación de un archivo nuevo resulta en la pérdida total de datos al reemplazar el archivo requerido para esta restauración.

20. Haga clic en **Sí** para continuar sin crear un archivo de recuperación.
21. Haga clic en **Siguiente** para confirmar las configuraciones.
22. Haga clic en **Examinar** y ubique el archivo de emergencia; la ubicación predeterninada es: C:\Documents and Settings\ All Users\Application Data\Infineon\TPM Software\RecoveryArchive\SPEmRecArchive.xml.
23. Haga clic en **Abrir** y **Siguiente**.
24. Haga clic en **Examinar** y ubique la señal de Recuperación creada durante la Inicialización original de **HP ProtectTools Embedded Security**, haga clic en señal y luego haga clic en **Abrir**.
25. Ingrese la contraseña de Señal y haga clic en **Siguiente**.
26. Seleccione el nombre de la máquina y haga clic en **Siguiente**.
27. Haga clic en **Siguiente** para confirmar las configuraciones.

    Si aparece un mensaje informando que la restauración falló, regrese a la etapa 1. Verifique cuidadosamente las contraseñas, ubicación y nombre de la señal y nombre y ubicación del archivo.
28. Si va a configurar la cuenta del usuario, certfíquese de que la casilla de verificación del **Asistente de Inicialización del Usuario Embedded Security** sea seleccionada. Haga clic en **Terminar**.

Etapas 29 hasta 41 restauran las Claves Básicas de Usuario. Estas etapas deben ser repetidas para cada usuario.

29. Si el **Asistente de Inicialización del Usuario Embedded Security** no se abre, haga clic con el botón derecho en el icono **HP ProtectTools Embedded Security** en la bandeja del sistema y haga clic con el botón izquierdo en **Restaurar los Recursos Embedded Security**.

    El **Asistente de Inicialización del Usuario Embedded Security** aparece.
30. Haga clic en **Siguiente**.

31. Haga clic en **Recuperar la clave de usuario básico** y haga clic en **Siguiente**.
32. Selecione un usuario, escriba la contraseña de la Clave de Usuario Básico original y luego haga clic en **Siguiente**.
33. Haga clic en **Siguiente** para confirmar las configuraciones y aceptar la ubicación predefinida de los datos de recuperación.
34. Seleccione los Recursos de Seguridad apropiados y haga clic en **Siguiente**.
35. Haga clic en **Siguiente** para saltar los archivos de ayuda.
36. Si existe más de un Certificado de Encriptación, haga clic en el certificado apropiado.

    Haga clic en **Siguiente** para aplicar el Certificado de Encriptación.
37. Haga clic en **Quiero cambiar mis configuraciones de la Unidad de Seguridad Personal** cuando solicitado y haga clic en **Siguiente**.
38. Confirme los Recursos de Seguridad y haga clic en **Siguiente**.
39. Confirme las Configuraciones y haga clic en **Siguiente**.
40. Ingrese la contraseña de la PSD y haga clic en **Aceptar**.
41. Haga clic en **Terminar** y en **Sí** para reiniciar.

PRECAUCIÓN: Proteja la contraseña de Usuario Básico. No se puede acceder ni recuperar a los datos encriptados sin esta contraseña.

Glosario

Archivo de Recuperación de Emergencia—el archivo es un área de almacenamiento protegida que permite la re-encriptación de claves de usuario básico desde una plataforma de una clave de propietario a otra.

Autoridad certificadora (CA)—un servicio que emite los certificados que se necesitan para ejecutar una infraestructura de claves públicas.

Certificados Digitales—credenciales electrónicas que confirman la identidad de un individuo o una empresa al unir la identidad del propietario del certificado digital con un par de claves electrónicas que se usan para firmar información digital.

Criptografía—la práctica y el estudio de la encriptación y el descifrado; la codificación de datos de manera tal que puedan ser sólo decodificados por personas específicas. Un sistema de encriptación y descifrado de datos es un sistema criptográfico. A menudo implica un algoritmo combinado con los datos originales (“texto simple”) con una o más “claves”- números o serie de caracteres conocidos sólo por el remitente y/o el destinatario. El resultado final es conocido como “texto cifrado.”

Descifrado—todo procedimiento usado en criptografía para convertir un texto cifrado (datos encriptados) en un texto simple.

Encriptación—por ejemplo, algoritmos, criptografía; todo procedimiento utilizado en criptografía para convertir un texto simple en un texto cifrado y así prevenir que destinatarios no autorizados lean esos datos. Existen muchos tipos de encriptación de datos, éstos son la base de la seguridad en las redes. Los tipos más comunes incluyen Data Encryption Standard y encriptación de claves públicas.

Firma Digital—recursos utilizados para verificar la identidad del remitente de un documento digital y certificar que el contenido no fue modificado después de que el destinatario firmó el documento.

Infraestructura de Claves Públicas (PKI)—una norma que define las interfaces para crear, usar y administrar certificados y claves criptográficas.

Migración—una tarea que permite la administración, restauración y transferencia de claves y certificados.

Proveedor de Servicios Criptográficos (CSP)—un proveedor o biblioteca de algoritmos criptográficos que se puede utilizar en una interfaz bien definida para realizar funciones criptográficas específicas.

Sistema de Encriptación de Archivos (EFS)—un sistema que encripta todos los archivos y las subcarpetas dentro de una carpeta seleccionada.

Trusted Platform Module (TPM)—proporciona un nivel de seguridad de hardware para datos. Incorporado en el sistema, el chip Embedded Security puede verificar la integridad del sistema y autenticar a terceros que acceden a la plataforma mientras aún permanecen bajo el control total de su usuario principal.

Unidad de Seguridad Personal (PSD)—proporciona un área de almacenamiento protegida para datos importantes.