

La solución Infineon Security Platform



Bienvenido a la solución de Infineon Security Platform

La Solución Security Platform utiliza el Trusted Platform Module para asegurar sus datos y aplicaciones.

Para conocer más visite nuestro sitio Web en:

<http://www.infineon.com/tpm/software>



©Infineon Technologies AG

La Solución Infineon Security Platform

Introducción

El Software de la Solución Infineon Security Platform es un conjunto integral de herramientas que toma ventaja del Trusted Platform Module embebido en su sistema. Esta solución provee servicios para crear certificados digitales fácilmente por medio de Infineon Trusted Platform Module y para la administración de estos certificados. Estos certificados pueden utilizarse para:

- Enviar y recibir correo electrónico seguro desde clientes de correo como Microsoft Windows Mail/Outlook Express, Microsoft Outlook o Mozilla Thunderbird
- Configurar exploradores (por ejemplo, Mozilla Firefox o Internet Explorer) y servidores Web (como ser, Microsoft Internet Information Server) para la autenticación de clientes
- Firmar de los macros de Microsoft Word.
- Encriptar archivos y carpetas
- Conexiones seguras de red

Los datos secretos del usuario se pueden migrar a otras computadoras para proveer una seguridad completa en las computadoras adicionales.

El Software de la Solución Infineon Security Platform incluye los siguientes componentes:

- Herramienta de Configuración de Security Platform
- Asistente para la inicialización rápida de Security Platform
- Asistente para la inicialización de Security Platform
- Asistente para la inicialización de usuarios de Security Platform
- Asistente para la migración de Security Platform
- Asistente para la copia de seguridad de Security Platform
- Asistente para la restauración de Security Platform
- Asistente para la importación de Security Platform PKCS #12
- Visor de certificados de Security Platform y selección de certificados
- Icono de Notificación de la Barra de tareas de Security Platform

- Servicios de integración de Security Platform
- Servicios de Security Platform
- Server Integration Services
- Personal Secure Drive

Además de proveer información sobre la [instalación del software de la solución Infineon Security Platform](#), este documento lo ayudará a lograr un uso óptimo de su Infineon Trusted Platform Module y el software de la Solución Infineon Security Platform para llevar a cabo tareas como:

- [Obtención de certificados digitales](#)
- [Encriptación de archivos y carpetas](#)
- [Configuración de clientes de correo electrónico para el envío de correo electrónico encriptado y firmado digitalmente](#)

Además, este documento servirá de ayuda para los administradores de empresas que deban realizar tareas como:

- [Mapeo de certificados con Internet Information Server y Active Directory](#)
- [Autenticación de clientes con Internet Explorer, autenticación de clientes con Mozilla Firefox](#)
- [Uso de certificados digitales para firmar macros electrónicamente en Microsoft Word](#)

Una tarea muy importante a llevar a cabo es la administración de la funcionalidad de la [copia de seguridad y recuperación de emergencia](#). Esta característica se maneja durante la inicialización de Security Platform y no afecta a las características de seguridad generales que se listaron más arriba. Este proceso es importante para evitar la pérdida de datos en caso de una falla de la computadora.



©Infineon

La Solución Infineon Security Platform

Ventajas de la utilización de Trusted Platform Module

El espectacular crecimiento de Internet y la tendencia de las redes corporativas a expandirse para permitir el acceso a los clientes y a los proveedores desde fuera del servidor de seguridad corporativo, ha dado una mayor importancia a la cuestión de la seguridad. Incluso a medida que se va generalizando el uso de formas de identificación electrónica en lugar de la identificación cara a cara y en formato papel, la seguridad y la privacidad se han convertido en motivos de gran preocupación. Sin embargo, parece que estas cuestiones se han resuelto con las aplicaciones basadas en la utilización de claves públicas. Algunos ejemplos de tipos de servicios que ofrece la tecnología de clave pública son la transmisión segura de la información mediante redes públicas, la firma digital para garantizar la autenticidad del correo electrónico y la autenticación de servidor a cliente y viceversa.

La comunicación en Internet crece continuamente. Muchas aplicaciones, como por ejemplo las que están destinadas al comercio electrónico, se basan en la confianza en el interlocutor y en la fiabilidad de la conexión. Es preciso ofrecer autenticidad, integridad, confidencialidad y privacidad. Con el desarrollo de [**TCG \(Trusted Computing Group\)**](#), se ha puesto en marcha una iniciativa empresarial eficaz. Su objetivo es aumentar la confianza en la seguridad de Internet. TCG ha definido un dispositivo, conocido como **Trusted Platform Module** (TPM, chip de seguridad), que asume la responsabilidad de un gran número de funciones de seguridad importantes.

El chip de seguridad constituye la base de la confianza en una plataforma determinada (por ejemplo, en equipos portátiles o de escritorio). Si el chip está integrado en un equipo que ejecuta un sistema operativo que lo detecta, el chip puede comprobar la integridad del sistema y autenticar usuarios de otros equipos que deseen acceder a las características de seguridad; en todo caso, el chip queda completamente bajo el control de su usuario principal. De este modo, la privacidad y la confidencialidad quedan garantizadas. Con las plataformas basadas en el chip de seguridad, por primera vez se podrá crear la base para una infraestructura de clave pública de ámbito internacional (PKI). Esto, a su vez, garantizará la seguridad de muchas aplicaciones para entornos privados y empresariales en particular, al mismo tiempo que se crean otros tipos de aplicaciones nuevas.

Las actividades de TCG y el nivel de seguridad resultante son muestra de las necesidades de la tecnología de seguridad de hoy en día. La arquitectura de

Infineon Trusted Platform Module está diseñada para ofrecer los niveles de seguridad más elevados de que se dispone actualmente, basados en una tecnología de seguridad verificada, y una fácil integración en el sistema proporcionando una solución de seguridad completa. Infineon Trusted Platform Module ofrece las implementaciones de cifrado de RSA y algoritmos hash (SHA-1 y MD-5) para obtener el mejor rendimiento posible, además de un generador de números aleatorios verdaderos (TRNG). Se trata de un dispositivo blindado que cuenta con los máximos niveles de seguridad para el análisis simple de potencia (SPA) y el análisis diferencial de potencia (DPA).

Hasta hace poco, los usuarios de equipos solían almacenar sus claves privadas y certificados en las unidades de disco duro de sus equipos; de este modo, la información quedaba expuesta a intrusos y a personas que podían acceder físicamente a la máquina. En cambio, Trusted Platform Module ofrece un medio de almacenamiento a prueba de falsificaciones para proteger la información.



Technologies AG

Solución Infineon Security Platform

Microsoft Windows

En esta página se ofrece información específica para las distintas versiones del sistema operativo Microsoft Windows.

Control de la cuenta del usuario

El control de la cuenta del usuario es una función importante que ofrece Windows Vista y versiones posteriores. Con el control de la cuenta del usuario, los administradores de sistemas pueden ejecutar la mayoría de las aplicaciones, componentes y procesos con un privilegio limitado, pero contando con "potencial de elevación" para tareas administrativas específicas y funciones de la aplicación. Cuando los usuarios comunes invoquen una tarea del sistema que requiera privilegios administrativos, como intentar instalar una aplicación, Windows notificará al usuario y requerirá la autorización del administrador, es decir, nombre de usuario y contraseña de una cuenta con privilegios administrativos, para completar la tarea. Además, el control de la cuenta del usuario hace que incluso las cuentas de los administradores funcionen como cuentas comunes la mayor parte del tiempo y en caso de que se intente una tarea a nivel administrativo, el administrador recibirá un pedido para elevar sus privilegios momentáneamente para poder completar sólo esa tarea en particular.

Windows usa un icono de escudo  para indicar que esa función en particular requiere de privilegios administrativos para realizar la tarea (p ej. para la restauración de Security Platform mediante el [Asistente para la inicialización de Infineon Security Platform](#)).



- En Windows 7, el icono de escudo no se encuentra siempre visible de forma predeterminada, sino únicamente después de una correcta configuración.
- El icono de escudo puede tener un aspecto ligeramente distinto en función de la versión de Windows.

Microsoft BitLocker

[BitLocker](#) de Microsoft, que se incorpora a algunas ediciones de Windows Vista y posteriores, se puede utilizar para cifrar un disco duro entero, lo que dificulta que alguien tenga acceso a los datos del equipo en caso de pérdida o robo. El cifrado de unidad BitLocker con o sin Trusted Platform Module provee la encriptación total del disco. Trusted Platform Module hace que la encriptación del disco sea incluso más segura ya que utiliza el chip para generar claves criptográficas basadas en los escaneos de los archivos de sistema principales, además de una clave para el disco duro en sí. Para configurar esta función vea el [Asistente para la inicialización de Infineon Security Platform](#) y [Herramienta de configuración de Infineon Security Platform](#).

Administración del Módulo de plataforma segura (TPM)

La aplicación *Administración del Módulo de plataforma segura (TPM)* de Microsoft es una opción que ofrece Windows Vista y versiones posteriores. Consúltela desde Microsoft TechNet. Existe información más detallada en Microsoft TechNet. Consúltela desde Microsoft TechNet.

Errores

Si ocurren errores TPM o TSS no esperados bajo Windows Vista o sistemas operativos posteriores, verifique si los comandos TPM no están bloqueados mediante las configuraciones de Windows Group Policy (Política de grupo de Windows).



©Infineon

Technologies AG

La solución Infineon Security Platform - Modos de funcionamiento

Modos de funcionamiento

Modo Servidor

En modo servidor, Server Integration Services integran al Security Platform en un Trust domain con gestión centralizada.

 Hay información más detallada sobre el modo servidor en la *guía técnica* para *Trusted Computing Management Server*.

Precondiciones para la inscripción de plataformas y de usuarios en el modo servidor

	Explicación
Inscripción de la Plataforma	<p>La inscripción de la plataforma se realiza automáticamente sin ninguna interacción con el usuario.</p> <p>Las precondiciones son:</p> <ul style="list-style-type: none">• La plataforma Trust Domain es miembro del grupo de inscripción de plataformas (Para más detalles vea la <i>Guía Técnica</i> para <i>Trusted Computing Management Server</i>).• Trusted Platform Module está habilitado y activado.• Trusted Platform Module no ha sido inicializado aun (ni por Infineon TPM Professional Package en modo Aislado ni por Trusted Domain Server en modo servidor, ni tampoco por ningún otro Software como <i>Trusted Platform Module (TPM) Management</i>) de Windows.• La plataforma Trust Domain está en línea, es decir que tiene una conexión de red con el servidor Trust Domain.
Inscripción de Usuarios	<p>La inscripción de usuarios se realiza de manera interactiva como en el modo stand-alone, si se cumplen las siguientes precondiciones:</p> <p>Las precondiciones son:</p> <ul style="list-style-type: none">• El usuario Trust Domain es miembro del grupo de inscripción de usuarios (Para más detalles vea la <i>Guía Técnica</i> para <i>Trusted Computing Management Server</i>).• Trusted Platform Module está habilitada y activada en la plataforma del usuario.

- La plataforma Trust Domain está en línea, es decir que tiene una conexión de red con el servidor Trust Domain.
- El usuario se ha conectado al dominio.

Modo aislado

En el modo independiente, el Security Platform no está integrado en un Trust Domain con gestión centralizada.

Diferencias entre los modos de funcionamiento:

La siguiente tabla enumera los comportamientos de los distintos componente de la interfaz del usuario en los modos de funcionamiento:

Componente	Modo aislado	Modo Servidor
Herramienta de configuración	Este componente es designado como un applet en el panel de control. Los administradores y usuarios pueden realizar tareas de inicialización y configuración de Security Platform Funciones y administración de todas las funcionalidades de Security Platform.	La configuración de todas las opciones del propietario de Security Platform y las configuraciones de autenticación son administradas por el Trusted Computing Management Server. Las páginas Avanzado y Migración no están disponibles.
Asistente de inicialización rápida	Combina inicialización de usuario y de plataforma con las configuraciones predeterminadas (recomendado para la mayoría de los usuarios).	Las tareas específicas de la plataforma se pasan por alto, ya que el Trust Computing Management Server se encarga de las mismas.
Asistente para la inicialización	Inicialización, habilitación y restauración de las funciones de Security Platform (pasos administrativos). Este asistente es totalmente funcional en este modo.	La inicialización, la habilitación y la restauración ocurren automáticamente una vez que el sistema cliente está integrado a un Trust Domain con gestión centralizada, es decir, el administrador no tiene que realizar esta tarea. El asistente de Security Platform no funciona si la plataforma es miembro del

		grupo de inscripción de plataforma.
Asistente para la inicialización de usuario	El asistente para la inicialización de usuarios soporta la inicialización de usuarios al Security Platform y la configuración de las funciones del Security Platform . Este asistente es totalmente funcional en este modo.	La inicialización de usuarios es posible sólo si el usuario actual es miembro del grupo de inscripción de usuarios especificado en el Trusted Computing Management Server. Este asistente también es totalmente funcional en este modo.
Asistente para la migración	La migración de certificados y claves específicas del usuario desde una plataforma de origen a una de destino involucra pasos administrativos y de usuario. Este asistente es totalmente funcional en este modo.	Este asistente no es funcional ya que la migración de los certificados y claves específicas del usuario es realizada por el Trusted Computing Management Server, es decir que el administrador y el usuario no tienen que realizar esta tarea.
Asistente para la copia de seguridad	Las restauraciones y copias de seguridad manuales y automáticas involucran pasos administrativos y de usuario. Asimismo, si se ha configurado el Personal Secure Drive (PSD) se podrán realizar restauraciones y copias de seguridad manuales de esta unidad.	Las tareas de copia de seguridad y restauración son realizadas por Server Integration Services. Si se ha configurado un Personal Secure Drive (PSD) se podrán realizar restauraciones y copias de seguridad manuales de esta unidad.
Asistente para el restablecimiento	La reconfiguración de la contraseña de usuario	El Trusted Computing Management Server se

<p>de la contraseña</p>	<p>básico involucra pasos de usuario y administrativos. El administrador prepara la reconfiguración de la contraseña para un usuario y le provee de un código de autorización para la reconfiguración de la contraseña. El usuario procede luego a reconfigurar su contraseña de usuario básico.</p>	<p>encarga de preparar y proveer los códigos de autorización para la reconfiguración de las contraseñas para el usuario y administrador específicos. Existe una opción adicional para obtener del servidor el código de autorización para la reconfiguración.</p>
<p>Asistente para la importación PKCS #12</p>	<p>Este asistente se utiliza para importar los archivos de Personal Information Exchange al Security Platform y es totalmente funcional en este modo.</p>	<p>No se observan cambios en el comportamiento de este asistente y también es totalmente funcional en este modo.</p>
<p>Icono de Notificación de la Barra de tareas</p>	<p>Realizar tareas administrativas de Security Platform y obtener información sobre el estado. Esta aplicación es totalmente funcional en este modo.</p>	<p>Las tareas que realiza el servidor sin la interacción del usuario no se encuentran disponibles en este modo.</p>



La Solución Infineon Security Platform

Instalarlo el Security Platform Solution Software

En caso de que ya exista una versión instalada del Software de la Solución de Infineon Security Platform en su sistema, no hay necesidad de desinstalar este software. Cualquier instalación preexistente puede sobrescribirse en una operación de un solo paso.



Actualización: La actualización de versiones de productos anteriores está detallada en *ReadmeUpgrade.txt*.

1. Ejecute el programa de instalación.

Nota: Si el Software de Infineon Security Platform ya se encuentra instalado en su sistema, se abrirá un cuadro de diálogo donde podrá elegir modificar, reparar, o quitar la instalación existente.

2. Comienza el asistente InstallShield y se muestra la versión del Software de la Solución de Infineon Security Platform junto con información legal.
3. Haga clic en el botón **Siguiente** para proceder con el proceso de instalación. Obtendrá el acuerdo de licencia de usuario final (EULA por sus siglas en inglés).
4. Lea atentamente el EULA. Acepte los términos del acuerdo de licencia. Haga clic en el botón **Siguiente** para proceder con el proceso de instalación.
5. Luego, deberá proveer cierta información para la instalación. Ingrese información personal y de su organización en las casillas de texto correspondientes.
6. Haga clic en el botón **Siguiente** para proceder con el proceso de instalación.
7. En la **ventana de Tipo de configuración**, seleccione el tipo de configuración deseado:
 - Seleccione **Completo** si desea instalar todos los componentes al directorio de instalación predeterminado.
 - De lo contrario seleccione **Personalizado**.
8. Seleccione los componentes que desea instalar. Puede leer la descripción de cada componente del lado derecho de la pantalla y decidir si lo instala en su sistema en ese momento, más adelante, o si no lo instala en absoluto.

Algunos componentes son obligatorios y no se pueden destildar. También puede seleccionar el directorio en el cual desea instalar el Software de la Solución Infineon Security Platform.

9. Haga clic en el botón **Siguiente** para proceder con el proceso de instalación.
10. Haga clic en el botón **Siguiente** para continuar con el proceso de instalación.
11. El asistente InstallShield instala el software de la Solución Infineon Security Platform.

El programa de instalación instala los siguientes componentes en su sistema, dependiendo de su selección:

- Herramienta de configuración de Security Platform
 - Asistente para la inicialización rápida de Security Platform
 - Asistente para la inicialización de Security Platform
 - Asistente para la inicialización de usuarios de Security Platform
 - Asistente para la migración de Security Platform
 - Asistente para la copia de seguridad de Security Platform
 - Asistente para el restablecimiento de la contraseña de Security Platform
 - Asistente para la importación de Security Platform PKCS #12
 - Visor de certificados y selección de certificados de Security Platform
 - Icono de Notificación de la Barra de tareas de Security Platform
 - Personal Secure Drive
 - Infineon TPM Cryptographic Service Providers
 - Security Platform Software Stack
 - Software del controlador del dispositivo Trusted Platform Module
 - Server Integration Services
12. La instalación de Infineon Security Platform Software.
 13. Seleccione **Preparar inscripción de TPM** para [habilitar](#) el Trusted Platform Module si así lo desea (sólo en sistemas con Trusted Platform Module deshabilitado y soporte de Interfaz de presencia física). De este modo se podrá inicializar la plataforma más tarde sin tener que reiniciar nuevamente el sistema.
 14. Seleccione la opción **Mostrar el archivo Readme**, si lo desea.
 15. Haga clic en **Finalizar** para completar la instalación.



TPM

©Infineon Technologies AG

La solución Infineon Security Platform

Configuración y administración de Infineon Security Platform

Cuando se entrega Infineon Security Platform al cliente, su estado inicial es, de forma predeterminada, el de deshabilitado. Esto garantiza que no se transfiera información confidencial de Infineon Security Platform al fabricante de la plataforma durante esta fase, ya que no hay ningún tipo de información secreta compartida.

El estado actual de Infineon Security Platform nunca se ve afectado por la instalación de la solución de software Infineon Security Platform.

Para poder utilizar Infineon Security Platform, antes debe realizar lo siguiente:

- Habilitar Infineon Security Platform de acuerdo con el procedimiento indicado en la documentación de Infineon Security Platform:
- Configure Infineon Security Platform y Usuario iniciando el Asistente para la inicialización rápida



En el [modo servidor](#), Security Platform se inicializa automáticamente si el sistema cliente está integrado a un Trust Domain con gestión centralizada, es decir, el administrador no tiene que realizar esta tarea.

Consulte [Herramientas de Infineon Security Platform Solution](#) para obtener información detallada sobre los asistentes y las herramientas administrativas.

Si ha configurado Infineon Security Platform y un usuario de Infineon Security Platform, ya está listo para [obtener un certificado basado en Trusted Platform Module](#).

Las operaciones que pueden realizarse se controlan mediante el estado actual de Infineon Security Platform. En la [información general sobre estados](#) se enumeran los valores de estado posibles.

En la sección de [preguntas más frecuentes](#) encontrará las respuestas a las preguntas más habituales relativas a la gestión de Security Platform.



©Infineon Technologies AG

La Solución Infineon Security Platform

Roles del usuario

La Solución Security Platform involucra varios roles del usuario:

- Todos los roles del Usuario de Security Platform están basados en cuentas de usuario de Windows (usuarios locales o de dominio). Estas cuentas de usuario se autentificaron en el inicio de sesión de Windows.
- Cada rol del usuario tiene un propósito.
- Al configurar el Security Platform, se inicializan los miembros de los diferentes roles del usuario.
- Un rol del usuario específico requiere una autenticación específica (por ejemplo, suministrar una contraseña específica).
- Una persona puede tomar diversos roles del usuario.

La tabla a continuación muestra todos los roles del usuario.

Rol del usuario	Basado en...	Propósito & Tareas	Inicialización	Autentificación
Propietario de Security Platform	Cuenta de usuario de Windows (local o de dominio), miembro del grupo de Administración	Realizar tareas administrativas críticas, por ejemplo, la restauración de Security Platform.	La inicialización de Security Platform habilita a un usuario de Windows para que actúe como Propietario de Security Platform.	Contraseña propietaria
Administrador de Security Platform (también llamado simplemente "Administrador")	Cuenta de usuario de Windows (local o de dominio), miembro del grupo de Administración	Realizar tareas administrativas, las cuales requieren de derechos de administración de Windows.	No se necesita una inicialización especial.	Además de autenticación como administrador de Windows algunas tareas administrativas requieren

				acceso a archivos o tarjetas de seguridad especiales se encuentran protegido: contraseñas independientes
Usuario de Security Platform (también llamado simplemente "Usuario")	Cuenta de usuario de Windows (local o de dominio)	Utilizar las características de Security Platform, por ejemplo, la encriptación de archivos y carpetas o correo electrónico seguro. Configurar las características y realizar tareas de Security Platform específicas del usuario.	La inicialización de Security Platform habilita a un usuario de Windows para que actúe como Usuario de Security Platform.	Contraseña de usuario básica
Agente de recuperación EFS/PSD (también llamado simplemente "Usuario")	Utilización de una clave privada y un certificado de recuperación dedicados.	Recuperar los datos EFS o PSD de un usuario en caso de que se pierdan las credenciales originales EFS/PSD.	La recuperación de EFS/PSD se habilita por medio del registro de los agentes de recuperación.	Clave privada del agente de recuperación



TPM
©Infineon Technologies AG

La Solución Infineon Security Platform

Autenticación de usuarios

Por cuestiones de seguridad, necesitará autenticarse al Infineon Security Platform antes de poder utilizar las funciones de seguridad. Por ejemplo, la encriptación de archivos requiere de su clave de usuario básico, la cual a su vez está protegida por su contraseña de usuario básico. Al ingresar esta contraseña se estará autenticando en el Security Platform. Sólo puede utilizar su clave de usuario básico luego de lograda la autenticación.

La Solución de Infineon Security Platform provee dos niveles de autenticación para proteger su clave de usuario básico:

Autenticación de contraseña

La clave de usuario básico se encuentra protegida con la *Contraseña de usuario básico*. Esta contraseña se debe ingresar manualmente.

Autenticación mejorada

La clave de usuario básico se encuentra protegida con la *Contraseña de usuario básico*. Esta frase de contraseña se almacena en forma segura por medio de un dispositivo de autenticación, como ser una tarjeta inteligente, una tarjeta de seguridad USB, un lector de huellas digitales u otro dispositivo de medición biométrica. Sólo se puede acceder a la frase de contraseña mediante este dispositivo de autenticación, por ejemplo al insertar una tarjeta inteligente e ingresar su PIN, o al colocar el dedo en el lector de huellas digitales.

Contraseñas y frase de contraseña

En el caso de **Autenticación de contraseña** las contraseñas "normales" sirven como contraseñas de usuario básico. aunque técnicamente es posible utilizar contraseñas largas y complejas, la mayoría son bastante cortas, ya que deben memorizarse.

Por el contrario con la **Autenticación mejorada** no hay necesidad de memorizar contraseñas, ya que se administran por medio del dispositivo de autenticación. Desde el punto de vista del usuario, la contraseña se reemplaza por un PIN o por una autenticación biométrica. De manera que el uso de la autenticación mejorada es más fácil. Por otro lado, gracias a las funciones de seguridad incorporadas en el dispositivo de autenticación, el nivel de seguridad es considerablemente mayor. Por ejemplo, una tarjeta inteligente tiene un contador de reintentos que bloquea la tarjeta luego de varias entradas erróneas del PIN. De esta manera los ataques por fuerza bruta son imposibles y se pueden utilizar PINs relativamente simples.

Una frase de contraseña es básicamente una *contraseña* larga y compleja. De *Frase de contraseña*. Una frase de contraseña es básicamente una contraseña larga y compleja.

La Solución Security Platform diferencia a estos términos de la siguiente manera:

- **Contraseña** se utiliza en el modo de autenticación de contraseña y representa la *Contraseña de usuario basico*.
- **Frase de contraseña** se utiliza en el modo de autenticación mejorada. También representa a una contraseña de usuario básico. La contraseña de usuario básico se llama *Frase de contraseña de usuario básico* en este contexto

Instalación y administración de la autenticación mejorada

Los dispositivos de autenticación se suministran como plug-ins de software instalables separados. El software de la Solución Security Platform detecta automáticamente los dispositivos de autenticación instalados.

La configuración de los dispositivos de autenticación es específica para cada usuario, es decir que diferentes usuarios de Security Platform pueden utilizar dispositivos de autenticación diferentes. El uso de la autenticación mejorada se puede controlar por medio de [políticas](#).

Configuración de la autenticación mejorada - Tareas administrativas

Configuración de la autenticación mejorada - Tareas administrativas	Componentes de software a utilizar
1. Dispositivo de autenticación	Instalación por separado. Consulte con su proveedor del plug-in del dispositivo de autenticación.
2. Habilite el uso de ciertos dispositivos de autenticación para todos los usuarios.	Si Security Platform aún no se encuentra inicializado: Asistente para la inicialización El Security Platform ya se encuentra inicializado. Herramienta de configuración - Avanzada - Configurar...
Configuración de la autenticación mejorada - Tarea del usuario	Componentes de software a utilizar
3. Seleccione el nivel de autenticación y el dispositivo para el usuario actual de Security Platform.	Si Security Platform aún no se encuentra inicializado: Asistente para la inicialización de usuario El usuario ya se encuentra inicializado. Herramienta de configuración - Configuraciones del usuario - Configurar...

La Solución Infineon Security Platform

Tarjetas de seguridad, archivos comprimidos y otros archivos de administración de Security Platform

La Solución Infineon Security Platform utiliza varios archivos para tareas de administración tales como las copias de seguridad, recuperaciones de emergencia o restablecimiento de las contraseñas (por ejemplo, tarjetas de seguridad y paquetes de archivos). Algunos de ellos son para los administradores de Security Platform, y otros para los usuarios. Asegúrese de no mezclar estos tipos de archivos.

La tabla a continuación brinda una introducción a los archivos de administración de Security Platform.

Archivo	Utilizado por...	Objetivo/Explicación
Archivo de copia de seguridad de la contraseña de propietario	Administrador	Utilizado para la autenticación de la contraseña de propietario (en vez de escribir la contraseña de propietario). Este archivo es compatible con el Archivo de copia de seguridad de la contraseña de propietario generado por la aplicación "Trusted Platform Module (TPM) Management".  No se requiere este archivo en el modo servidor ya que el Trusted Computing Management Server se encarga de la tarea de preparar y proveer esta contraseña.
Paquete de archivos que se utilizan para la restauración, recuperación de emergencia y restablecimiento de	Administrador/Usuario	Contienen credenciales y la configuración de Security Platform y las copias de seguridad de Personal Secure Drive. Creados por las copias de seguridad automáticas y

las contraseñas		<p>manuales. Necesarios para la restauración en caso de un daño del disco duro o pérdida de datos o un Trusted Platform Module dañado. Se requieren los datos de restablecimiento de las contraseñas en un paquete de archivos para restablecer las contraseñas de usuario básico.</p> <p> En el modo servidor, estos archivos no son necesarios ya que el restablecimiento de la contraseña, la copia de seguridad y la restauración de Security Platform son realizadas por Trusted Computing Management Server.</p>
Tarjeta de seguridad para el restablecimiento de contraseñas	Administrador	<p>Creado durante la configuración de las Funciones de Security Platform (cuando se utiliza el Asistente para la inicialización de Security Platform).</p> <p>Necesario para la restauración en caso de una recuperación de emergencia (Trusted Platform Module dañado).</p> <p> En el modo servidor, este archivo no es necesario ya que el restablecimiento de la contraseña es llevado a cabo por Trusted Computing Management Server.</p>
Tarjeta de seguridad	Administrador	Creado durante la

<p>para la recuperación de emergencia</p>		<p>configuración de las Funciones de Security Platform (cuando se utiliza el Asistente para la inicialización de Security Platform).</p> <p>Necesario para preparar el restablecimiento de la contraseña de un usuario específico.</p> <p> En el modo servidor, este archivo no es necesario ya que la restauración de Security Platform es llevada a cabo por Trusted Computing Management Server.</p>
<p>Recuperación de emergencia/Tarjeta de seguridad para restablecimiento de contraseña</p>	<p>Administrador</p>	<p>Creado durante la inicialización de Security Platform (cuando se utiliza el Asistente para la inicialización rápida de Security Platform).</p> <p>Combina la Tarjeta de seguridad para la recuperación de emergencia y la Tarjeta de seguridad para el restablecimiento de contraseña en un archivo.</p>
<p>Paquete de archivos de migración</p>	<p>Usuario</p>	<p>Contiene las claves y certificados de usuario que se van a migrar a otro Security Platform. Creado durante el paso de <i>Exportación</i> de la migración. Necesario para el paso de <i>Importación</i> de la migración.</p> <p> En el modo servidor, este archivo no es necesario ya que</p>

		la migración es llevada a cabo por Trusted Computing Management Server.
Datos secretos personales para el restablecimiento de la contraseña	Usuario	Creado durante la configuración de los valores del Usuario de Security Platform. Necesario para restablecer la contraseña de usuario básico.
Archivo del código de autorización del restablecimiento	Administrador/Usuario	<p>Contiene el código de autorización de restablecimiento necesario para restablecer la contraseña de usuario básico de un usuario Creado durante los pasos administrativos del restablecimiento de la contraseña. Necesario durante los pasos del usuario del restablecimiento de la contraseña.</p> <p> En modo servidor, este archivo es creado por Trusted Computing Management Server.</p>
Archivo PKCS #12 (archivo de Personal Information Exchange)	Usuario	Contiene la clave privada y el certificado de un usuario. Necesario para la importación de un certificado.



La Solución Infineon Security Platform

Uso avanzado de Security Platform

[Datos de restauración y de copia de seguridad de Security Platform](#)

[Recuperación de datos de EFS y PSD por medio de un agente de recuperación](#)

[Migración de claves a otros sistemas](#)

[Restablecer la contraseña de usuario básico](#)

[Defensa contra el ataque de diccionario](#)

Technologies AG



Solución Infineon Security Platform

Datos para la copia de seguridad y restauración de Security Platform

La copia de seguridad de Security Platform incluye todos los datos que se requieren en caso de una emergencia. Luego de una falla de hardware o de un medio de almacenamiento, o una falla del Trusted Platform Module, la restauración de Security Platform reestablece el acceso a las Funciones de Security Platform para todos los usuarios.

Además puede realizar una copia de seguridad y restaurar sus datos del Personal Secure Drive. La copia de seguridad de Security Platform no incluye los datos de otras aplicaciones que utilizan la Solución Security Platform (por ejemplo el correo electrónico seguro).



- En el [modo servidor](#), la Copia de seguridad y la Restauración de las credenciales y configuraciones del usuario son llevadas a cabo por el Trusted Computing Management Server, excepto la Copia de seguridad y Restauración de los archivos imagen de Personal Secure Drive (PSD).
- La actualización de las [configuraciones y credenciales del usuario](#), administrada por el Trusted Computing Management Server, también se basa en la Copia de seguridad y Restauración.

Alcance de la copia de seguridad

La copia de seguridad de Security Platform abarca los siguientes datos:

Credenciales y configuración de Security Platform	
Contenidos de la copia de seguridad	Contenidos de la copia de seguridad Una copia de las credenciales y configuración específicas del usuario que se encuentren almacenadas en Security Platform.
Propósito	La restauración de las credenciales y configuración específicas del usuario, luego de una falla en el hardware o en el medio de almacenamiento. De otra forma los usuarios ya no podrían acceder a las Funciones de Security Platform y los datos del usuario se perderían.
Archivos	<ul style="list-style-type: none">• Paquete de archivos de la copia de seguridad grabado automáticamente ("Archivo comprimido de la copia de seguridad del sistema", por ejemplo: archivo SPSystemBackup.xml y carpeta SPSystemBackup): Configurado por el administrador de Security Platform. Contiene las credenciales y la configuración de todos los usuarios de Security Platform (para una o más computadoras de Security Platform). También contiene la identificación de la computadora y del usuario que se utilizan para hacer corresponder cada computadora con sus usuarios durante el proceso de restauración.• Paquete de archivos de la copia de seguridad grabado manualmente (por ejemplo SPBackupArchive.xml): Creado por el Usuario de Security Platform. Contiene las credenciales y la configuración de un Usuario de Security Platform (para una computadora de Security Platform). También contiene la identificación de la computadora y del usuario que se utiliza para hacer corresponder la computadora con su usuario durante el proceso de restauración.
Recuperación de emergencia	
Contenidos	Todas las claves de usuario básico de Security Platform,

de la copia de seguridad	específicamente encriptadas para la recuperación de emergencia.
Propósito	<p>Reencriptación de todas las claves de usuario básico luego de una falla en el Trusted Platform Module. En este caso se debe configurar una nueva Security Platform y crear un nuevo propietario. La recuperación de emergencia permite la reencriptación de las claves de usuario básico desde el propietario anterior al nuevo.</p> <p>De otra forma los usuarios ya no podrían acceder a las Funciones de Security Platform y los datos del usuario se perderían.</p>
Archivos	<ul style="list-style-type: none"> • Los datos de recuperación de emergencia para todos los usuarios están incluidos en los Paquetes de archivos de copia de seguridad escritos de modo automático. También se los incluye para el usuario en cuestión en los archivos de copia de seguridad escritos de modo manual si la Copia de seguridad automática ya se ha configurado en el momento de realización de la copia de seguridad manual. • Tarjeta de seguridad de recuperación de emergencia (por ejemplo, SPEmRecToken.xml) o Recuperación de emergencia/Tarjeta de seguridad de restablecimiento de la contraseña combinada (por ejemplo, SpToken_<PCName>.xml): Creado por el administrador de Security Platform. Se requiere para la restauración de los datos de recuperación de emergencia.

Personal Secure Drive

Contenidos de la copia de seguridad	Una copia de las credenciales PSD, los valores de configuración y los datos encriptados.
Propósito	<p>La restauración de los valores de configuración y datos encriptados de PSD luego de una falla en el hardware o en el medio de almacenamiento.</p> <p>Caso contrario los usuarios ya no podrían desencriptar sus datos de PSD.</p>

Notas:

- A diferencia de la copia de seguridad de PSD, las herramientas de copia de seguridad del disco rígido estándar producen copias de seguridad no encriptadas.
- Si se perdieron las credenciales de PSD y no se encuentra disponible ninguna copia de seguridad de las credenciales, pero sí se encuentra disponible un archivo imagen de PSD o archivo imagen de la copia de seguridad, dichos datos pueden ser recuperados por medio de la [Recuperación del Personal Secure Drive](#).

Archivos

- Los valores de la configuración PSD se incluyen tanto en los **Paquete de archivos de la copia de seguridad grabados automáticamente** como en los **Paquete de archivos comprimidos de la copia de seguridad grabados manualmente**.
- **Archivo de copia de seguridad de PSD** (por ejemplo SpPSDBackup.fsb): Se puede crear una copia de la copia de seguridad del archivo imagen de PSD durante una copia de seguridad manual del Usuario de Security Platform.

Tipos de copia de seguridad

Tipo	Explicación
Copia de seguridad del sistema ("Copia de seguridad automática")	<p>Siempre incluye las credenciales y configuraciones de la computadora y todos los usuarios que están inicializados en el momento en el que se realiza la copia de seguridad del sistema (incluyendo datos de recuperación de emergencia).</p> <p>Detalles sobre cómo realizar la Copia de seguridad del sistema</p>
Copia de seguridad manual	<p>Incluye las credenciales y valores de la computadora y del usuario actual.</p> <p>Incluye los datos de recuperación de emergencia para el usuario actual si la Copia de seguridad automática ya ha sido configurada al momento de realizar la copia de seguridad manual.</p> <p>Otra opción es realizar una copia de seguridad de los archivos imagen del Personal Secure Drive (PSD) actualmente configurados para el usuario actual.</p> <p>Detalles sobre cómo realizar la Copia de seguridad manual</p>

Casos de restauración

Existen diferentes casos de restauración dependiendo del tipo de emergencia:

Caso de restauración	Alcance de la restauración afectada
Disco duro dañado o pérdida de datos	Credenciales y configuración de Security Platform, Personal Secure Drive
Nuevo Trusted Platform Module	Recuperación de emergencia
Nuevo Security Platform a inicializar:	Recuperación de emergencia, credenciales y configuración de Security Platform, Personal Secure Drive

Cómo realizar una copia de seguridad y una restauración

Cómo configurar una copia de seguridad automática ("Copia de seguridad del sistema")	Componente de software a utilizar
<p>Tarea administrativa: Configurar las copias de seguridad automáticas para todos los usuarios (incluyendo credenciales y configuración de Security Platform, recuperación de emergencia y los valores de configuración de PSD).</p>	<p>Si Security Platform aún no está inicializada:</p> <p>Configuración por medio del Asistente de inicialización rápida</p> <p>Aquí se configura automáticamente la Copia de seguridad del sistema con los valores predeterminados.</p> <p>Configuración por medio del Asistente de inicialización de Security Platform</p> <p>Siga los pasos mencionados:</p> <ul style="list-style-type: none">• Ejecute la herramienta de Configuración de Infineon Security Platform. En la página de Bienvenida del Asistente de inicialización rápida, seleccione Inicialización avanzada.• Seleccione inicialización de Security Platform y haga clic en Siguiente.• Establezca la Contraseña de propietario y haga clic en Siguiente• Durante el Asistente para la inicialización, tilde la casilla de verificación Copia de seguridad automática (incluye Recuperación de emergencia) y haga clic Siguiente.

- Seleccione la ubicación en el disco rígido en donde guardar el Archivo de la copia de seguridad. Se crearán el archivo de la copia de seguridad que consiste en un archivo XML (por ej. SPSsystemBackup.xml) y una carpeta (por ej. SPSsystemBackup) será creado en la ubicación predeterminada: *\%ALLUSERSPROFILE%\My Documents\Security Platform*.
- La copia de seguridad programada por defecto está configurada para ejecutarse a diario a las 12:00 PM. Para cambiar la hora, haga clic en **Programa...** , y seleccione el tiempo de inicio para crear una copia de seguridad programada y haga clic en **Aceptar**; a continuación, haga clic en **Siguiente**.
- Seleccione la opción **Crear una nueva tarjeta de seguridad de recuperación**.
- Seleccione la ubicación de su preferencia para guardar el archivo de la Tarjeta de seguridad de recuperación de emergencia (nombre de archivo predeterminado: SPEmRecToken.xml).
- Configure una nueva contraseña para la tarjeta de seguridad y haga clic en **Siguiente**.
- Confirme las configuraciones y haga clic en **Siguiente**.
- Tilde la casilla de verificación

Ejecutar copia de seguridad automática ahora. Haga clic **Finalizar** en la página de finalización.

- Se realiza una copia de seguridad de las credenciales y configuraciones de Security Platform por primera vez. Las copias de seguridad regulares se llevarán a cabo según lo programado.

Si Security Platform ya se encuentra inicializada: [Herramienta de configuración - Copia de seguridad - Configurar...](#)

Siga los pasos mencionados:

- Ejecute el Infineon Security Platform Settings Tool y seleccione **Copia de seguridad**.
- Haga clic **Configurar...** para ejecutar el Asistente para la inicialización.
- Seleccione la ubicación en el disco rígido en donde guardar el Archivo de la copia de seguridad. Se crearán el archivo de la copia de seguridad que consiste en un archivo XML (por ej. SPSsystemBackup.xml) y una carpeta (por ej. SPSsystemBackup) será creado en la ubicación predeterminada: `\%ALLUSERSPROFILE%\My Documents\Security Platform`.
- La copia de seguridad programada por defecto está configurada para ejecutarse a

diario a las 12:00 PM. Para cambiar la hora, haga clic en **Programa...** , y seleccione el tiempo de inicio para crear una copia de seguridad programada y haga clic en **Aceptar**; a continuación, haga clic en **Siguiente**.

- Confirme las configuraciones y haga clic en **Siguiente**.
- Tilde la casilla de **Ejecutar copia de seguridad automática ahora** y haga clic **Finalizar** en la página de finalización.
- Se realiza una copia de seguridad de las credenciales y configuraciones de Security Platform por primera vez. Las copias de seguridad regulares se llevarán a cabo según lo programado.

 En el [modo servidor](#) este botón está desactivado ya que las copias de seguridad automáticas son llevadas a cabo por el Trusted Computing Management Server, es decir que aquí no se requiere configuración explícita por parte del usuario.

Cómo realizar una copia de seguridad ("Copia de seguridad manual")

Tarea del usuario: Ejecutar una copia de seguridad manualmente para el usuario actual.

Componente de software a utilizar

Siga los pasos mencionados:

- Ejecute el Infineon Security Platform Settings Tool y seleccione **Copia de seguridad**.

[Herramienta de Configuración - Copia de seguridad - Copia de seguridad...](#)

- Haga clic **Copia de seguridad...** para ejecutar el Asistente para la copia de seguridad.
- Haga clic **Buscar...** y seleccione la ubicación en el disco rígido en donde se guardará el archivo de copia de seguridad (Nombre de archivo predeterminado: SPBackupArchive.xml). Haga clic en **Siguiente**.
- Configure los valores de copia de seguridad del Personal Secure Drive (ver [Configurar los valores de copia de seguridad de Personal Secure Drive](#)) y haga clic en **Siguiente**.
- Confirme las configuraciones y haga clic en **Siguiente**.
- Haga clic **Finalizar** en la página de Finalización.

 En [modo servidor](#), sólo puede hacer copias de seguridad de Personal Secure Drives (PSD). En el modo servidor, Trusted Computing Management Server realiza la copia de seguridad de las credenciales y valores del usuario. Además de las condiciones arriba mencionadas, este botón está deshabilitado si no tiene configurado su Personal Secure Drive (PSD).

Cómo realizar una restauración

Tarea administrativa: Preparar una

Componente de software a utilizar

[Herramienta de Configuración -](#)

restauración para determinados usuarios.

Tarea del usuario: Ejecutar manualmente la restauración para el usuario actual. Si se ha preparado una restauración para el usuario actual, complete dicha restauración.



Si se encuentra disponible un paquete de archivos de la copia de seguridad grabado manualmente y no se necesitan restaurar datos de una recuperación de emergencia, el usuario puede llevar a cabo la restauración sin la preparación del administrador.

[Copia de seguridad - Realizar una restauración todo...](#)

Cómo restaurar ("Restauración manual")

Tarea del usuario: Ejecutar manualmente la restauración para el usuario actual.

Si los datos de Recuperación de emergencia se encuentran en la copia de seguridad manual y el usuario actual es el administrador, esta copia de seguridad también puede ser utilizada para una restauración de Recuperación de emergencia del usuario actual.

Componente de software a utilizar

Siga los pasos mencionados:

- Ejecute el Infineon Security Platform Settings Tool y seleccione **Copia de seguridad**. [Security Module - Copia de seguridad - Restaurar...](#)
- Haga clic **Restaurar...** para ejecutar el Asistente para la copia de seguridad.
- Si desea restaurar sus valores y credenciales, tilde la casilla de verificación **Restaurar mis valores y credenciales**. Haga clic en **Buscar...** y busque el paquete de archivos de copia de seguridad (Nombre de archivo predeterminado: SPBackupArchive.xml).
- Haga clic en **Siguiente**.

- Autentíquese y haga clic en **Siguiente**.
- Confirme las configuraciones y haga clic en **Siguiente**.
- Si desea restaurar uno o más Personal Secure Drives, configure los valores de restauración de su Personal Secure Drive (ver [Configurar los valores de restauración del Personal Secure Drive](#)).
- Haga clic en **Siguiente**.
- Confirme las configuraciones y haga clic en **Siguiente**.
- Otra opción es tildar la casilla de verificación **Iniciar el Asistente de inicialización del usuario de Security Platform** si desea configurar otras funciones de Security Platform.
- Haga clic **Finalizar** en la página de Finalización.
- Sus certificados ya están restaurados. Puede visualizar sus certificados en **Configuraciones del usuario - Certificados de Security Platform**.
- Haga clic con el botón derecho del mouse sobre el icono de notificación de la barra de tareas y cargue su PSD. Autentíquese.



En [modo servidor](#), sólo puede restaurar su Personal Secure Drive (PSD). Trusted Computing Management Server realiza la restauración de las credenciales y configuraciones en el modo servidor.

Políticas relacionadas con la copia de seguridad

- Se puede imponer la configuración de las copias de seguridad automáticas por medio de la política [*Imponer la configuración de la copia de seguridad que incluya la recuperación de emergencia.*](#)
- La ruta de destino de la copia de seguridad para las copias de seguridad automáticas se puede imponer por medio de la política [*Ubicación del paquete de archivos de la copia de seguridad.*](#)
- Por medio de la política [*Implementar copias de seguridad del sistema inmediatamente.*](#), se puede implementar la actualización de la copia de seguridad del sistema luego de realizados cambios significativos a los datos de Security Platform.



La Solución Infineon Security Platform

Administración de la funcionalidad para la recuperación de emergencia

El Software de la Solución Infineon Security Platform está diseñado para ofrecer un respaldo a gran escala, no sólo para un caudal de trabajo estándar, sino también para las operaciones de recuperación en el sistema en el caso de una situación de error grave.

El peor tipo de problema es un daño al Trusted Platform Module. Esta situación da como resultado la pérdida del propietario de Infineon Security Platform, el cual constituye la raíz física de los secretos y también la raíz lógica de todas las claves específicas del usuario de Infineon Security Platform. Cada vez que se deba reemplazar el Trusted Platform Module se crea un nuevo propietario de Infineon Security Platform, ya que no existe un modo para transferir una clave existente de un Trusted Platform Module a otro.

Para solucionar este posible problema se integró un mecanismo de recuperación de emergencia en el Software de la solución Infineon Security Platform. Este mecanismo permite la re-encryptación de las Claves del usuario básico desde un propietario de Infineon Security Platform hacia otro. Este mecanismo permite la re-encryptación de las claves de usuario básico desde una clave de propietario de Infineon Security Platform a otra. Para lograrlo se debe configurar la copia de seguridad de las Funciones de Security Platform (incluyendo la recuperación de emergencia) al configurar Infineon Security Platform. El administrador lo lleva a cabo utilizando el [Asistente para la inicialización rápida](#) o el [Asistente para la inicialización de Security Platform](#).

La restauración en caso de emergencia se realiza por medio del [Asistente para la copia de seguridad de Security Platform](#).



En el [modo servidor](#), las tareas de copia de seguridad y restauración son llevadas a cabo por el Trusted Computing Management Server, excepto la copia de seguridad y restauración de los archivos de imagen de Personal Secure Drive (PSD).

Tarjeta de seguridad para la recuperación de emergencia, contraseña y paquete de archivos

El concepto de recuperación de emergencia es similar al del [Restablecimiento de la contraseña](#) en cuanto a la utilización de la tarjeta de seguridad, la contraseña y el paquete de archivos.

La restauración de las claves de usuario en caso de emergencia requiere de determinada información almacenada en un paquete de archivos. Los datos de la recuperación de emergencia en este paquete de archivos sólo se pueden utilizar en combinación con una tarjeta de seguridad de recuperación que esté protegida con una contraseña independiente.

El paquete de archivos contiene copias encriptadas de las claves de usuario básico para permitir la restauración en caso de una falla del Trusted Platform Module. Si no se configura la recuperación de emergencia, los usuarios pueden tener dificultades para restaurar sus datos encriptados en caso de una falla del Security Platform. La recuperación de emergencia se configura una vez y los componentes de Security Platform acceden posteriormente al paquete de archivos correspondiente, de manera automática. El paquete de archivos debe ser accesible para todos los usuarios de esta Security platform.

Consulte las [Preguntas más frecuentes](#) para ver algunos aspectos generales sobre el manejo de la recuperación de emergencia.

[Restaurar paso a paso los datos de recuperación de emergencia](#)



Inicialización de usuario forzada cuando el paquete de archivos de la copia de seguridad no está disponible:

Si no se puede cargar la clave de usuario básico (por ejemplo al eliminar y volver a obtener la propiedad de Trusted Platform Module) el asistente para la inicialización de usuarios de Security Platform no permite continuar con la inicialización del usuario.

En este tipo de situaciones lo correcto es restaurar los datos de la recuperación de emergencia.

Si por alguna razón el paquete de archivos de la copia de seguridad no se encuentra disponible (por ejemplo si se perdió o está dañado) no se podrán restaurar la clave de usuario básico. En este caso, para continuar

con la creación de una nueva clave de usuario básico, se debe iniciar el asistente para la inicialización de usuarios de Security Platform por medio del [parámetro de la línea de comandos](#): *SpUserWz.exe /forceinit*.

Nota:

- Se creará una nueva clave de usuario básico y por consiguiente se perderán todos los datos protegidos con anterioridad.
- Parámetro de la línea de comandos: *SpUserWz.exe /forceinit* no se encuentra soportado en el [modo servidor](#).



La Solución Infineon Security Platform

Restaurar paso a paso los datos de recuperación de emergencia

Con los datos de recuperación de emergencia puede restaurar la funcionalidad de Infineon Security Platform ante alguna falla y posterior reemplazo de su Trusted Platform Module. El proceso de restauración cuenta de dos partes:

Realizado por un administrador de Security Platform:

- Recreación de la funcionalidad básica del Infineon Security Platform (que incluye la activación de Trusted Platform Module, la inicialización de Security Platform y la restauración de los datos de recuperación de emergencia).



En [modo servidor](#), el Trusted Platform Module debe ser habilitado y activado antes de que el administrador conecte el sistema al Trust Domain. No hay disponibles otras tareas de administración, ya que Trusted Computing Management Server administra estas tareas.

Realizado por todos los usuarios de Security Platform:

- Restauración de las claves de usuario básico para obtener acceso nuevamente a los datos protegidos, o generación de nuevas claves de usuario básico, que resultan en la pérdida de todos los datos protegidos existentes.



Prerrequisitos:

- **Paquete de archivos de la copia de seguridad incluyendo los datos de la recuperación de emergencia:** Este archivo se crea al configurar la función de copia de seguridad de Security Platform. Se recomienda encarecidamente configurar la copia de seguridad incluyendo la recuperación de emergencia para preservar los datos del usuario en caso de una falla grave del sistema. El paquete de archivos de la copia de seguridad debe estar accesible para el proceso de restauración. Debe almacenarse en una ubicación segura como ser una carpeta de red con copias de seguridad regulares. Si se ubica en un disco duro local, se recomienda incluir este archivo en las copias de seguridad periódicas. La página de [preguntas más frecuentes](#) brinda consejos adicionales para configurar correctamente los datos de la recuperación de emergencia.

- **Tarjeta de seguridad para la recuperación de emergencia:** Este archivo protege los datos de recuperación de emergencia del uso no autorizado y requiere del conocimiento de una contraseña aparte. Se crea al configurar la función de copia de seguridad de Security Platform. Debe ser almacenado por separado del Paquete de archivos de copia de seguridad en un medio extraíble en un entorno seguro. La tarjeta de seguridad para la recuperación de emergencia debe estar accesible para el proceso de restauración.
- En el [modo servidor](#), las tareas de copia de seguridad y restauración son llevadas a cabo por el Trusted Computing Management Server, excepto la copia de seguridad y restauración de los archivos de imagen de Personal Secure Drive (PSD).

Pasos administrativos

Paso 1 - Preparación del Trusted Platform Module

Una falla de su Trusted Platform Module es una de las razones posibles para una restauración. Si esto ocurre, primero debe habilitarse el nuevo chip en la BIOS del sistema.

Si el causante del mal funcionamiento fue otro hardware (por ejemplo, una falla del disco duro), se debe configurar correctamente el sistema (restaurar el sistema operativo, los perfiles de usuario y los datos protegidos) antes de restaurar el Infineon Security Platform.

Procedimiento:

Esta operación la lleva a cabo un administrador del sistema. He aquí una descripción específica sobre cómo habilitar el chip:

Paso 2 - Inicialización de Security Platform y restauración de los datos de recuperación de emergencia

Una vez habilitado el Trusted Platform Module, debe inicializar el Security Platform y restaurar los datos de la recuperación de emergencia. El paquete de archivos de la copia de seguridad y la tarjeta de seguridad de recuperación de emergencia deben estar accesibles para realizar este paso.

Procedimiento:

Sólo un administrador de Infineon Security Platform puede restaurar los datos de la recuperación de emergencia. Ejecute el asistente para la inicialización de Infineon Security Platform y seleccione [Restaurar Security Platform desde un paquete de archivos de la copia de seguridad](#).

Paso del usuario

Recuperación de un Usuario de Infineon Security Platform

Luego de finalizada las operaciones administrativas, se puede llevar a cabo la operación de recuperación para los usuarios de Infineon Security Platform. Se debe realizar de manera individual la restauración de cada Usuario de Infineon Security Platform .

Procedimiento:

Abra el [Asistente para la inicialización de usuarios de Security Platform](#). Una vez inicializado, el asistente detecta en forma automática el estado de recuperación. Ofrece la posibilidad de crear una nueva clave de usuario básico o de restaurar una ya existente desde un paquete de archivos de la copia de seguridad. Por lo general se debe recuperar una clave existente, de lo contrario todos los datos encriptados previamente no estarán disponibles. Siga las indicaciones en pantalla para finalizar el proceso.



La solución Infineon Security Platform

Actualizar las configuraciones y credenciales del usuario (Modo Servidor)

Cuando sea necesaria una actualización de sus configuraciones y credenciales de usuario, se le informará mediante un cuadro de texto. Este cuadro de texto aparece en el área de notificación de la barra de tareas cuando esté conectado a Windows. Puede hacer clic en el cuadro de texto para llevar a cabo la actualización. Si no ve, o no le da importancia a este cuadro de texto, puede iniciar la actualización más adelante mediante el [elemento del menú de notificaciones de la barra de tareas](#).

Se requiere una actualización de sus configuraciones y credenciales en las siguientes circunstancias:

- Si aun no tiene configuraciones y credenciales de usuario en la plataforma actual (ya que acaba de registrarse en esta plataforma), pero Trusted Computing Management Server ya tiene configuraciones y credenciales para su cuenta de usuario (por haberlas utilizado en otra plataforma).
- Ya tiene configuraciones y credenciales de usuario en la plataforma actual, pero estas han sido modificadas desde otra plataforma.
- Tenía configuraciones y credenciales de usuario en la plataforma actual pero se extraviaron (por ejemplo, debido a una ruptura del disco rígido).
- Sus credenciales de usuario y valores de configuración actuales no son consistentes (por ejemplo porque ha fallado un cambio anterior). En este caso necesita conseguir sus últimos credenciales y valores de configuración conocidos válidos del servidor.

De esta manera, sus configuraciones y credenciales son sincronizadas en caso de plataformas múltiples y restauradas en plataformas dañadas.



- Asegúrese de no tener cargado un Personal Secure Drive antes de actualizar sus configuraciones y credenciales.
- Observe que la actualización de sus configuraciones y credenciales requiere de su [autenticación de usuario](#).



©Infineon

La Solución Infineon Security Platform

Recuperación de datos de EFS y PSD por medio de un agente de recuperación

El agente de recuperación le permite acceder a sus datos de EFS o PSD en los siguientes casos:

- Se han perdido las credenciales de encriptación de datos.
- No se encuentra disponible la copia de seguridad de las credenciales.
- Los datos encriptados se encuentran disponibles (archivos EFS, archivo imagen de PSD o archivo imagen de copia de seguridad).
- Se encuentra disponible un agente de recuperación.

Se encuentra disponible información más detallada sobre la recuperación de EFS en Microsoft TechNet.

La información detallada sobre la Recuperación de PSD se encuentra disponible aquí: [Recuperación de Personal Secure Drive](#).



©Infineon Technologies AG

La Solución Infineon Security Platform

Migración de claves a otros sistemas

Una vez que se configura el usuario del sistema como Usuario de Infineon Security Platform, puede surgir la necesidad de suministrar el entorno de seguridad específico del usuario, no sólo en la computadora donde se realizó la instalación, sino también en aquellas en donde el usuario tenga acceso. La instalación de instalaciones múltiples en diferentes computadoras no será de ayuda, ya que los elementos de seguridad no son compatibles - por ejemplo, el inicio de sesión para correo electrónico en una computadora no se aceptará en la otra debido a las distintas claves de inicio de sesión.

Conceptos básicos de la migración

Infineon Security Platform ofrece la posibilidad de mantener y administrar esta situación al brindar una ruta de migración para los datos secretos específicos del usuario. La idea básica de esta tecnología es la separación estricta del rol administrativo y el operacional de la migración. Esta separación es necesaria para garantizar la personalidad de los datos secretos que se migran, y al mismo tiempo asegurar que no existe ningún medio para transferir los datos secretos sin el conocimiento de una instancia administrativa.

Una vez finalizada una migración de un usuario, la computadora de destino almacena el mismo entorno de seguridad que también se encuentra disponible en la computadora de origen. Desde el punto de vista del Usuario de Infineon Security Platform, no hay diferencia entre el comportamiento operacional de los sistemas.

Sin embargo, las dos computadoras siguen siendo Infineon Security Platforms independientes. La migración de las claves de usuario no tienen ningún impacto en la estructura de seguridad primaria del Infineon Security Platform. Lo más importante de todo es que los datos secretos que se encuentran almacenados en el Trusted Platform Module permanecen inalterados por esta operación.



En el [modo servidor](#), la migración de las configuraciones y credenciales específicas del usuario es llevada a cabo por Trusted Computing Management Server. Al conectarse, los usuarios obtienen las actualizaciones necesarias cuando sus configuraciones y credenciales han sido modificadas. Esto también se conoce por *roaming*. La actualización desde la base de datos del servidor sobrescribe las configuraciones y credenciales locales específicas del usuario.

En el modo [Aislado](#) se fusionan las configuraciones y credenciales específicas del usuario sobre la computadora de origen y destino de la migración.

La operación de migración se lleva a cabo por medio del [Asistente para la migración de Infineon Security Platform](#).



Migración a una computadora que no posee claves y certificados de usuario:

El proceso de migración instala nuevas claves y certificados de usuario en la máquina a la que realiza la migración.

Será necesario que configure las Funciones de Security Platform para utilizarlas con las nuevas claves y certificados.



Migración a una computadora con claves y certificados de usuario existentes (clave de usuario básico diferente):

El proceso de migración invalidará sus claves y certificados de Security Platform existentes que se encuentren instalados en la máquina a la que está migrando. Sus datos encriptados se pueden perder como resultado de esta operación. Desencripte sus datos antes de proceder con la migración o consulte a su administrador de sistemas sobre el procedimiento de recuperación de datos.



Migración a una computadora que posee claves y certificados de usuario (la misma clave de usuario básico):

Si la computadora de destino ya utiliza la misma clave de usuario básico que la computadora de origen, el proceso de migración combinará sus claves y certificados de usuario. Luego de la migración, las claves y certificados del paquete de archivos de migración estarán activas. Se guardarán las claves y certificados anteriores. De esta forma no pierde ningún dato encriptado.

Por ejemplo, si encriptó sus datos con EFS o PSD tanto en la computadora de origen de la migración como en la de destino, pero utilizó certificados diferentes en ambas computadoras, la migración activará el certificado desde la computadora de origen a la de destino. Se guardará el certificado que utilizaba anteriormente la computadora de destino y podrán reactivarse en cualquier momento.



Migración y Personal Secure Drive:

- Si un usuario tenía Personal Secure Drives configurados en la computadora de origen en un medio extraíble (por ejemplo una memoria USB), este medio también puede ser utilizado en la computadora de destino.
- Si un usuario tenía Personal Secure Drives configurados en la computadora de origen en un disco duro fijo, es importante realizar una copia de seguridad de todos los archivos imagen del Personal Secure Drive a ser migrados, y también almacenar los archivos imagen de copia de seguridad de la computadora de origen en una ubicación a la que pueda accederse desde ambas computadoras. Para utilizar una copia de un Personal Secure Drive de origen en la computadora de destino, el archivo imagen de la copia de seguridad

en cuestión de la computadora de origen debe ser restaurado. Tenga en cuenta que tendrá dos Personal Secure Drives independientes en la computadora de origen y destino después de la migración. Los usuarios podrían tener que reconfigurar los Personal Secure Drives en la computadora de destino (ver [Administración de Personal Secure Drives](#)). Para reconfigurar un Personal Secure Drive, seleccione *Deseo cambiar mis configuraciones de Personal Secure Drive* y siga las indicaciones en pantalla.

- Tenga en cuenta que las configuraciones y credenciales de PSD en la computadora de destino serán sobrescritas si las Claves del usuario básico difieren en la computadora de origen y destino. En tal caso se recomienda que guarde una copia no encriptada de los datos de su PSD antes de la migración. Puede realizarlo borrando el PSD con la opción de guardar una copia no encriptada (ver [Administración de los Personal Secure Drives](#)).



La Solución Infineon Security Platform

Migración paso a paso

El proceso de migración de credenciales consta de dos partes - los pasos administrativos y los pasos del usuario. La primera parte consiste de la autorización, configuración y administración del proceso de migración realizado por el administrador. Una vez que finaliza la migración de las claves y certificados, el usuario deberá reconfigurar los Personal Secure Drives en la computadora de destino con las nuevas credenciales.



En el [modo servidor](#), la migración de los certificados y claves de específicas del usuario es llevada a cabo por Trusted Computing Management Server, es decir, no tiene que realizar los pasos de migración (excepto los pasos del usuario 3 y 4).

Pasos administrativos

Paso 1 - Exportación de la identidad de la computadora de destino

El llevar a cabo una migración requiere que primero se identifique a la computadora de destino adonde se intentará migrar las claves y certificados del usuario. Para poder lograrlo, el administrador de la computadora de destino pone a disposición (exporta) una clave pública para identificar dicha computadora. Esta clave se utilizará posteriormente para asociar las claves y certificados del usuario a esta computadora (Nota: Cuando el contenido se encuentra protegido por medio de la clave pública del sistema de destino, sólo la clave privada de la computadora, que se encuentra protegida por el Trusted Platform Module, puede acceder a las claves y certificados que se migraron). Este paso es necesario para crear una raíz de confianza en la operación de migración - asegurándose de que sólo los sistemas de destino pueden acceder a las credenciales sensibles al usuario.

Procedimiento:

El administrador del Infineon Security Platform del sistema de destino debe exportar el certificado de la computadora (clave pública) a un archivo. Siga los pasos mencionados:

- Seleccione **Migración** en la Infineon Security Platform Settings Tool.
- Seleccione **Esta es la plataforma de destino** y haga clic en **Guardar....**
- Busque una ubicación de su preferencia para guardar el archivo, la cual sea accesible desde ambas computadoras. El archivo se guarda bajo un nombre predeterminado como **SpPubKeyArchive.xml**.

Medios de almacenamiento aceptables: Medios extraíbles o disco de red mapeado.

Tome nota de la ubicación y nombre de archivo de la clave exportada ya que será requerida para el siguiente paso.

Paso 2 - Autorización del propietario de la computadora de origen

El próximo paso en la migración requiere que el propietario de la computadora de origen (a migrar) autorice la migración de las claves y certificados de usuario a una computadora de destino específica. Para ello es necesario que el propietario tenga acceso a la clave pública de la computadora de destino. Es la clave pública que el administrador de la computadora de destino exportó previamente (vea el paso 1 más arriba). La autorización de la computadora de destino por parte del Propietario de Infineon Security Platform hace que la pila del software de seguridad asegure que las claves y certificados de usuario se puedan asociar solamente con la computadora de destino especificada.

Procedimiento:

El administrador del Infineon Security Platform de la computadora de origen (computadora a migrar) debe autorizar la exportación de las credenciales de usuario a la computadora de destino deseada. Siga los pasos mencionados:

- Seleccione **Migración** en la Infineon Security Platform Settings Tool.
- Seleccione **Esta es la plataforma de origen** y haga clic en **Autorizar...**
- En la pantalla de Autorizar migración, haga clic en **Importar...**
- Seleccione la ubicación del archivo de la clave pública **SpPubKeyArchive.xml** y haga clic en **Abrir**.
- Escriba la Contraseña de propietario de la computadora de origen o suministre el Archivo de copia de seguridad con la contraseña de propietario y haga clic en **Aceptar**.
- Verifique que estén listados el nombre del servidor de la computadora de destino

	y el ID de plataforma único y haga clic en Cerrar .
<p>Paso 1 y Paso 2 combinados - Exportación y autorización automáticas</p>	<p>Procedimiento:</p>
<p>Una forma alternativa de combinar y ejecutar los dos pasos anteriores es la auto-exportación y autorización, que omite el paso 1 mencionado más arriba y es muy similar al paso 2. El Propietario de Infineon Security Platform de la computadora de origen autoriza la migración de las claves y los certificados del usuario de una computadora específica hacia la computadora de destino. La diferencia está en que en lugar de identificar manualmente el archivo con las credenciales de la computadora de destino, se identifica a la plataforma de destino por medio del cuadro de diálogo de búsqueda de la computadora de red estándar. Una vez que se identificó el sistema, Infineon Security Platform intenta contactarse dinámicamente con la máquina de destino (por medio de DCOM) y solicita las claves y certificados de la plataforma. Si el sistema de destino está equipado con el Infineon Security Platform, la información de migración se transfiere automáticamente entre las dos computadoras.</p> <p>Prerrequisitos:</p> <ul style="list-style-type: none"> • Computadora de origen: El usuario actual (Propietario de Infineon Security Platform) debe ser miembro del grupo de administradores de la computadora de destino. • Computadora de destino: Infineon Security Platform debe estar instalado y habilitado. 	<p>El administrador del Infineon Security Platform de la computadora de origen (computadora a migrar) debe autorizar la exportación de las credenciales y claves de usuario a la computadora de destino deseada. Siga los pasos mencionados:</p> <ul style="list-style-type: none"> • Seleccione Migración en el Infineon Security Platform Settings Tool. • Seleccione Esta es la plataforma de origen y haga clic en Autorizar.... • En la pantalla de Autorizar migración, haga clic en Buscar... Se abrirá el cuadro de diálogo de búsqueda de la red. • Busque y encuentre la computadora de destino y seleccione OK. • Esto dará inicio a la transferencia automática de la información de migración desde la computadora de origen a la computadora de

- Computadora de destino: La política del sistema *Permitir a los administradores obtener la clave pública SRK remotamente* debe estar habilitada.
- Computadora de destino: No debe haber ningún firewall que bloquee la solicitud entrante DCOM (como el firewall integrado en Microsoft Windows XP, ni cualquier otro firewall).
- La red debe estar configurada para permitir solicitudes DCOM.
- Tanto la computadora de origen como la de destino deben ser miembros de dominios compatibles entre sí.

En los casos en que la autorización automática no es posible, se deben seguir los pasos manuales (1 & 2) mencionados más arriba.

destino.

Pasos del usuario



Si un usuario tenía configurado Personal Secure Drive en la computadora de origen, es importante realizar una copia de seguridad del mismo y guardar el archivo de copia de seguridad de PSD (nombre predeterminado: **SpPSDBackup.fsb**) de la computadora de origen en una ubicación accesible desde las dos computadoras. Para utilizar copias de los archivos imagen del PSD de origen en la computadora de destino se deben tener disponibles los archivos imagen de copia de seguridad de la computadora de origen.

Paso 1 - Exportar las claves y certificados del usuario desde la computadora de origen

Una vez completados los pasos administrativos, los usuarios individuales de Infineon Security Platform pueden exportar en forma segura sus claves y certificados (protegidos por la clave pública del sistema de destino y por lo tanto sólo pueden ser leídos por la plataforma de destino).

Procedimiento:

Los usuarios de Infineon Security Platform en la computadora de origen exportan sus claves y certificados para la migración. Siga los pasos mencionados:

- Seleccione **Migración** en el Infineon Security Platform Settings Tool.
- Seleccione **Esta es la plataforma de origen** y haga clic en **Exportar....**
- Seleccione la computadora de destino de la lista y haga clic en **Siguiente**.
- Busque una ubicación de su preferencia para guardar el archivo, que sea accesible desde ambas computadoras. El archivo se guarda bajo un nombre predeterminado como

	<p>SpMigrationArchive.xml. Haga clic en Siguiente.</p> <ul style="list-style-type: none"> • Ingrese la contraseña de usuario básico para la computadora de origen y haga clic en Siguiente. • Confirme las configuraciones y haga clic en Siguiente. • En la pantalla de Finalización verifique que la exportación de los certificados y claves de usuario se haya realizado con éxito y haga clic en Finalizar. <p>Tome nota del nombre y ubicación del archivo y de la copia de seguridad de PSD ya que serán requeridos en el siguiente paso.</p>
<p>Paso 2 - Importación de las claves y certificados del usuario a la computadora de destino</p>	<p>Procedimiento:</p>
<p>Posteriormente, se les solicita a los usuarios que "importen" las claves y certificados a las computadoras de destino, siempre que tengan una cuenta de usuario.</p>	<p>En una computadora de destino, los usuarios individuales de Infineon Security Platform pueden importar sus claves y certificados. Siga los pasos mencionados:</p> <ul style="list-style-type: none"> • Seleccione Migración en el Infineon Security Platform Settings Tool. • Seleccione Esta es la plataforma de destino y

haga clic en **Importar....**

- Seleccione la ubicación del archivo **SpMigrationArchive.xml** y haga clic en **Siguiente.**
- Ingrese la contraseña de usuario básico configurada en la computadora de origen y haga clic en **Siguiente.**
- Confirme las configuraciones y haga clic en **Siguiente.**
- Si las funciones de Security Platform ya estaban configuradas en la plataforma de destino, aparecerá un mensaje de advertencia. Lea el mensaje de advertencia cuidadosamente y haga clic en **Sí.**
- En la pantalla de Finalización verifique que la migración de los certificados y claves de usuario se haya realizado con éxito y haga clic en **Finalizar.**
- En la pantalla de finalización del asistente tendrá la oportunidad de avanzar automáticamente al siguiente paso seleccionando la opción **Ejecutar el asistente para la inicialización de usuarios de Security Platform.**

 Tenga en cuenta los consejos en [Migración y Personal Secure Drives](#).

Paso 3 - Configurar las aplicaciones para que utilicen las claves y certificados que se migraron

Procedimiento:

Una vez finalizada la migración de claves y certificados es importante asociar estas nuevas credenciales a cualquier aplicación individual que el usuario tenga intenciones de utilizar en la computadora de destino.

Como las credenciales se pueden usar en diversas aplicaciones, el método para la importación de las claves y certificados migrados será exclusivo para cada proveedor de software de las aplicaciones individuales. Por ejemplo, los usuarios pueden configurar la encriptación del sistema de archivos para usar el certificado migrado. Siga los pasos mencionados:

- Vaya a **Configuraciones de usuario** en el Infineon Security Platform Settings Tool.
- Haga clic en **Configurar...**
- Siga las instrucciones en pantalla y haga clic en **Cambiar...** en las funciones de Security Platform - página de certificado de encriptación.
- Seleccione el certificado migrado, haga clic en **OK** y prosiga a la siguiente página del asistente.

Paso 4 - Reconfiguración de las características del usuario - Personal Secure Drive

Procedimiento:

Una vez que haya finalizado la migración de las claves y los certificados, el usuario debe reconfigurar los valores de Personal Secure Drive en la computadora de destino.

Si uno o más Personal Secure Drives habían sido configurados en la computadora de origen, se deberán reconfigurar los Personal Secure Drives migrados en la computadora de destino (vea [Administración de Personal Secure Drives](#)). Para reconfigurar un Personal Secure Drive, seleccione *Deseo cambiar mis configuraciones de Personal Secure Drive* y siga las instrucciones en pantalla. Para utilizar una copia de un Personal Secure Drive de origen en la computadora de destino, el archivo imagen de la copia de seguridad en cuestión (nombre de archivo predeterminado: **SpPSDBackup.fsb**) de la computadora de origen debe estar restaurado. Tenga en cuenta que tendrá dos Personal Secure Drives independientes en la computadora de origen y destino después de la restauración.



La Solución Infineon Security Platform

Restablecer la contraseña de usuario básico

La Solución Infineon Security Platform permite restablecer las contraseñas de usuario básico.

Esta funcionalidad puede utilizarse en el caso en que un Usuario de Security Platform haya olvidado su contraseña de usuario básico o tenga problemas con su dispositivo de autenticación. Caso contrario se bloquearía el acceso a las Funciones de Security Platform para ese usuario. En tal caso se perderían datos confidenciales.



En el [modo servidor](#), el Trusted Computing Management Server realiza la tarea de crear una Tarjeta de seguridad para el restablecimiento de la contraseña para todos los usuarios, preparando y proporcionando el Código de autorización para el restablecimiento de la contraseña para usuarios específicos, es decir, usted no debe realizar estas tareas. De este modo se deshabilitan todos los botones excepto *Restablecer* y *Habilitar*.

Tarjeta de seguridad para el restablecimiento de la contraseña, contraseña y paquete de archivos

El concepto de restablecimiento de la contraseña es similar al de la [Recuperación de emergencia](#) en cuanto a la utilización de la tarjeta de seguridad, la contraseña y el paquete de archivos.

El restablecimiento de la contraseña de usuario básico de un usuario requiere de cierta información almacenada en un paquete de archivos. Los datos de restablecimiento de la contraseña de este paquete de archivos sólo pueden utilizarse en combinación con una tarjeta de seguridad de restablecimiento de la contraseña que esté protegida por una contraseña independiente.

El paquete de archivos contiene ciertos datos encriptados para cada usuario que permiten el cambio de la contraseña de usuario básico de un usuario que no tenga conocimiento de la contraseña actual. Si no se configura el restablecimiento de la contraseña, los usuarios no podrán restablecer sus contraseñas de usuario básico. El restablecimiento de la contraseña se configura una vez y los componentes de Security Platform acceden posteriormente al paquete de archivos correspondiente, de manera automática. El paquete de archivos debe ser accesible para todos los usuarios de esta Security Platform.

Cómo habilitar la función de restablecimiento de la contraseña

La función de restablecimiento de la contraseña de usuario básico sólo puede utilizarse si el administrador de Security Platform configuró esta funcionalidad para todos los usuarios.

Un Usuario específico de Security Platform sólo puede restablecer su contraseña luego de haber habilitado esta función para su cuenta de usuario. La habilitación requiere de la contraseña de usuario básico o la autenticación mejorada actuales. Por lo tanto, un usuario no puede habilitar y realizar el restablecimiento de su contraseña de usuario básico si ya ha perdido su contraseña actual.

Cómo restablecer una contraseña de usuario

Por razones de seguridad, el restablecimiento de la contraseña consiste de dos tareas - una administrativa y una de usuario. Si su cuenta de usuario se utiliza como administrador de Security Platform y como Usuario de Security Platform, puede restablecer su contraseña en un sólo paso.

Restablecimiento paso a paso de la contraseña

Cómo habilitar el restablecimiento de la contraseña	Componente de software a utilizar
<p>1. Tarea administrativa: Configurar los datos de restablecimiento de la contraseña para todos los usuarios.</p> <p> Este paso puede imponerse por medio de la política <i>Imponer la configuración del restablecimiento de la contraseña.</i></p>	<p>Si Security Platform aún no está inicializada:</p> <p>Configuración por medio del Asistente de inicialización rápida</p> <p>Aquí se configura automáticamente el Restablecimiento de la contraseña con los valores predeterminados.</p> <p>Configuración por medio del Asistente de inicialización de Security Platform</p> <p>Para configurar la Reconfiguración de la contraseña siga los pasos mencionados:</p> <ul style="list-style-type: none">• Ejecute Herramienta de Configuración Infineon Security Platform. En la página de Bienvenida del Asistente para la inicialización rápida, seleccione Inicialización avanzada.• Durante el Asistente para la inicialización, tilde la casilla de verificación Reconfiguración de la contraseña y haga clic en Siguiente.• Seleccione la opción Crear una nueva tarjeta de seguridad.• Seleccione la ubicación de su preferencia para guardar el archivo de la Tarjeta de seguridad de reconfiguración de la contraseña (nombre de archivo

predeterminado:

SPPwdResetToken.xml).

Medios de almacenamiento

aceptables: Medios extraíbles o disco de red mapeado.

- Configure una nueva contraseña para la tarjeta de seguridad y haga clic en **Siguiente**.
- Confirme las configuraciones y haga clic en **Siguiente**.
- En la pantalla de finalización, haga clic en **Finalizar**.

Si Security Platform ya se encuentra inicializado: [Herramienta de Configuración - Restablecer contraseña - Configurar...](#)

Para configurar la Reconfiguración de la contraseña siga los pasos mencionados:

- Ejecute Infineon Security Platform Settings Tool y seleccione **Reconfiguración de la contraseña**.
 - Clic en **Configurar...**
 - Seleccione la opción **Crear una nueva tarjeta de seguridad**.
 - Seleccione la ubicación de su preferencia para guardar el archivo de la Tarjeta de seguridad de reconfiguración de la contraseña (nombre de archivo predeterminado: **SPPwdResetToken.xml**).
- Medios de almacenamiento aceptables:** Medios extraíbles o disco de red mapeado.
- Configure una nueva contraseña

para la tarjeta de seguridad y haga clic en **Siguiente**.

- Confirme las configuraciones y haga clic en **Siguiente**.
- En la pantalla de finalización, haga clic en **Finalizar**.

2. Tarea de usuario: Habilitar la funcionalidad de restablecimiento para el usuario actual.



Este paso puede imponerse por medio de la política [*Imponer la habilitación del restablecimiento de la contraseña*](#).

Si el usuario aún no se encuentra inicializado: [*Asistente para la inicialización de usuario*](#)

Para habilitar la Reconfiguración de la contraseña y crear un nuevo Secreto personal para el usuario, siga los pasos mencionados:

- Ejecute Herramienta de Configuración Infineon Security Platform. En la página de Bienvenida del Asistente para la inicialización rápida, seleccione **Inicialización avanzada**.
- Durante el asistente para la inicialización de usuarios, tilde la casilla de verificación **Habilitar la reconfiguración de mi Contraseña de usuario básico en caso de una emergencia**.
- Seleccione una ubicación en el disco rígido para guardar el archivo del Secreto personal (nombre de archivo predeterminado: **SPPwdResetSecret.xml**). Haga clic en **Siguiente**.
- Confirme las configuraciones y haga clic en **Siguiente**.
- Las funciones de Security Platform pueden configurarse más adelante. Destilde todas las

opciones y haga clic en **Siguiente**.

- En la pantalla de finalización, haga clic en **Finalizar**.

Si el usuario ya se encuentra inicializado: [Herramienta de Configuración - Restablecer contraseña - Habilitar...](#)

Para crear un nuevo Secreto personal para el usuario actual, siga los pasos mencionados:

- Ejecute Infineon Security Platform Settings Tool y seleccione **Reconfiguración de la contraseña**.
- Clic en **Habilitar...** Aparece un mensaje informativo. Lea cuidadosamente este mensaje y haga clic en **OK**.
- Seleccione una ubicación en el disco rígido para guardar el archivo del Secreto personal (nombre de archivo predeterminado: **SPPwdResetSecret.xml**).
- Cuando se le pregunte **¿Desea reemplazarlo?**, haga clic en **Sí**.
- Autentifíquese y haga clic en **Siguiente**.
- Confirme las configuraciones y haga clic en **Siguiente**.
- En la pantalla de finalización, haga clic en **Finalizar**.

Cómo restablecer una contraseña de usuario

Componente de software a utilizar

3. Tarea administrativa: Preparar el

[Herramienta de Configuración -](#)

restablecimiento de la contraseña para un usuario específico, o preparar y restablecer la cuenta de administrador actual en un sólo paso.

[Restablecer contraseña - Preparar...](#)
(comienza el asistente para el restablecimiento de la contraseña)

Para crear el Código de autorización para la reconfiguración de la contraseña para un usuario determinado, siga los pasos mencionados:

- Ejecute Infineon Security Platform Settings Tool y seleccione **Reconfiguración de la contraseña**.
- Clic en **Preparar...**
- Seleccione de la lista al usuario determinado cuya contraseña deba reconfigurarse y haga clic en **Siguiente**.
- Busque la ubicación del archivo de la tarjeta de seguridad para la reconfiguración de la contraseña (nombre de archivo predeterminado: **SPPwdResetToken.xml**), e ingrese la contraseña de protección para ese archivo. Haga clic en **Siguiente**.
- Seleccione la ubicación (por ej. unidad de red mapeada o carpeta compartida en el disco rígido) para guardar el Código de autorización de reconfiguración de la contraseña (nombre de archivo predeterminado: **SPPwdResetCode.xml**), para que el usuario pueda tener acceso al mismo. Haga clic en **Siguiente**.
- En la pantalla de finalización,

haga clic en **Finalizar**.

Para preparar y reconfigurar la Contraseña de usuario básico para el administrador actual, siga los pasos mencionados:

- Ejecute Infineon Security Platform Settings Tool y seleccione **Reconfiguración de la contraseña**.
- Clic en **Preparar...**
- Seleccione al administrador cuya contraseña deba reconfigurarse y haga clic en **Siguiente**.
- Busque la ubicación del archivo de la tarjeta de seguridad para la reconfiguración de la contraseña (nombre de archivo predeterminado: **SPPwdResetToken.xml**), e ingrese la contraseña de protección para ese archivo. Haga clic en **Siguiente**.
- Busque la ubicación del archivo de Secreto personal (nombre de archivo predeterminado: **SPPwdResetSecret.xml**) y haga clic en **Siguiente**.
- Ingrese y confirme la nueva Contraseña de usuario básico y haga clic en **Siguiente**.
- Confirme las configuraciones y haga clic en **Siguiente**.
- En la pantalla de finalización, haga clic en **Finalizar**.

4. Tarea de usuario: Restablecer la contraseña para el usuario actual (sólo es posible si ya está preparado el

[Herramienta de Configuración - Restablecer contraseña - Restablecer...](#) (comienza el asistente

restablecimiento de la contraseña para este usuario).

para el restablecimiento de la contraseña)

Para reconfigurar la Contraseña de usuario básico para el usuario actual, siga los pasos mencionados:

- Ejecute Infineon Security Platform Settings Tool y seleccione **Reconfiguración de la contraseña**.
- Clic en **Reconfigurar...**
- Busque la ubicación del archivo de Secreto personal (nombre de archivo predeterminado: **SPPwdResetSecret.xml**).
- Seleccione la ubicación del archivo de Código de autorización para la reconfiguración de la contraseña (nombre de archivo predeterminado: **SPPwdResetCode.xml**) y haga clic en **Siguiente**.
- Ingrese y confirme la nueva Contraseña de usuario básico y haga clic en **Siguiente**.
- Confirme las configuraciones y haga clic en **Siguiente**.
- En la pantalla de finalización, haga clic en **Finalizar**.



Solución Infineon Security Platform

Defensa contra el ataque de diccionario



Notas:

- Este tema es de importancia sólo para los Security Platforms con un Trusted Platform Module 1.2. Los detalles del mecanismo de defensa ante ataques por diccionario de Security Platform son sólo válidos para los Security Platforms con un Infineon Trusted Platform Module 1.2.
- Este tema va dirigido especialmente hacia los propietarios de Security Platform.

Un **ataque de diccionario** es un método que se utiliza para producir brechas en los sistemas de seguridad, en especial en aquellos sistemas basados en contraseñas. Con este método el atacante prueba sistemáticamente todas las contraseñas posibles comenzando por aquellas palabras que tienen una gran probabilidad de ser utilizadas, como ser nombres o lugares. Se utiliza la palabra "diccionario" ya que el atacante utiliza las palabras existentes en uno de ellos para intentar descubrir la contraseña. Los ataques de diccionario se realizan por lo general por medio de un software ahorrando el tiempo que lleva el ingreso manual de cada contraseña.

Un ataque de diccionario contra la Solución Security Platform puede tener como objetivo detectar la [contraseña de propietario](#), una contraseña de usuario [básico o claves protegidas por contraseña](#) . Un ataque de diccionario contra una contraseña también se llama **ataque de contraseña**. Por medio del estándar TCG 1.2 se introdujo un mecanismo de protección contra los ataques de diccionario. Solución Security Platform hace uso de este mecanismo. Tenga presente que las medidas de defensa no sólo se toman ante un ataque real sino también frente a ingresos accidentales de contraseña fallidos.

Cómo evitar los ataques de diccionario

Tenga en cuenta las siguientes recomendaciones para evitar los ataques de diccionario:

- Siga los consejos generales sobre seguridad tal como se comunican en los portales relacionados con el tema.
- Establezca valores de límite pequeños para los ataques de diccionario (vea la política [Configurar límite para ataque de diccionario](#)).
- Utilice contraseñas complejas para evitar que un atacante las descubra.

Cómo reaccionar ante un ataque de diccionario

Si Security Platform informa de un ataque de diccionario tenga presente las siguientes recomendaciones:

- Para empezar, deje su sistema deshabilitado temporalmente.
- Desconecte su sistema de la red.
- Busque información adicional en el Visor de Eventos de Microsoft.
- Busque información sobre las últimas amenazas de seguridad en diferentes portales que traten el tema.
- Rastree y elimine la aplicación o el servicio que realizó el ataque. Considere la posibilidad de ponerse en contacto con un especialista en seguridad para que lo asista.
- Tome medidas de seguridad para bloquear futuros intentos de ataque (por ejemplo, instale parches de seguridad, configure un firewall y las políticas de seguridad).

Finalmente, puede conectar nuevamente su sistema a la red. Debe reiniciar su sistema para habilitar Security Platform.

[Medida de defensa contra el ataque de diccionario](#)

[Interfaz de usuario para el ataque de diccionario](#)

Technologies AG



La solución Infineon Security Platform

Medidas de defensa contra el ataque de diccionario



Notas:

- Este tema es de importancia sólo para los Security Platform con un Trusted Platform Module 1.2. Los detalles del mecanismo de defensa ante ataques por diccionario de Security Platform son sólo válidos para los Security Platforms con un Infineon Trusted Platform Module 1.2.
- Este tema va dirigido especialmente hacia los propietarios de Security Platform.

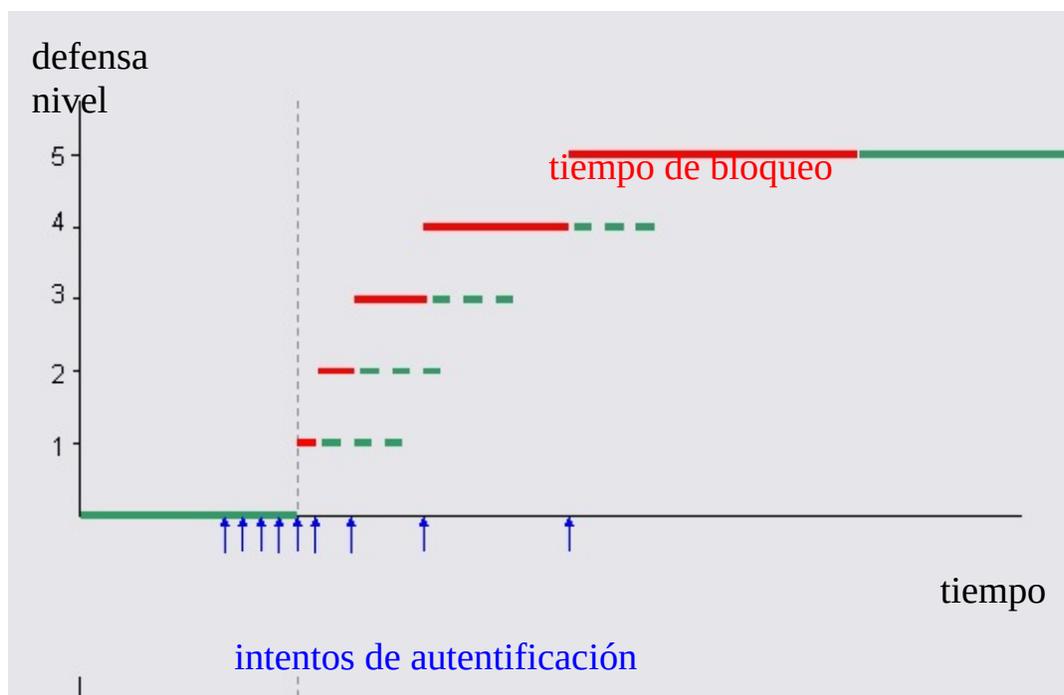
La Solución Security Platform rechaza los ataques de diccionario por medio de las siguientes medidas:

- Al detectar múltiples intentos de autenticación fallidos, Security Platform se **deshabilita temporalmente** hasta el próximo reinicio del sistema. De esta manera el propietario de Security Platform puede tomar medidas contra el ataque antes de volver a habilitar Security Platform.
- Además, se activa un **tiempo de bloqueo** : Por un determinado período de tiempo se rechazan los intentos de autenticación. Con cada nuevo intento de autenticación fallido se incrementa el **nivel de defensa** con lo que el tiempo de bloqueo se duplica.
- Si dentro de un determinado tiempo no se detectan nuevos intentos fallidos de autenticación, el nivel de defensa disminuye nuevamente.
- El nivel de defensa se puede **restablecer** a través del propietario de Security Platform.

Las siguientes imágenes ilustran estas medidas.

El nivel de defensa aumenta con los subsiguientes intentos fallidos de autenticación

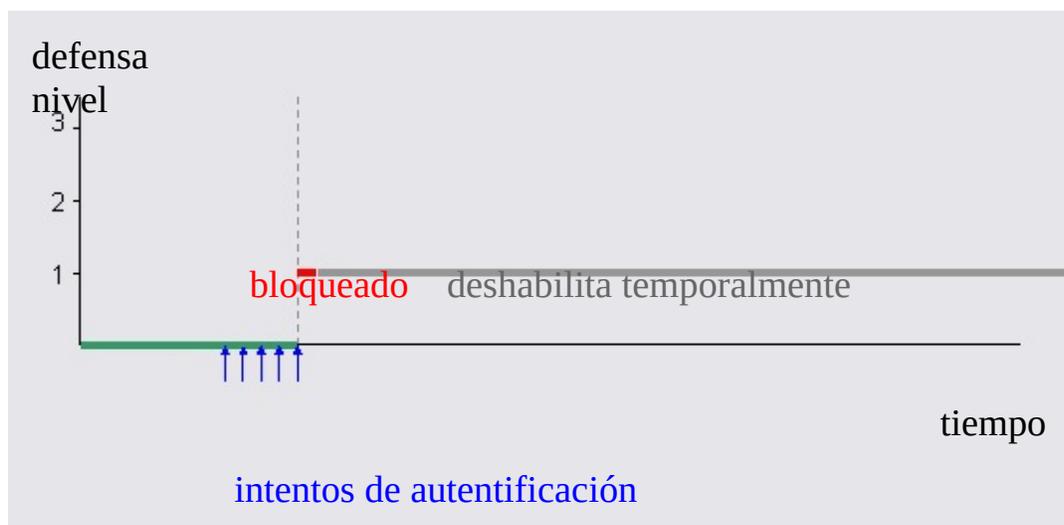
Esta imagen ilustra el caso en que un intento fallido produce un incremento en el nivel de defensa y del tiempo de bloqueo, si no se deshabilitara el Security Platform.



En este ejemplo se ilustra el quinto intento como límite para la defensa. El atacante intenta autenticarse continuamente. Así, aumenta el nivel de defensa tan pronto como termina el tiempo de bloqueo actual.

Aquí se muestra cómo se evita el incremento del nivel de defensa al deshabilitar temporalmente el Security Platform.

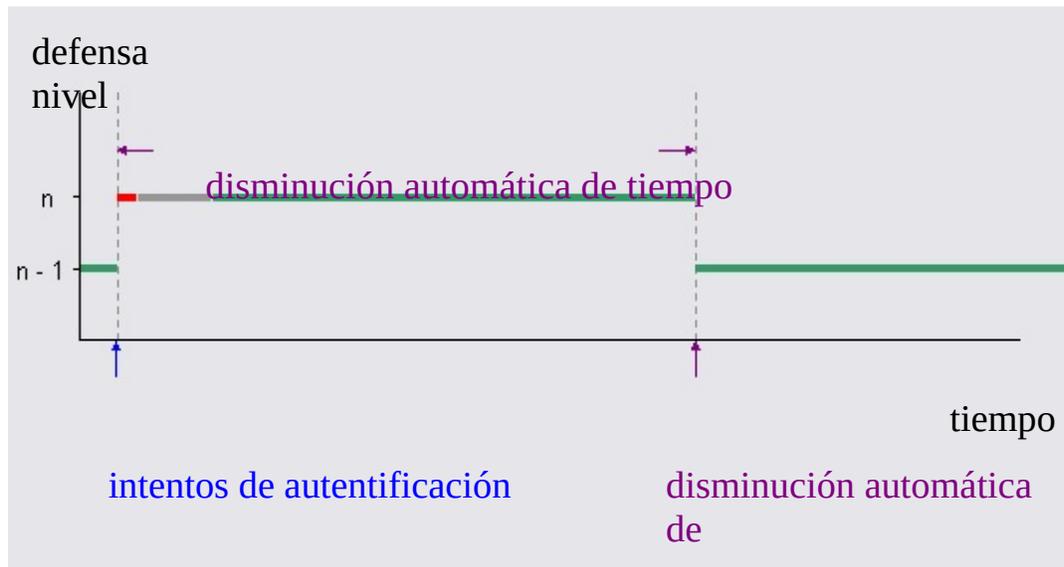
Para bloquear los ataques en una fase temprana y evitar prolongados períodos de tiempo de bloqueo, se deshabilita temporalmente el Security Platform tan pronto como se excede el límite para la defensa.



En este ejemplo, el Security Platform ya no puede recibir ataques, incluso si se termina el tiempo de bloqueo. Security Platform se habilitará nuevamente sólo después del próximo reinicio del sistema.

Disminución automática del nivel de defensa

Aquí se ilustra de qué manera el nivel de defensa disminuye nuevamente luego de un período de tiempo, siempre y cuando no existan nuevos intentos fallidos de autenticación.



Aquí se puede ver el incremento del nivel de defensa y del tiempo de bloqueo (en rojo) que causa un intento de autenticación fallido. Aquí se supone que se reinicia el sistema luego de un corto período de tiempo (en gris). Al transcurrir el tiempo de autodisminución, disminuye automáticamente el nivel de defensa. Observe que para los niveles de defensa bajos el tiempo de autodisminución es mucho mayor que el tiempo de bloqueo.

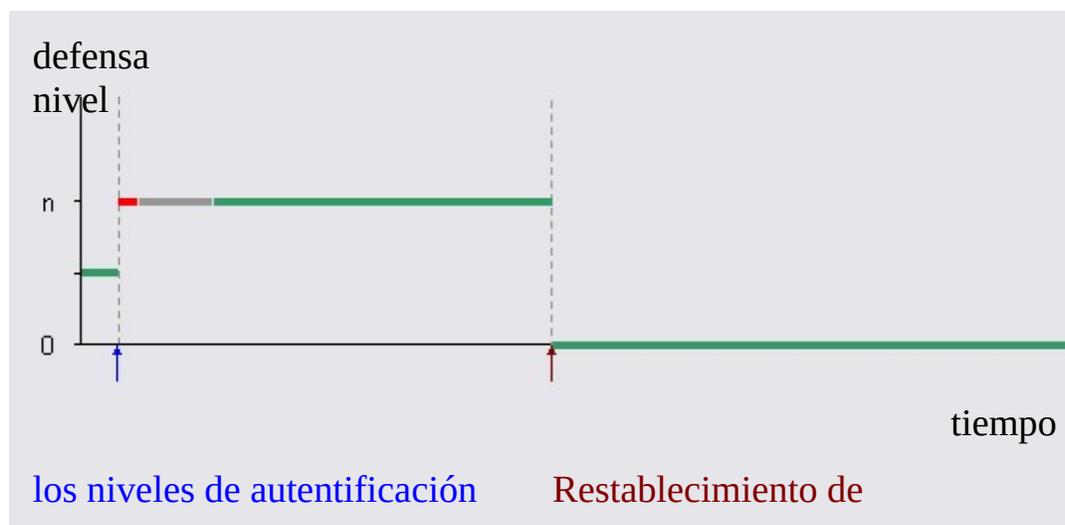


Notas:

- El tiempo de autodisminución es independiente del tiempo de bloqueo y del reinicio del sistema.
- La autodisminución no requiere de un reinicio del sistema.
- Para los bajos niveles de defensa el tiempo de autodisminución es mucho mayor que el tiempo de bloqueo.

Restablecimiento del nivel de defensa

En esta imagen se observa el nivel de defensa que logró el propietario de Security Platform.



Como en la imagen anterior, se puede observar el incremento del nivel de defensa, el tiempo de bloqueo (**en rojo**) y el sistema que se deshabilita temporalmente hasta el próximo reinicio del sistema (**en gris**). Aquí se asume que el propietario de Security Platform restablece el nivel de defensa ya que no desea esperar que disminuya automáticamente el nivel del mismo.

Parámetros de defensa de un típico ataque de diccionario

La siguiente tabla muestra algunos parámetros de defensa de un típico ataque de diccionario para los Infineon Trusted Platform Module. Los valores enumerados pueden ser distintos a los de su propio Trusted Platform Module.

Intentos permitidos para la autenticación de claves (por ejemplo, los utilizados para la autenticación del usuario de Security Platform)	5	Se toman medidas de defensa contra un ataque de diccionario luego de 5 intentos fallidos dentro de las 6 horas (vea la política Configurar el límite para el ataque de diccionario y Configurar valores de defensa de ataques por diccionario).
Intentos permitidos de autenticación para el propietario de Security Platform	3	Se toman medidas de defensa contra un ataque de diccionario luego de 3 intentos fallidos dentro de las 6 horas (vea la política Configurar el límite para el ataque de diccionario y Configurar valores de defensa de ataques por diccionario).
Intentos permitidos para la autenticación de datos (por ejemplo, los utilizados por Windows BitLocker en combinación con PIN)	10	Se toman medidas de defensa de ataques por diccionario luego de 10 intentos fallidos en un plazo de 6 horas (ver la política Configurar el límite para el ataque de diccionario y Configurar los valores de defensa de ataques por diccionario).
Tiempo de bloqueo mínimo	~10 s	Tiempo de bloqueo inicial luego de que el límite se excede en 10 segundos.
Tiempo de bloqueo máximo	~24 h	El tiempo de bloqueo máximo es de 24 horas. Este límite se puede alcanzar con menos de 15 intentos fallidos de autenticación luego de exceder el límite.
Tiempo de disminución automática del nivel de	~6 h	Luego de 6 horas de haber alcanzado un cierto nivel de defensa, éste disminuye en 1

defensa

automáticamente.

Tenga presente que esto se aplica sólo si no hubieron intentos fallidos de autenticación dentro de las 6 horas. De esta forma se aumenta en 1 el nivel de defensa.

Esta configuración resulta en un alto nivel de seguridad en caso de un ataque real de diccionario. Por otro lado los ingresos accidentales de contraseñas incorrectas se manejan de una forma flexible y práctica para el usuario.



El tiempo de bloqueo y el nivel de defensa disminuyen automáticamente el tiempo sólo en los sistemas que se encuentran en ejecución.



©Infineon Technologies AG

Solución Infineon Security Platform

Interface de usuario para el ataque de diccionario



Notas:

- Este tema es de importancia sólo para los Security Platform con un Trusted Platform Module 1.2. Los detalles del mecanismo de defensa ante ataques por diccionario de Security Platform son sólo válidos para los Security Platforms con un Infineon Trusted Platform Module 1.2.
- Este tema va dirigido especialmente hacia los propietarios de Security Platform.

Tanto el propietario de Security Platform como el administrador son responsables de la configuración y de las medidas de defensa a tomar contra un ataque de diccionario. Si se presenta el caso de un ingreso incorrecto de una contraseña o de un ataque real se informa debidamente al usuario de Security Platform.

La siguiente lista enumera las partes de la interfaz de usuario que se relacionan con el ataque de diccionario:

Configuración del límite para el ataque de diccionario

Tanto el propietario de Security Platform como un administrador autorizado pueden establecer la cantidad de intentos fallidos que se permiten antes de que se tomen medidas de defensa contra el ataque de diccionario. Se puede realizar por medio de la [configuración de las funciones de Security Platform](#) o por medio de la política [Configurar el umbral de ataques por diccionario](#).

Restablecimiento del nivel de defensa

Modo stand-alone:

El propietario de Security Platform puede [restablecer](#) el nivel de defensa por medio de la Herramienta de [configuraciones - Avanzado - Restablecer...](#) Se inicia el Asistente para la inicialización de Security Platform *SpTPMWz.exe* con el parámetro de línea de comando - *resetattack*.



Para llevar a cabo esta operación se requiere la contraseña de propietario. Se puede escribir la Contraseña de propietario o suministrar un Archivo de copia de seguridad con la contraseña de propietario. Asegúrese de

suministrar la contraseña correcta. Luego de varios intentos fallidos al ingresar la contraseña de propietario su Security Platform se bloqueará temporalmente. En ese momento ya no podrá restablecer el nivel de defensa para el ataque de diccionario.

Modo servidor:

Trusted Computing Management Server provee un modo seguro y eficiente controlado por el servidor para restablecer el nivel de defensa de ataques por diccionario:

- La funcionalidad de restablecimiento del nivel de defensa puede configurarse y administrarse sin la presencia local de administradores o sin conocimiento de las contraseñas de propietario.
- Cualquier la plataforma Trust Domain puede inicializar el restablecimiento del nivel de defensa de manera remota desde cualquier computadora con conexión el servidor Trust Domain.



Si el administrador conoce la contraseña de propietario, el nivel de defensa también se puede restablecer de manera local iniciando el asistente para la inicialización de Security Platform *SpTPMWz.exe* con el parámetro de línea de comando *-resetattack* o */resetattack*. Este es el único uso permitido del asistente para la inicialización de Security Platform en modo servidor.

Notificaciones y advertencias

Estos son **mensajes** que explican el estado actual, y en las siguientes situaciones se muestran las medidas de defensa:

- Autenticación fallida (para el propietario de Security Platform y usuarios de Security Platform)
- Exceso del límite del ataque de diccionario
- Intento de autenticación durante un bloqueo

No caso de um ataque de dicionário real (que no sea causa de una autenticación accidental fallida) se muestra un **mensaje de error**.



©Infineon Technologies AG

La Solución Infineon Security Platform

Configurar los valores de defensa de ataques por diccionario

Por medio de esta página podrá configurar la cantidad de intentos de autenticación que deben permitirse para los diversos tipos de autenticación antes de que se tomen medidas de defensa de ataques por diccionario.



Notas:

- Este tópico sólo es relevante para las Security Platforms con Trusted Platform Module 1.2. Los detalles del mecanismo de defensa de ataques por diccionario de Security Platform sólo son válidos para Security Platforms con Infineon Trusted Platform Module 1.2.
- Este tópico está dirigido principalmente al propietario de Security Platform.



Disponibilidad de la página:

- Esta página del asistente sólo se encuentra disponible si la [política Configurar el umbral de ataques por diccionario](#) no está configurada.

La siguiente tabla le muestra algunos consejos sobre cómo utilizar la página del asistente.

Elementos de la página	Explicación
<input type="radio"/> <i>Contadores de autenticación específicos</i>	Seleccione esta opción si desea especificar la cantidad de intentos permitidos para cada tipo de autenticación por separado.
<input checked="" type="checkbox"/> <i>Sólo los contadores relevantes de Security Platform</i>	Seleccione esta opción si sólo desea configurar los tipos de autenticación que son relevantes para la solución Security Platform. En tal caso sólo aparecerán en pantalla los siguientes tipos de autenticación: <ul style="list-style-type: none">• Autenticación del propietario• Autenticación de clave (por ejemplo, la utilizada para la autenticación del usuario de Security Platform)

	<ul style="list-style-type: none"> • Autenticación de datos (por ejemplo, la utilizada por Windows BitLocker en combinación con PIN) <p>Libere esta opción si también quiere configurar otros tipos de autenticación que no sean relevantes para la Solución Security Platform. Para tener información detallada sobre estos tipos de autenticación, revise las especificaciones de Trusted Computing Group (TCG) y de su proveedor de Trusted Platform Module. Advierta que las medidas del diccionario para defensas frente ataques, son tomadas cuando se supera el número de intentos permitidos para un cierto contador, tanto si el tipo correspondiente de autenticación es relevante para Security Platform o no.</p>
<input type="radio"/> <i>Contador de autenticación global</i>	<p>Seleccione esta opción si desea especificar un contador de autenticación global para todos los tipos de autenticación. Cualquier autenticación fallida incrementará este contador, independientemente del tipo de autenticación.</p>
<input type="checkbox"/> <i>Tipos de autenticación</i>	<p>Esta lista enumera todos los tipos de autenticación con los valores mínimos, máximos y los actualmente configurados para la cantidad de intentos de autenticación permitidos. Cambie la cantidad de intentos permitidos a su criterio. Asegúrese de ingresar sólo datos enteros dentro del rango permitido desde mínimo a máximo.</p>
<input checked="" type="checkbox"/> <i>Deshabilitar temporalmente la plataforma</i>	<p>Seleccione esta opción si desea que las medidas de defensa incluyan la deshabilitación temporal de Security Platform.</p>



Solución Infineon Security Platform

Medidas de defensa contra el ataque de diccionario



Notas:

- Este tema es de importancia sólo para los Security Platform con un Trusted Platform Module 1.2. Los detalles del mecanismo de defensa ante ataques por diccionario de Security Platform son sólo válidos para los Security Platforms con un Infineon Trusted Platform Module 1.2.
- Este tema va dirigido especialmente hacia los propietarios de Security Platform.

El restablecimiento del nivel de defensa comienza por mostrar información sobre el estado del ataque de diccionario. Luego se solicita la contraseña de propietario de Security Platform.

Pasos para el restablecimiento del nivel de defensa

Paso	Comentario
1. Información de estado del ataque de diccionario	<p>Esta página proporciona la siguiente información detallada que se necesita para decidir si el nivel de defensa debe ser reiniciado o no:</p> <p>Estado de ataques por diccionario general: Indica si las medidas de defensa de ataques por diccionario se encuentran actualmente en vigencia o no.</p> <p>Tiempo de bloqueo restante: Muestra en pantalla el tiempo restante si un bloqueo se encuentra actualmente en vigencia.</p> <p>Lista de tipos de autenticación: Muestra en pantalla la información de estado para varios tipos de autenticación, por ejemplo los tipos de autenticación para las claves (como los utilizados para la autenticación del usuario de Security Platform), el propietario y para el acceso a los datos sellados (por ejemplo, los utilizados por Windows BitLocker en combinación con PIN).</p> <p>Aparece en pantalla la siguiente información para cada tipo de autenticación:</p> <ul style="list-style-type: none">• Intentos permitidos: Cantidad de intentos de autenticación permitidos para Trusted Platform Module antes de que se tomen medidas de defensa de ataques por diccionario (ver Interfaz del usuario para ataques por diccionario, sección "Configurar el umbral de ataques por diccionario").• Contador actual: Cantidad de intentos fallidos actualmente vigentes.• Siguiente tiempo de bloqueo: Indica el tiempo de bloqueo después de la siguiente autenticación fallida si el contador actual ya se encuentra por encima de la cantidad de intentos permitidos. De lo contrario indica el tiempo de bloqueo cuando se está por exceder el umbral. <p>El contador actual y el siguiente tiempo de bloqueo dependen de</p>

	<p>la cantidad de intentos permitidos, de la cantidad total de anteriores autenticaciones fallidas y del tiempo transcurrido desde la última autenticación fallida (ver disminución automática del nivel de defensa).</p> <p>Actualizar: Haga clic sobre este botón o presione la tecla "F5" para actualizar la información de estado de los ataques por diccionario.</p> <p>Mostrar los tipos de autenticación no críticos: En el modo predeterminado sólo aparecen en pantalla los tipos de autenticación con contadores actuales superiores a cero. Tilde esta opción para mostrar además en pantalla los tipos de autenticación con contador actual en cero.</p> <p> Observe que la información de estado del ataque de diccionario se muestra solamente si se puede recuperar del Trusted Platform Module.</p>
<p>2. Suministrar la contraseña de propietario de Security Platform</p>	<p>Se requiere la contraseña de propietario para restablecer el nivel de defensa. Se puede escribir la Contraseña de propietario o se puede suministrar un Archivo de copia de seguridad con la contraseña de propietario.</p> <p> Por favor asegúrese de proporcionar la contraseña correcta. De lo contrario se pueden tomar medidas de defensa contra un ataque de diccionario. De ser así, ya no podrá restablecer el nivel de defensa del ataque de diccionario.</p>



La Solución Infineon Security Platform

Herramientas de la solución de Infineon Security Platform



Existen diferentes comportamientos de las herramientas de la solución Security Platform en el [modo servidor](#).

El Software de la Solución de Infineon Security Platform provee las siguientes herramientas administrativas:

Herramienta de la Solución de Security Platform	Propósito
Herramienta de Configuración de Security Platform	<ul style="list-style-type: none">• Entrega información variada del Trusted Platform Module de su sistema.• Lleva a cabo diversas tareas administrativas. <p>Este componente es designado como un applet en el panel de control. Esto suministra un punto de acceso para la administración de Infineon Security Platform.</p>
Asistente para la inicialización rápida de Security Platform	<ul style="list-style-type: none">• Configure rápidamente Infineon Security Platform y Usuario (recomendado para la mayoría de los usuarios).
Asistente para la inicialización de Security Platform	<ul style="list-style-type: none">• Configura su Infineon Security Platform (para usuarios expertos).
Asistente para la inicialización de usuarios de Security Platform	<ul style="list-style-type: none">• Configura los usuarios de su Infineon Security Platform (para usuarios expertos).
Asistente para la migración de Security Platform	<ul style="list-style-type: none">• Migra los certificados y las claves de usuario de Infineon Security Platform desde una Infineon Security Platform hacia otra en un canal preservando la privacidad y la seguridad.
Asistente para la copia	<ul style="list-style-type: none">• Realiza copias de seguridad o restaura la

de seguridad de Security Platform	información relativa a las operaciones de Security Platform.
Asistente de restablecimiento de la contraseña de Security Platform	<ul style="list-style-type: none"> • Restablece las contraseñas de usuario básico.
Asistente para la importación de Security Platform PKCS #12	<ul style="list-style-type: none"> • Importa archivos de intercambio de información personal dentro de Security Platform.
Visor de certificados y selección de certificados de Security Platform	<ul style="list-style-type: none"> • Administración de certificados.
Icono de Notificación de la Barra de tareas de Security Platform	<ul style="list-style-type: none"> • Llevar a cabo tareas administrativas de Security Platform y obtener información de estado.
Administración de políticas de Security Platform	<ul style="list-style-type: none"> • Administra las políticas de sistema y políticas de usuario de Infineon Security Platform.
Servicios de integración de Security Platform	<ul style="list-style-type: none"> • Habilita las aplicaciones estándares para utilizar la funcionalidad de Trusted Platform Module.
Servicios de Security Platform	<ul style="list-style-type: none"> • Provee una pila de software funcional de Trusted Computing Group (TCG).

La Solución Infineon Security Platform

Uso de los asistentes de Security Platform

La solución Security Platform utiliza la herramienta de configuraciones como punto central de acceso para administrar Infineon Security Platform. Los asistentes facilitan las tareas de configuraciones iniciales y posteriores.

Páginas del asistente

Página de bienvenida

Esta es la primer página del asistente. Le explica el propósito del asistente. Esta página es mostrada solo si se necesita la funcionalidad completa del asistente. Esta no es mostrada si el asistente es iniciado desde la herramienta de configuraciones para realizar una tarea de administración definida.

Páginas interiores del asistente

Estas páginas lo consultan sobre el ingreso del usuario para recolectar información requerida para realizar las tareas del asistente.

Página de confirmación

La página de confirmación realiza un sumario de toda la información relevante y las acciones a llevar a cabo.



Hasta el momento, no se han realizado cambios. Las acciones listadas serán realizadas solo si hace clic en **Siguiente**.

Página de finalización

Esta es la última página del asistente. Esto lo informa sobre la finalización del asistente (fallada o exitosa) y lista todas las acciones que han sido completadas.

Si el proceso de configuración completo requiere iniciar otro asistente antes de poder utilizar las características de Security Platform, puede entonces seleccionar continuar automáticamente con el próximo asistente.

Ejemplo: Luego de haber inicializado o restaurado su Security Platform (Asistente para la inicialización de plataforma), usted puede querer continuar con la inicialización o restauración de los usuarios (Asistente para la inicialización de usuarios).

En la página de finalización del **Asistente para la inicialización de Security Platform**, puede decidir si desea realizar [copias de seguridad automáticas](#) para actualizar el archivo de copias de seguridad del sistema con los cambios significativos. Esta opción sólo está disponible si no está configurada la política [Implementar copias de seguridad del sistema](#)

inmediatamente.

Indicación de progreso del asistente

El Indicador de progreso del asistente, ubicado en la esquina superior derecha de la página del asistente, permite visualizar los pasos requeridos del asistente y resalta el paso actual. El Indicador de progreso del asistente es soportado por todos los Asistentes que tengan múltiples páginas y pasos de configuración. Le informa acerca de los pasos a ser realizados para llevar a cabo ciertas tareas:

- Cada paso es representado por un pequeño rectángulo.
- El rectángulo iluminado representa el paso actual.
- Mueva el puntero del ratón por encima de los rectángulos para ver información sobre los pasos individuales.

Comportamiento del asistente en caso de falla

En caso de falla los cambios que se intentaban realizar a Security Platform no se llevan a cabo. En lugar de esto, será mostrado un mensaje de error.

Condiciones previas generales para ejecutar asistentes

Precondición	Explicación
Derechos administrativos y políticas de Windows.	<p>Asistente para la inicialización de Security Platform/Asistente para la inicialización rápida de Security Platform (si la plataforma todavía no ha sido inicializada):</p> <p>El usuario actual debe tener derechos administrativos en Windows (por ejemplo, el usuario actual debe ser miembro del grupo administradores).</p> <p>En un sistema con Trusted Platform Module deshabilitado, el usuario actual debe estar habilitado para reiniciar la computadora.</p>
Políticas de Security Platform	<p>El acceso a los asistentes de Security Platform puede ser restringido por las políticas Permiso de registración de plataforma y Permiso de registración de usuario.</p>
Estado del usuario	<p>Asistente para el restablecimiento de la contraseña, asistente de importación PKCS #12 :</p> <p>El usuario actual debe ser un usuario de Security Platform inicializado.</p>
Estado de Security Platform & Trusted Platform Module	<p>Asistente de inicialización de Security Platform :</p> <p>Las causas posibles de errores son:</p> <ul style="list-style-type: none">• La propiedad de Infineon Security Platform ha cambiado luego de la instalación de Security Platform.• El Trusted Platform Module tiene un propietario, pero Infineon Security Platform no está instalado aún. No puede realizarse una instalación en esta situación. <p>Todos los asistentes:</p> <p>Requieren una conexión a Trusted Platform Module. Las posibles causas de error son:</p> <ul style="list-style-type: none">• Trusted Platform Module deshabilitado o deshabilitado temporalmente.• Un Trusted Platform Module faltante.• Problemas con el software del controlador

	 Información detallada sobre el estado de Infineon Security Platform está disponible Aquí .
Consistencia en la configuración común	Todos los asistentes: La configuración de Security Platform debe estar en un estado consistente. Ejemplos de posibles causas de error son: <ul style="list-style-type: none">• Opciones de configuración del archivo de copia de seguridad inválidas.• La tarjeta de seguridad de recuperación de emergencia o la tarjeta de seguridad del restablecimiento de contraseña no puede ser creada.



La Solución Infineon Security Platform

Cuadros de diálogo de la contraseña y de autenticación de usuario básico

La administración de Security Platform y el uso de sus características requieren de su autenticación en el Security Platform. El cuadro de diálogo de autenticación depende del modo de autenticación que se utilice y de la acción que requiera su autenticación.

- [Introducción](#)
- [Políticas de la contraseña de usuario básico y complejidad de las contraseñas](#)
- [Cuadros de diálogo requeridos para el uso de las Funciones de Security Platform](#)
- [Cuadros de diálogo requeridos para la administración de Security Platform](#) -
[Configuración de la contraseña de usuario básico](#)
 - [Modificación de la contraseña de usuario básico](#)
 - [Verificación de la contraseña de usuario básico](#)

Introducción

La siguiente tabla muestra los distintos tipos de las contraseñas y cuadros de diálogo de autenticación que aparecen en diferentes circunstancias.

Tipo de acción	Acciones requeridas del usuario	Ejemplos de soluciones Security Platform
Establecer una contraseña de usuario básico	<p>Modo de autenticación de la contraseña:</p> <ul style="list-style-type: none">• Ingrese y confirme su contraseña. <p>Modo de autenticación avanzado:</p> <ul style="list-style-type: none">• Ingrese y confirme la contraseña.• Inserte el dispositivo de autenticación e ingrese el PIN (o realice alguna otra acción dependiendo del dispositivo de autenticación , por ejemplo, coloque su dedo en el lector de huellas digitales)	<ul style="list-style-type: none">• Inicialización de usuarios (Asistente para la inicialización rápida o Asistente para la inicialización de usuarios)• Restablecimiento de la contraseña (Herramienta de Configuración - Restablecimiento de la contraseña - Restablecer...)
Cambiar la contraseña de usuario básico	<p>Modo de autenticación de la contraseña:</p> <ul style="list-style-type: none">• Ingrese su antigua contraseña.• Ingrese y confirme su nueva contraseña. <p>Modo de autenticación avanzado:</p> <ul style="list-style-type: none">• Inserte el dispositivo de autenticación e ingrese	<ul style="list-style-type: none">• Cambio de la contraseña (Herramienta de Configuración - Restablecimiento de la contraseña - Cambiar...)

	<p>el PIN (o realice alguna otra acción dependiendo del dispositivo de autenticación , por ejemplo, coloque su dedo en el lector de huellas digitales)</p> <ul style="list-style-type: none"> • Ingrese y confirme su nueva frase de contraseña. 	
<p>Verificar la contraseña de usuario básico</p>	<p>Modo de autenticación de la contraseña:</p> <ul style="list-style-type: none"> • Ingrese su contraseña. <p>Modo de autenticación avanzado:</p> <ul style="list-style-type: none"> • Inserte el dispositivo de autenticación e ingrese el PIN (o realice alguna otra acción dependiendo del dispositivo de autenticación, e.j. coloque su dedo en el lector de huellas digitales). <p>O, si prefiere no utilizar su dispositivo de autenticación avanzada, puede ingresar su frase de contraseña.</p>	<ul style="list-style-type: none"> • La autenticación del usuario requiere del uso de las Funciones de Security Platform (por ejemplo, encriptación de archivos o e-mail seguro) • Habilite el restablecimiento de las contraseñas (Herramienta de Configuración - Restablecimiento de la contraseña - Habilitar...) • Exporte el archivo de migración (Herramienta de Configuración - Migración - Exportar...) • Importe archivo de migración (Herramienta de Configuración - Migración - Importar...) • Restablezca las credenciales de usuario (Herramienta de Configuración - Copia de seguridad - Restaurar...)



Políticas de la contraseña de usuario básico y complejidad de las contraseñas

En la sección [manejo de las contraseñas](#) hay información disponible sobre las políticas y la complejidad de las contraseñas.

Cuadros de diálogo requeridos para el uso de las Funciones de Security Platform

La siguiente tabla explica los cuadros de diálogo requeridos para el uso de las Funciones de Security Platform (como ser: encriptación de archivos o e-mail seguro)

Autenticación de contraseña	
<input type="password"/> <i>Contraseña de usuario básico</i>	Ingrese su contraseña de usuario básico actual.
<input checked="" type="checkbox"/> <i>Recordar la contraseña para todas las aplicaciones</i>	Tilde esta casilla de verificación para prevenir pedidos múltiples de autenticación causadas por diferentes aplicaciones por medio de las Funciones de Security Platform.
<input type="checkbox"/> <i>Detalles...</i>	Haga clic aquí para obtener detalles sobre la aplicación que solicita su autenticación al Security Platform.
Autenticación avanzada con frase de contraseña	
<input type="password"/> <i>Frase de la contraseña de usuario básico</i>	Ingrese su frase de la contraseña de usuario básica actual.
<input type="checkbox"/> <i>Autenticación</i>	Si quiere utilizar su dispositivo de autenticación en lugar de ingresar su frase de contraseña, cambie el método de autenticación.
<input checked="" type="checkbox"/> <i>Ocultar escritura</i>	Si desea ver la frase de la contraseña ingresada, desmarque esta casilla de verificación.
<input checked="" type="checkbox"/> <i>Recordar la frase de la contraseña</i>	Tilde esta casilla de verificación para prevenir pedidos múltiples de autenticación causadas por diferentes aplicaciones por medio de las Funciones de Security

<i>para todas las aplicaciones</i>	Platform.
<input type="checkbox"/> <i>Detalles...</i>	Haga clic aquí para obtener detalles sobre la aplicación que solicita su autenticación al Security Platform.
Autenticación avanzada con tarjeta inteligente o tarjeta de seguridad USB segura	
<input checked="" type="checkbox"/> <i>PIN</i>	Inserte su tarjeta inteligente o la tarjeta de seguridad USB segura. Ingrese su PIN.
<input type="checkbox"/> <i>Autenticación</i>	Si quiere utilizar su frase de la contraseña en lugar de ingresar su dispositivo de autenticación, desmarque esta casilla de verificación.
<input checked="" type="checkbox"/> <i>Recordar el PIN para todas las aplicaciones</i>	Tilde esta casilla de verificación para prevenir pedidos múltiples de autenticación causadas por diferentes aplicaciones por medio de las Funciones de Security Platform.
<input type="checkbox"/> <i>Detalles...</i>	Haga clic aquí para obtener detalles sobre la aplicación que solicita su autenticación al Security Platform.
Autenticación avanzada con otro dispositivo de autenticación	
<input type="checkbox"/> <i>Auto-autenticación</i>	Utilice su dispositivo de autenticación avanzada para autenticarse (por ejemplo, coloque su dedo en el lector de huellas digitales)  Para más información, consulte la ayuda en línea de su plug-in de Autenticación avanzada.

<input type="checkbox"/> <i>Autenticación</i>	Si quiere utilizar su frase de la contraseña en lugar de ingresar su dispositivo de autenticación, desmarque esta casilla de verificación.
<input checked="" type="checkbox"/> <i>Recordar para todas las aplicaciones</i>	Tilde esta casilla de verificación para prevenir pedidos múltiples de autenticación causadas por diferentes aplicaciones por medio de las Funciones de Security Platform.
<input type="checkbox"/> <i>Detalles...</i>	Haga clic aquí para obtener detalles sobre la aplicación que solicita su autenticación al Security Platform.



Cuadros de diálogo requeridos para la administración de Security Platform

Las siguientes tablas explican las contraseñas de usuario básico y los cuadros de diálogo de autenticación requeridos para la administración de Security Platform.

Establecimiento de la contraseña de usuario básico (inicialización de usuarios, restablecimiento de la contraseña)

Autenticación de contraseña	
<input type="password"/> <i>Contraseña</i>	Ingrese una contraseña de acuerdo a la configuración de la política de las contraseñas . Esta contraseña será su nueva contraseña de usuario básico.
<input type="password"/> <i>Confirme la contraseña</i>	Ingrese la contraseña nuevamente para confirmarla.
Autenticación avanzada con tarjeta inteligente o tarjeta de seguridad USB segura	
<input type="password"/> <i>Frase de la contraseña</i>	Ingrese una frase de la contraseña de acuerdo a la configuración de la política de las contraseñas . Esta frase de la contraseña será su nueva frase de la contraseña de usuario básico.
<input type="password"/> <i>Confirme la frase de la contraseña</i>	Ingrese la frase de la contraseña nuevamente para confirmarla.
<input type="password"/> <i>PIN</i>	Inserte su tarjeta inteligente o la tarjeta de seguridad USB segura. Ingrese su PIN.

Autenticación avanzada con otro dispositivo de autenticación	
☒ <i>Frase de la contraseña</i>	Ingrese una frase de la contraseña de acuerdo a la configuración de la política de las contraseñas . Esta frase de la contraseña será su nueva frase de la contraseña de usuario básico.
☒ <i>Confirme la frase de la contraseña</i>	Ingrese la frase de la contraseña nuevamente para confirmarla.
☒ <i>Auto-autenticación</i>	Utilice su dispositivo de autenticación avanzada para autenticarse (por ejemplo, coloque su dedo en el lector de huellas digitales)  Para más información, consulte la ayuda en línea de su plug-in de Autenticación avanzada.



Cambiar la contraseña de usuario básico

Autenticación de contraseña	
☒ <i>Contraseña anterior</i>	Ingrese su contraseña de usuario básico actual.
☒ <i>Nueva contraseña</i>	Ingrese una contraseña de acuerdo a la configuración de la política de las contraseñas . Esta contraseña será su nueva contraseña de usuario básico.
☒ <i>Confirme la nueva contraseña</i>	Ingrese la nueva contraseña una vez más para confirmarla.
Autenticación avanzada con tarjeta	

inteligente o tarjeta de seguridad USB segura	
 <i>PIN</i>	Inserte su tarjeta inteligente o la tarjeta de seguridad USB segura. Ingrese su PIN.
 <i>Nueva frase de la contraseña</i>	Ingrese una frase de la contraseña de acuerdo a la configuración de la política de las contraseñas . Esta frase de la contraseña será su nueva frase de la contraseña de usuario básico.
 <i>Confirme la nueva frase de la contraseña</i>	Ingrese la frase de la contraseña nuevamente para confirmarla.
Autenticación avanzada con otro dispositivo de autenticación	
 <i>Nueva frase de la contraseña</i>	Ingrese una frase de la contraseña de acuerdo a la configuración de la política de las contraseñas . Esta frase de la contraseña será su nueva frase de la contraseña de usuario básico.
 <i>Confirme la nueva frase de la contraseña</i>	Ingrese la frase de la contraseña nuevamente para confirmarla.
 <i>Auto-autenticación</i>	Utilice su dispositivo de autenticación avanzada para autenticarse (por ejemplo, coloque su dedo en el lector de huellas digitales)  Para más información, consulte la ayuda en línea de su plug-in de autenticación avanzada.



Verificación de la contraseña de usuario básico (habilitar el restablecimiento de la contraseña, exportar/importar el paquete de archivos de migración, restaurar las credenciales del usuario)

Autenticación de contraseña	
<input type="password"/> <i>Contraseña</i>	Ingrese su contraseña de usuario básico actual.
Autenticación mejorada	
<input checked="" type="radio"/> <i>Dispositivo de autenticación</i> <input type="radio"/> <i>Frase de contraseña</i>	Especifique si desea utilizar su dispositivo de autenticación o ingrese su frase de contraseña.
Autenticación avanzada con frase de contraseña	
<input type="password"/> <i>Frase de la contraseña</i>	Ingrese su frase de la contraseña de usuario básica actual.
Autenticación avanzada con tarjeta inteligente o tarjeta de seguridad USB segura	
<input type="password"/> <i>PIN</i>	Inserte su tarjeta inteligente o la tarjeta de seguridad USB segura. Ingrese su PIN.
Autenticación avanzada con otro dispositivo de	

autenticación

Auto- autenticación

Utilice su dispositivo de autenticación avanzada para autenticarse (por ejemplo, coloque su dedo en el lector de huellas digitales)

 Para más información, consulte la ayuda en línea de su plug-in de autenticación avanzada.



©Infineon Technologies AG

La Solución Infineon Security Platform

Manejo de las contraseñas

Contraseñas utilizadas en la Solución Security Platform

La Solución Infineon Security Platform utiliza muchas contraseñas diferentes. Algunas son para los administradores de Security Platform y otras para los usuarios. Asegúrese de no mezclar las diferentes contraseñas.



En el [modo servidor](#), las contraseñas administrativas y los códigos de autorización de restablecimiento no son válidos ya que Trusted Computing Management Server se encarga de la tarea de preparar y proveer estas contraseñas.

La tabla a continuación le ofrece una introducción a las contraseñas de Security Platform y sus usos.

Contraseña	Utilizado por...	Objetivo/Explicación
Contraseña de propietario	Administrador	Se establece durante la inicialización de Security Platform y es un requisito para realizar las cruciales tareas administrativas de Security Platform. Se puede establecer de forma manual o se puede crear una Contraseña de propietario aleatoria. Se puede guardar en un Archivo de copia de seguridad con la contraseña de propietario, el cual puede ser utilizado para la autenticación de la Contraseña de propietario (en vez de escribir la Contraseña de propietario). Este archivo es compatible con el Archivo de copia de seguridad con contraseña de propietario generado por la aplicación "Trusted Platform Module (TPM) Management" de Microsoft.
Contraseña de la tarjeta de seguridad	Administrador	Protege la tarjeta de seguridad para la recuperación de emergencia, necesaria

para la recuperación de emergencia		para realizar dicha tarea de recuperación.
Contraseña de la tarjeta de seguridad para el restablecimiento de contraseña	Administrador	Protege la tarjeta de seguridad para el restablecimiento de la contraseña necesaria cuando el usuario debe cambiar su contraseña de usuario básico .
Contraseña de usuario básico (también conocido como "Contraseña" en el modo de autenticación mejorado o llamado "Frase de contraseña de Usuario básico")	Usuario	<p>Protege la clave de usuario básico necesaria para acceder a los datos específicos del usuario de Infineon Security Platform. Por ejemplo, no se puede utilizar ninguna función de Infineon Security Platform sin esta contraseña.</p> <p>La contraseña de usuario básico también es necesaria para restaurar y migrar los datos de usuario y configurar ciertos valores de configuración del mismo. Se puede restablecer, si tanto el administrador como el usuario configuraron esta característica.</p> <p>En el modo de Autenticación avanzada esta contraseña se reemplaza por la "frase de contraseña", que se encuentra protegida por el dispositivo de autenticación.</p> <p> Esta es la contraseña principal del Usuario de Security Platform . A modo de simplificación, a menudo se lo llama "contraseña".</p>
Contraseña PKCS #12	Usuario	Protege la clave privada del usuario que se encuentra almacenada en el archivo PKCS #12.
Restablecer el	Usuario	Esta cadena de código no es una

código de autorización

contraseña en realidad, pero bastante similar desde el punto de vista del usuario. Se crea automáticamente durante la preparación de un restablecimiento de contraseña de usuario. Se requiere para restablecer una contraseña de usuario básico.

Consejos generales con respecto a las contraseñas

- Utilice diferentes contraseñas para propósitos diferentes. Específicamente, no vuelva a utilizar su contraseña de Windows. Si vuelve a utilizar su contraseña de Windows para todas las contraseñas relacionadas con Security Platform, el avanzado nivel de seguridad basado en el hardware ya no será efectivo. Un intruso que sepa su Contraseña de Windows podría acceder a sus datos de EFS y PSD, utilizar sus credenciales para identificación y autorización y además podría alterar las configuraciones de Security Platform.
- Se recomienda el uso de caracteres especiales para mejorar la calidad de las contraseñas. Sin embargo, debe recordar que algunos caracteres cambian su posición en el teclado dependiendo de la configuración local. Algunos caracteres pueden incluso no estar disponibles dependiendo del idioma. También, algunos caracteres pueden no estar permitidos dentro de las contraseñas dependiendo de su sistema operativo y de otros componentes de software.
- Evite utilizar contraseñas que se puedan encontrar en diccionarios, incluso al combinar tales palabras para construir una contraseña.
- Al agregar dígitos y utilizar mayúsculas mejora la calidad de la contraseña.
- La longitud mínima y máxima de una contraseña normalmente permanece sin cambios una vez que se configura el sistema. Por lo tanto la apariencia de la contraseña puede variar entre diferentes sistemas. Sin embargo, los aspectos generales se mantienen para cada instalación del software.
- No es posible copiar el contenido de los campos de contraseña para evitar ataques espías a las contraseñas.

Complejidad de la contraseña

La siguiente tabla contiene una introducción sobre los requerimientos de complejidad de la contraseña:

Requerimientos de complejidad de la contraseña

Se requieren caracteres de 3 de las siguientes 4 categorías:

- Caracteres en mayúsculas en inglés (**A a Z**)
- Caracteres en minúsculas en inglés (**a a z**)
- Dígitos en base 10 (**0 a 9**)
- Caracteres no alfanuméricos (por ejemplo, **!, \$, #, %**)

Políticas de la contraseña del propietario y complejidad de la contraseña

Hay requerimientos especiales en cuanto a la longitud y complejidad de la contraseña del propietario. La siguiente tabla hace una introducción a la configuración de políticas de las contraseñas predeterminadas:

Longitud mínima predeterminada	6 caracteres
Se requiere complejidad en la contraseña	No

Políticas de contraseña de usuario básica y complejidad de las mismas

Existen requerimientos especiales con respecto a la longitud y complejidad de las contraseñas de usuario básica. La siguiente tabla hace una introducción a la configuración de políticas de las contraseñas predeterminadas:

	Autenticación de las contraseñas - no se utiliza ningún dispositivo de autenticación	Autenticación avanzada - el dispositivo de autenticación protege la frase de contraseña
Longitud mínima predeterminada	6 caracteres	20 caracteres
Se requiere complejidad en la contraseña	No	No

Su administrador puede cambiar esta configuración. Se encuentran disponibles más detalles acerca de las Políticas de las contraseñas de usuario básico en las [Políticas de usuario](#) de la descripción de Infineon Security Platform.



Pídale a su administrador las políticas para su contraseña de usuario básico actual, si sus derechos de acceso no le permiten ver o configurar las políticas de las contraseñas.



Las opciones dentro del campo de contraseña pueden ser restringidas dependiendo de la política del sistema [Habilitar seguridad severa en el campo de contraseña](#).



La solución Infineon Security Platform - Herramienta de configuración

Herramienta de configuración de Infineon Security Platform

Con la Herramienta de Configuración de Security Platform puede obtener información variada sobre el Trusted Platform Module de su sistema. También puede realizar diversas tareas administrativas. Este componente está diseñado como un applet en el panel de control. Esto suministra un punto de acceso para la administración de Infineon Security Platform.

La siguiente tabla muestra las páginas de la Herramienta de Configuración:

Página	Explicación
Información	<ul style="list-style-type: none">• Determina las configuraciones más importantes de Infineon Security Platform
Configuración de usuario	<ul style="list-style-type: none">• Cambiar la contraseña de usuario básico• Configura las funciones específicas del usuario de Security Platform.• Administra los certificados de Security Platform• Deshabilita temporalmente el Security Platform
Copia de seguridad	<ul style="list-style-type: none">• Configura copias de seguridad automáticas (tarea administrativa)• Realiza copias de seguridad manuales y restauraciones.• Crea dispositivos de autenticación de copias de seguridad <p> En el modo servidor, las copias de seguridad y las restauraciones son llevadas a cabo por Trusted Computing Management Server. Si se ha configurado el Personal Secure Drive (PSD) se pueden realizar Restauraciones y Copias de seguridad manuales de esta unidad.</p>
Migración	<ul style="list-style-type: none">• Exporta claves y certificados de usuario de Security Platform• Importa claves y certificados de usuario de Security Platform <p> Esta página no está disponible en el modo servidor, ya que la migración de las claves y certificados específicos del</p>

	<p>usuario es llevada a cabo por el Trusted Computing Management Server, es decir, usted no tiene que realizar esta tarea.</p>
<p>Restablecimiento de la contraseña</p>	<ul style="list-style-type: none"> • Realiza la configuración para todos los usuarios (tarea administrativa) • Habilita el usuario actual • Prepara el restablecimiento de la contraseña para un usuario determinado (tarea administrativa) • Restablece la contraseña de usuario básico para el usuario actual <p> En el modo servidor, Trusted Computing Management Server realiza las tareas de configuración, habilitación y preparación de los códigos de autorización de restablecimiento de la contraseña, ni el administrador ni el usuario tienen que realizar esta tarea. Por lo tanto, todas las opciones están deshabilitadas, excepto la opción <i>Restablecer</i>.</p>
<p>BitLocker</p>	<ul style="list-style-type: none"> • Utilice el cifrado de unidad BitLocker junto con el Trusted Platform Module para encriptar datos en su disco <p> • Esta página sólo está disponible si el Sistema Operativo soporta la encriptación de unidad BitLocker (p. ej. para las ediciones Enterprise y Ultimate de Windows 7 y Windows Vista), y si el usuario actual tiene derechos de administración.</p> <ul style="list-style-type: none"> • Esta página no está disponible en el modo servidor. Sin embargo puede configurar BitLocker a través del Applet del Panel de Control de Microsoft BitLocker.
<p>Avanzado</p>	<ul style="list-style-type: none"> • Cambiar la contraseña de propietario • Configura funciones específicas de la plataforma de Security Platform • Deshabilita/habilita Security Platform • Configura las políticas de Security Platform

- Restablezca el nivel de defensa de ataques por diccionario



- Esta página es visible sólo si el usuario actual tiene derechos de administración.
- Esta página no está disponible en el [modo servidor](#), ya que el Trusted Computing Management Server realiza la tarea de configuración de las políticas y características de Security Platform.

Inicio de la aplicación

- **Administrar Security Platform**

Iniciar la herramienta de configuración del [icono de notificación de la barra de tareas](#).



Bajo sistemas operativos con control de cuentas de usuario (como Windows 7 y Windows Vista) la herramienta de configuración se inicia sin privilegios elevados.

-  **Administrar Security Platform**

Iniciar la herramienta de configuración del [icono de notificación de la barra de tareas](#) con privilegios elevados.



Disponible sólo para usuarios con derechos administrativos bajo sistemas operativos con control de cuentas de usuarios (como Windows 7 y Windows Vista).



La Solución Infineon Security Platform - Herramienta de configuración

Información sobre Infineon Security Platform

Esta página muestra las configuraciones más importantes de Infineon Security Platform.

Si el Infineon Security Platform se encuentra deshabilitado, la información disponible será limitada.

La tabla a continuación describe toda la información y funciones.

Elementos de la página	Explicación
 <i>La solución Security Platform</i>	Versión del producto de la solución Security Platform y modo de funcionamiento del usuario actualmente registrado.
 <i>Estado de Security Platform</i>	Los estados modo de operación, usuario, propietario y chip se describen en la Introducción al estado de Security Platform .
 <i>Trusted Platform Module</i>	Fabricante y versión de hardware y firmware de Trusted Platform Module.
 <i>Autocomprobación</i>	Haga clic aquí para verificar la funcionalidad del Trusted Platform Module. A continuación se mostrará el resultado.
 <i>Más detalles...</i>	Haga clic aquí para obtener información detallada sobre la configuración de Infineon Security Platform.



La Solución Infineon Security Platform - Herramienta de Configuración

Más detalles

Este diálogo lista la información del sistema más significativa. Esta información incluye:

- Versión del producto
- [Modo de operación](#)
- [Estado de Security Platform](#)
- Información de componentes
- Información de soporte avanzadas

Puede guardar esta información en un archivo:

Botón	Explicación
<input type="checkbox"/> <i>Guardar...</i>	<p>La información de diagnóstico se puede almacenar en un archivo para su análisis fuera de línea. Se abre un cuadro de diálogo de selección de archivos donde puede seleccionar la unidad y carpeta de destino y en donde debe definir el nombre del archivo.</p> <p>El formato del archivo de diagnóstico de Security Platform es el formato de texto estándar (extensión *.txt). De esta forma el archivo se puede visualizar en una gran variedad de aplicaciones.</p>



©Infineon

Technologies AG

La solución Infineon Security Platform - Herramienta de configuración

Estado de Security Platform

El estado actual de la Infineon Security Platform está definido por el estado actual de los siguientes cuatro componentes:

Estado Chip (Estado Trusted Platform Module)

Proporciona información sobre el estado general del Trusted Platform Module. Pueden ocurrir los siguientes estados:

- **Habilitado** - El Trusted Platform Module está accesible y en uso por el Software de Infineon Security Platform.
- **Desabilitado** - El uso de Trusted Platform Module se encuentra bloqueado. Puede lograrse mediante una configuración en la BIOS del sistema o una configuración en el software de Infineon Security Platform.
Posible solución: Si el Trusted Platform Module está deshabilitado en la BIOS, vea su documentación de la BIOS del sistema. De lo contrario [habilite](#) el Trusted Platform Module en el software Infineon Security Platform.
- **Temporalmente deshabilitado** - El Trusted Platform Module está accesible, pero su uso se encuentra bloqueado hasta tanto no se reinicie el sistema. Las características de seguridad que utilizan al chip no están disponibles.
Posible solución: [Habilite](#) el Trusted Platform Module en el software Infineon Security Platform y reinicie el sistema.

Estado Propietario

Proporciona información sobre el estado general de la Infineon Security Platform. Pueden ocurrir los siguientes estados:

- **No inicializado** - El Infineon Security Platform aún no se inicializó y no se ha quitado la posesión del mismo, o el estado de inicialización es incompatible (por ejemplo, causado por una interrupción debida a la pérdida de energía).
Posible solución: Inicialice Security Platform con el [Asistente para la inicialización rápida de Security Platform](#) o con el [Asistente para la inicialización de Security Platform](#).
- **Inicializado** - Se llevaron a cabo las operaciones de configuración básicas, el Trusted Platform Module está operativo y se tomó posesión del Infineon Security Platform. Ya existe un propietario de Infineon Security Platform en Trusted Platform Module.
- **Inicializado pero con cambios** - Se tomó posesión del Infineon Security Platform, pero después de esta operación se cambió el propietario de Infineon Security Platform. La administración de Security Platform lo indica como estado del propietario **Inicializado (Modo 1)**.
Posible solución: Ejecute el [Asistente para la inicialización de Security Platform](#) y siga las indicaciones en pantalla.
- **TPM inicializada, Security Platform no inicializada** - En versiones anteriores Software de la Solución de Infineon Security Platform, el nombre era "**Initialized other OS**" (Otro sistema operativo inicializado).
Escenario 1: En el sistema operativo Windows 7, una circunstancia posible es que el Trusted Platform Module haya sido inicializado con la aplicación de Microsoft [administración del Módulo de plataforma segura \(TPM\)](#), es decir, la propiedad del Trusted Platform Module ha sido tomada pero Infineon Security Platform no ha sido configurada.
Escenario 2: Esto también puede ocurrir en computadoras de plataformas múltiples con diversas versiones de sistemas operativos instaladas, donde la propiedad fue tomada utilizando un sistema y luego se inició un sistema diferente.
En cualquiera de los dos escenarios, la configuración de Infineon Security Platform permanece activa. La administración de Security Platform lo indica como estado del propietario **Inicializado (Modo 2)**.
Posible solución: Ejecute el [Asistente para la inicialización de Security Platform](#) y siga las indicaciones en pantalla.

Estado de usuario

Proporciona información sobre el estado del actualmente anotado en el usuario. Pueden ocurrir los siguientes estados:

- **No inicializado** - El usuario que inició sesión actualmente ya no es un usuario de Infineon Security Platform, o el estado de inicialización del usuario es incompatible (por ejemplo, causado por una interrupción debida a una pérdida de energía).
Posible solución: Inicialice el usuario con el [Asistente para la inicialización rápida de Security Platform](#) o con el [Asistente para la inicialización de usuarios de Security Platform](#).
- **Inicializado** - El usuario que inició sesión actualmente es un usuario válido de Infineon Security Platform. Es decir, se realizó la configuración del usuario que inició sesión actualmente. Se generó una clave de usuario básico y se almacenó en un paquete de archivos de recuperación de emergencia, si es que existe.
- **Inicializado pero con cambios** - Se configuró el usuario de Infineon Security Platform y luego cambió la posesión del Infineon Security Platform. No se puede utilizar la clave de usuario básico de quien inició sesión actualmente, en el Infineon Security Platform. La Administración de Security Platform indica que es un estado de usuario inicializado (**Modo 3**).
Posible solución:
Contacte a su administrador para ejecutar el [Asistente para la inicialización de Security Platform](#) y tilde la opción *Recuperar un Security Platform desde un paquete de archivos de copia de seguridad*. De esta manera las credenciales de usuario se pueden preparar para su restauración desde un paquete de archivos de copia de seguridad creado previamente. Luego inicie sesión con su propia cuenta de usuario y ejecute el [Asistente para la inicialización de usuarios](#). (vea [Restauración paso a paso de los datos de recuperación de emergencia](#)).
Si no se encuentra disponible un paquete de archivos de copia de seguridad, se debe realizar una reinicialización forzada de usuario. Esto se logra ejecutando el [Asistente para la inicialización de usuarios](#) con el parámetro de línea de comando **-forceinit**.



Parámetro de la línea de comandos: **SpUserWz.exe /forceinit** no se encuentra soportado en el [modo servidor](#).

Estado de sesión de usuario

Este estado sólo está disponible en [modo servidor](#).

Los Estados de sesión de usuario controlan el acceso de escritura a las credenciales de usuario y a los valores de configuración. Esto asegura que no haya cambios de conflictos concurrentes de otras plataformas. Un estado de sesión se refiere a un determinado usuario o una determinada plataforma. Puede cambiar el estado de las sesión a través el submenú *Credenciales de usuario/Configuración* en [el menú Taskbar Notification](#). Se usan los siguientes estados:

- **Sólo lectura:** Sin acceso actual a la escritura. El acceso a la escritura es posible cambiando al estado *Lectura/Escritura temporario* o *Lectura/Escritura permanente*, ya que no hay otra plataforma en uno de los dos posibles estados de Lectura/Escritura. Estado predeterminado.
- **Lectura/escritura momentánea:** Estado utilizado implícitamente por Trusted Computing Management Server para el acceso a la escritura. Bloquea los cambios provenientes de otras plataformas. Después del acceso a la escritura, vuelve a establecerse el estado *Sólo lectura*.
- **Lectura/escritura permanente:** Estado introducido específicamente por el usuario a través de la Configuración/Credenciales de Usuario de elemento del menú de notificación de la barra de tareas - Solicitud de copia de trabajo local. Permite que se cambien "offline" las credenciales de usuario y los valores de configuración en una copia de trabajo local. Bloquea los cambios provenientes de otras plataformas. El estado se puede cambiar a *Sólo lectura* a través de *Configuración/Credenciales de Usuario de elemento del menú de notificación de la barra de tareas - Aceptar cambios locales* o *Configuración/Credenciales de Usuario - Descartar cambios locales*.



La Solución Infineon Security Platform - Herramienta de Configuración

Configuraciones del usuario de Infineon Security Platform

Por medio de esta página puede configurar todos los valores de seguridad más importantes para el usuario de Infineon Security Platform que se encuentre en sesión actualmente.



Disponibilidad de la página:

- Esta página sólo se encuentra disponible en un Security Platform inicializado.
- En una Infineon Security Platform que no ha sido configurada aparece una casilla de mensaje informando sobre la situación para así poder iniciar [Asistente para la inicialización rápida](#) . En el [modo servidor](#) no aparece un mensaje mientras Security Platform se inicializa automáticamente si el sistema cliente se encuentra integrado en un Trust Domain con administración centralizada.
- Aparece un mensaje para el usuario que no ha sido inicializado informándolo sobre la situación para poder iniciar [Asistente para la inicialización rápida](#). En el [modo servidor](#) aparece una casilla de mensaje informando sobre la situación sólo si el usuario actual es miembro del Grupo de inscripción de usuarios para así poder iniciar [Asistente para la inicialización rápida](#).

Botones:

- Si el Infineon Security Platform se encuentra deshabilitado, si no está configurado aún o si el usuario en sesión no se inicializó, se deshabilitan los botones.
- La habilitación de algunas funciones depende de su [configuración de la política de usuario](#).

La tabla a continuación describe todas las funciones de configuración del usuario.

Botón	Explicación
<input type="checkbox"/> <i>Cambiar...</i>	Haga clic aquí para cambiar su contraseña de usuario básico. El paquete de archivos que contiene los datos de recuperación de emergencia se actualiza para que se refleje el

	cambio de la contraseña.
<input type="checkbox"/> <i>Configurar...</i>	<p>Haga clic aquí para configurar las siguientes características:</p> <ul style="list-style-type: none"> • Correo electrónico seguro • Encriptación de archivos y carpetas por medio de Encrypting File System (EFS) y Personal Secure Drive (PSD) • Autenticación avanzada <p>Se iniciará el Asistente para la inicialización rápida o el Asistente para la inicialización de usuarios de acuerdo con el estado de configuración de las funciones del usuario.</p>
<input type="checkbox"/> <i>Administrar...</i>	<p>Haga clic aquí para visualizar, importar o borrar los certificados protegidos por Security Platform.</p> <p>Se ejecutará el visor de certificados de Infineon Security Platform.</p>
<input type="checkbox"/> <i>Deshabilitar/ Habilitar...</i>	<p>Se puede realizar la operación respectiva dependiendo del estado actual de Infineon Security Platform. Deshabilitar suspende la funcionalidad del Infineon Security Platform hasta que el sistema vuelva a reiniciarse. Las aplicaciones diseñadas para utilizar el Security Platform ya no tendrán acceso a los datos protegidos por el Trusted Platform Module, incluyendo los datos protegidos por EFS, el Personal Secure Drive y otros. El acceso a los datos protegidos se restaura una vez rehabilitado el Security Platform.</p> <p>Si desea habilitar el Infineon Security Platform se le pedirá que reinicie el sistema.</p> <p>Si la funcionalidad se encuentra bloqueada en la configuración de la política del usuario, este botón se deshabilita. Observe que esta función sólo está disponible en Security Platforms con un Trusted Platform Module 1.2.</p>



La Solución Infineon Security Platform - Herramienta de Configuración

Copia de seguridad de Infineon Security Platform

Por medio de esta página puede crear una copia de seguridad y restaurar las credenciales de Security Platform, la configuración de Security Platform y los Personal Secure Drives.

Si la opción de [Autenticación avanzada](#) está habilitada, también puede crear copias de seguridad de su dispositivo de autenticación.



Botones:

- Los botones para las tareas de administración están deshabilitadas para los usuarios sin derechos de administración.
- Los botones están deshabilitados si las funciones correspondientes no están disponibles en un estado determinado de Security Platform.

La tabla a continuación describe toda las funciones de copia de seguridad y restauración.

Botón	Explicación
<input type="checkbox"/> <i>Configurar...</i>	<p>Haga clic aquí para configurar copias de seguridad automáticas de Security Platform.</p> <p>Se ejecutará el Asistente para la inicialización del Infineon Security Platform.</p> <p> • Esta función sólo está disponible si la cuenta de usuario actual tiene derechos de administración.</p> <p>• En el modo servidor este botón está desactivado ya que las copias de seguridad automáticas son llevadas a cabo por el Trusted Computing Management Server, es decir que aquí no se requiere configuración explícita por parte del usuario.</p>
<input type="checkbox"/> <i>Restaurar todo...</i>	<p>Haga clic aquí para restaurar sus configuraciones y credenciales desde un archivo de copia de seguridad del sistema. Además se puede realizar una Restauración de recuperación de emergencia.</p> <p>También se puede realizar la restauración desde un archivo escrito de modo manual si no tiene un Paquete de archivos de copia de seguridad en el sistema. En tal caso, sólo es posible</p>

la Restauración de recuperación de emergencia si el archivo escrito de modo manual incluye los datos correspondientes. Si tiene copias de seguridad de sus archivos imagen, de Personal Secure Drive, también se las puede restaurar. En tal caso se puede restaurar un archivo imagen para un PSD ya configurado o se puede configurar un nuevo PSD para utilizar este archivo imagen restaurado.

Iniciará la parte de restauración del [Asistente para la copia de seguridad de Infineon Security Platform](#).



- Este botón está deshabilitado si el Infineon Security Platform está deshabilitado o si el usuario no tiene derechos administrativos.
- En el [modo servidor](#) este botón está desactivado ya que las restauraciones desde las copias de seguridad del sistema son llevadas a cabo por el Trusted Computing Management Server, es decir que aquí no se requiere configuración explícita por parte del usuario.

Copia de seguridad...

Haga clic aquí para iniciar una copia de seguridad manual de su configuración y credenciales de Security Platform. Si ha establecido Personal Secure Drives, también puede realizar copias de seguridad para los mismos.

Se ejecutará el [Asistente para copia de seguridad del Infineon Security Platform](#).



- Este botón está deshabilitado si el Infineon Security Platform está deshabilitado o si aun no fue configurado.
- Sólo se pueden realizar copias de seguridad para Personal Secure Drives en el [modo servidor](#). Además de las condiciones arriba mencionadas, este botón está deshabilitado si no tiene configurado su Personal Secure Drive (PSD).

Restaurar...

Haga clic aquí para comenzar una restauración manual del paquete de archivos de configuraciones y credenciales de Security Platform.

Si posee una copia de seguridad de su Personal Secure Drive (PSD), también puede realizar una restauración del mismo. Se ejecutará la parte de restauración del [Asistente para la copia de seguridad del Infineon Security Platform](#).



- Este botón está deshabilitado si el Infineon Security Platform está deshabilitado o si aun no fue configurado.
- En el [modo aislado](#), si cuenta con derechos administrativos, puede realizar restauración de recuperación de emergencia.
- Además de las condiciones mencionadas, en el [modo servidor](#), este botón está deshabilitado si el usuario no está inicializado y si Personal Secure Drive (PSD) no está configurado.

Crear...

Haga clic aquí para crear un dispositivo de autenticación de la copia de seguridad.



Esta característica sólo está disponible si está habilitada la [Autenticación avanzada](#).



La Solución Infineon Security Platform - Herramienta de Configuración

Migración de Infineon Security Platform

La migración involucra la copia y transferencia segura de las credenciales de seguridad del usuario desde una plataforma de origen hasta una de destino. Dependiendo de la configuración actual del sistema, el usuario de Infineon Security Platform puede migrar las claves y certificados de usuario hacia o desde el Infineon Security Platform local.

Esta prestación está cubierta por el asistente para la migración de Infineon Security Platform.



Disponibilidad de la página:

- Esta página sólo se encuentra disponible en un Security Platform inicializado.
- Esta página no está disponible en el [modo servidor](#) ya que la migración de las credenciales de seguridad específicas del usuario desde una plataforma de origen a una plataforma de destino es llevada a cabo por Trusted Computing Management Server, es decir que el administrador o el usuario del sistema cliente local no tienen que realizar esta tarea.

[Migración paso a paso](#)

La tabla a continuación describe toda las funciones de migración.

Botón	Explicación
<input type="checkbox"/> <i>Aprenda más...</i>	Haga clic aquí para visualizar una guía detallada paso a paso para realizar la migración.
<input checked="" type="radio"/> <i>Esta es la plataforma de origen</i>	Tilde esta opción para indicar que desea exportar las credenciales desde este Security Platform. Se pueden llevar a cabo las acciones de la plataforma de origen Exportar... y Autorizar...
<input type="checkbox"/> <i>Exportar...</i>	Exporta las claves y certificados de usuario a la plataforma de destino. Se realiza por medio de la opción de exportación del Asistente para la migración de Infineon Security Platform . El dueño de la plataforma debe autorizar la plataforma de destino previo a la exportación.

	<p> Si se cumple alguna de las siguientes situaciones, este botón se encuentra deshabilitado:</p> <ul style="list-style-type: none"> • El Infineon Security Platform se encuentra deshabilitado. • Infineon Security Platform no se inicializó. • El usuario de Infineon Security Platform aún no se inicializó.
<p><input type="checkbox"/> <i>Autorizar...</i></p>	<p>Cada migración de claves y certificados de usuario desde un Infineon Security Platform a otro requiere de una autorización de migración en el Security Platform de origen por parte del Propietario de Infineon Security Platform. Este botón conduce al cuadro de diálogo de autorización.</p> <p> Si se cumple alguna de las siguientes situaciones, este botón se encuentra deshabilitado:</p> <ul style="list-style-type: none"> • El Infineon Security Platform se encuentra deshabilitado. • Infineon Security Platform no se inicializó. • El usuario actual no posee derechos de administración.
<p><input checked="" type="radio"/> <i>Esta es la plataforma de destino</i></p>	<p>Tilde esta opción para indicar que desea importar las credenciales a este Security Platform. Se pueden llevar a cabo las acciones de la plataforma de destino Importar... y Guardar...</p>
<p><input type="checkbox"/> <i>Importar...</i></p>	<p>Importa las claves y certificados de usuario desde una plataforma de origen. Se realiza por medio de la opción de importación del Asistente para la migración de Infineon Security Platform.</p> <p> Si se cumple alguna de las siguientes situaciones, este botón se encuentra deshabilitado:</p> <ul style="list-style-type: none"> • El Infineon Security Platform se encuentra deshabilitado. • Infineon Security Platform no se inicializó.
<p><input type="checkbox"/> <i>Guardar...</i></p>	<p>La información de migración de un Infineon Security Platform se puede exportar a un archivo, y éste luego se puede importar al Infineon Security Platform de destino. La información de migración se encuentra en un archivo en formato XML. Este es el paso inicial para la migración de claves de usuario.</p>



Si se cumple alguna de las siguientes situaciones, este botón se encuentra deshabilitado:

- Cambió el Propietario de Infineon Security Platform (también se indica en la página de [Información](#)).
- Infineon Security Platform no se encuentra inicializada, pero ya existe un Propietario de Infineon Security Platform.
- Las Teclas del usuario básico del Administrador de Infineon Security Platform que ha iniciado sesión no coinciden con el propietario de Infineon Security Platform
- El Infineon Security Platform se encuentra deshabilitado.



La Solución Infineon Security Platform - Herramienta de Configuración

Restablecimiento de la contraseña de Infineon Security Platform

Esta página provee acceso a todas las tareas necesarias para configurar y llevar a cabo el restablecimiento de las contraseñas de usuario básico.



Disponibilidad de la página:

- En el [modo stand-alone](#), esta página sólo se encuentra disponible en un Security Platform inicializado.

Botones:

- Los botones para las tareas de administración están deshabilitadas para los usuarios sin derechos de administración.
- Los botones están deshabilitados si las funciones correspondientes no están disponibles en un estado determinado de Security Platform: Por ejemplo, si el administrador aún no configuró el restablecimiento de la contraseña, no se puede habilitar ni se puede realizar un restablecimiento de la misma.
- En el [modo servidor](#), el Trusted Computing Management Server realiza la tarea de crear una tarjeta de seguridad para el restablecimiento de la contraseña para todos los usuarios, permitiendo el restablecimiento de la contraseña y preparando y suministrando el código de autorización de restablecimiento de la contraseña para usuarios específicos, es decir, ni el administrador ni el usuario tienen que realizar esta tarea. Por lo tanto, todos los botones están deshabilitados, excepto el botón *Restablecer*.

La siguiente tabla describe todas las funciones para el restablecimiento de la contraseña.

Botón	Explicación
<input type="checkbox"/> <i>Configurar...</i>	Haga clic aquí para crear una tarjeta de seguridad para el restablecimiento de la contraseña para todos los usuarios. Esta acción requiere derechos de administración.
<input type="checkbox"/> <i>Habilitar...</i>	Haga clic aquí para habilitar el restablecimiento de la contraseña para el usuario actual. Sólo es posible si el administrador configuró antes el restablecimiento de la

	contraseña.
<input type="checkbox"/> <i>Preparar...</i>	Haga clic aquí para preparar y proveer el código de autorización para el restablecimiento de la contraseña para un usuario específico. También puede preparar y restablecer su propia cuenta en un sólo paso. Ambas opciones requieren derechos de administración.
<input type="checkbox"/> <i>Restablecer...</i>	Haga clic aquí para restablecer la contraseña de usuario básico para la cuenta de usuario actual. Sólo es posible si se preparó el restablecimiento de la contraseña para la cuenta de usuario actual.



La solución Infineon Security Platform - Herramienta de configuración

BitLocker

En esta página puede utilizar el cifrado de unidad BitLocker junto con el Trusted Platform Module para encriptar datos en su disco. La configuración del BitLocker se realiza por medio del Applet del panel de control de Microsoft BitLocker.



Disponibilidad de la página:

- Esta página sólo está disponible si el Sistema Operativo soporta la encriptación de unidad BitLocker (p. ej. para las ediciones Enterprise y Ultimate de Windows 7 y Windows Vista), y si el usuario actual tiene derechos de administración.
- Esta página no está disponible en el [modo servidor](#).

La tabla a continuación describe las funciones de BitLocker.

Botón	Explicación
 Estado actual...	Estado actual de el cifrado de unidad BitLocker. Estados posibles: <i>Configurado</i> , <i>No configurado</i> , <i>Requiere configuración</i> , <i>Encriptando</i> o <i>Desencriptando</i> .
 Configurar...	Haga clic aquí para iniciar el Applet del panel de control de Microsoft BitLocker.  Este botón se encuentra deshabilitado si Trusted Platform Module no está inicializado.



©Infineon

Technologies AG

La solución Infineon Security Platform - Herramienta de configuración

Configuraciones avanzada de Infineon Security Platform

Por medio de esta página puede configurar todos los valores de políticas y de propietario de Security Platform.

Los cambios que se pueden realizar a las configuraciones se limitan a la computadora local.

La [configuración de la política](#) de Infineon Security Platform se encuentra en el archivo de plantilla de la política de Infineon Security Platform.



Disponibilidad de la página:

- Esta página está disponible sólo si el usuario actual tiene derechos de administración.
- Esta página no está disponible en el [modo servidor](#).

Botones:

- Los botones para la administración del sistema y las políticas del usuario no están disponibles en las ediciones de Windows que no admiten Administración de directivas de grupo como, por ejemplo, las ediciones de Windows Home.
- Los botones están deshabilitados si las funciones correspondientes no están disponibles en un estado determinado de Security Platform.

La tabla a continuación describe todas las funciones avanzadas.

Botón	Explicación
<input type="checkbox"/> <i>Cambiar...</i>	<p>Haga clic aquí para cambiar la contraseña de propietario de Security Platform. (ver Cambie contraseña de propietario).</p> <p> • Esta característica no se encuentra disponible si Infineon Security Platform está deshabilitado o si aún no ha sido inicializado.</p> <p>• En el modo servidor, esta característica no está disponible ya que Security Platform se inicializa automáticamente si el sistema cliente está integrado en un Trust Domain con gestión centralizada.</p>

☐ *Configurar...*

Haga clic aquí para configurar las siguientes características:

- Copia de seguridad automática (incluye recuperación de emergencia)
- Restablecimiento de la contraseña
- Autenticación mejorada
- Defensa de ataques de diccionario

Se ejecutará el [Asistente para la inicialización del Infineon Security Platform](#).



- Esta característica no se encuentra disponible si Infineon Security Platform está deshabilitado o si aún no ha sido inicializado.
- En el [modo servidor](#), esta característica no está disponible ya que Trusted Computing Management Server realiza las tareas de restablecimiento de contraseña y copia de seguridad y restaurar.
- Tenga en cuenta que la función *Defensa de ataques por diccionario* sólo se encuentra disponible en Security Platforms con Infineon Trusted Platform Module 1.2 si la política [Configurar el umbral de ataques por diccionario](#) no se encuentra configurada.

☐ *Deshabilitar/Habilitar...*

Haga clic aquí para deshabilitar o habilitar el Security Platform.

Se puede realizar la operación respectiva dependiendo del estado actual de Infineon Security Platform. Para esta operación se requiere la contraseña de propietario.

Deshabilitar Security Platform: Las aplicaciones diseñadas para utilizar el Security Platform ya no tendrán acceso a los datos protegidos por el Trusted

Platform Module, incluyendo los datos protegidos por EFS, el Personal Secure Drive y otros. El acceso a los datos protegidos se restaura una vez rehabilitado el Security Platform.



En un sistema que soporta el cifrado de unidad BitLocker (por ejemplo, Windows Vista Enterprise o Ultimate), si desactiva el Security Platform mientras BitLocker está activo, el sistema operativo le pedirá que ingrese la contraseña de BitLocker al reiniciar.

Habilitar Security Platform en la BIOS: En algunos estados de la plataforma necesitará habilitar el Security Platform explícitamente en la BIOS. Si se le solicita que reinicie el sistema para que la habilitación sea efectiva y Security Platform no se encuentra habilitado luego del reinicio, deberá habilitar explícitamente el Security Platform en la BIOS (vea [Habilitación del Trusted Platform Module](#)).



- Esta función no se encuentra disponible si Infineon Security Platform está deshabilitado en BIOS.
- Esta función no se encuentra disponible si aún no se ha inicializado Infineon Security Platform.
- En el [modo servidor](#) esta característica no está disponible porque este modo no permite la habilitación/deshabilitación de Trusted Platform Module basada en el propietario.

Restablecer...

Haga clic aquí para [restablecer](#) el nivel de defensa de ataques por diccionario.

Se inicia el Asistente para la inicialización de Security Platform *SpTPMWz.exe* con el parámetro de línea de comando *-resetattack*.



- Este botón sólo se encuentra disponible

	<p>en Security Platforms con un Trusted Platform Module 1.2.</p> <ul style="list-style-type: none">• Éste es el único uso permitido del Asistente para la inicialización de Security Platform en el modo servidor .
<p>■ <i>Sistema...</i></p>	<p>Haga clic aquí para administrar la configuración de las políticas del sistema. Se ejecutará la administración de las políticas del sistema de Infineon Security Platform.</p> <p> • Las políticas no estarán disponibles en ediciones de Windows que no admiten Administración de directivas de grupo como, por ejemplo, las ediciones de Windows Home.</p> <ul style="list-style-type: none">• En el modo servidor esta característica no está disponible ya que no se pretende que el administrador local configure y administre las configuraciones de la política. Las políticas son configuradas en todo el dominio por un administrador de dominios mediante el Trusted Computing Management Server.
<p>■ <i>Usuario...</i></p>	<p>Haga clic aquí para administrar la configuración de las políticas del usuario. Se ejecutará la administración de las políticas del usuario de Infineon Security Platform.</p> <p> • Las políticas no están disponibles en las ediciones de Windows Home.</p> <ul style="list-style-type: none">• En el modo servidor esta característica no está disponible ya que no se pretende que el administrador local configure y administre las configuraciones de la política. Las políticas son configuradas en todo el dominio por un administrador de dominios mediante el Trusted



La solución Infineon Security Platform - Asistente para la copia de seguridad

Cambia la contraseña del propietario

Por medio de este diálogo se podrá cambiar la contraseña de propietario.



Disponibilidad de diálogo:

- Este diálogo sólo se encuentra disponible desde la página *Avanzado* de la Herramienta de configuración.
- Este diálogo no se encuentra disponible en el [modo servidor](#) ya que Trusted Computing Management Server administra las contraseñas de propietario.

Por favor tenga en cuenta los consejos generales con respecto al [manejo de contraseñas](#).

La siguiente tabla le muestra algunos consejos sobre cómo utilizar este diálogo:

Elemento del diálogo	Explicación
<input type="checkbox"/> <i>Contraseña anterior</i>	<p>Ingrese la contraseña de propietario anterior aquí. Se puede escribir la contraseña o se puede suministrar un archivo de copia de seguridad con la contraseña de propietario.</p> <p> Para garantizar el cumplimiento de los principales requerimientos de calidad para la contraseña del propietario ingresada manualmente, debería considerar el conjunto de reglas básicas para el manejo de contraseñas.</p>
<input type="checkbox"/> <i>Desde archivo...</i>	<p>Haga clic aquí para suministrar el archivo de copia de seguridad con la contraseña de propietario si ha guardado su contraseña de propietario en un archivo de copia de seguridad y no desea escribir dicha contraseña.</p>
<input type="checkbox"/> <i>Contraseña nueva</i>	<p>Ingrese la contraseña de propietario nueva aquí. Se puede escribir la contraseña o generar una contraseña aleatoria.</p>
<input type="checkbox"/> <i>Aleatorio</i>	<p>Haga clic aquí para generar una contraseña de propietario aleatoria en vez de escribir una contraseña</p>

	<p>nueva. De este modo se asegurará de utilizar una contraseña segura que cumpla con los requerimientos de complejidad y longitud de contraseñas.</p> <p> Asegúrese de desocultar, imprimir o guardar la contraseña aleatoria antes de cerrar este diálogo.</p>
<input type="checkbox"/> <i>Confirme la contraseña nueva</i>	Ingrese nuevamente la contraseña para confirmar (no es necesario si ha generado una nueva contraseña aleatoria).
<input type="checkbox"/> <i>Para el archivo...</i>	Haga clic aquí para guardar la nueva contraseña de propietario en un archivo de copia de seguridad. Podrá utilizar este archivo para la autenticación del propietario en vez de escribir la contraseña.
<input type="checkbox"/> <i>Impresión...</i>	<p>Haga clic sobre este botón para imprimir la nueva contraseña de propietario.</p> <p> Asegúrese de almacenar la impresión en una ubicación segura.</p>
<input checked="" type="checkbox"/> <i>Ocultar la contraseña</i>	Si desea ver las contraseñas, desilte esta casilla de verificación.

 Tenga en cuenta que debido a la política de [Habilitación de seguridad estricta para campo de contraseña](#) podría no tener permitido cortar, copiar, pegar y ver contraseñas en texto simple.



La solución Infineon Security Platform - Asistente para la inicialización rápida

Asistente para la inicialización rápida de Infineon Security Platform

El asistente de inicialización rápida de Security Platform está diseñado para que la mayoría de los usuarios puedan inicializar rápidamente la Security Platform y el usuario con los valores predeterminados. Estas operaciones son requeridas para habilitar la funcionalidad de Infineon Security Platform y para proveer las bases para todas las actividades futuras en Infineon Security Platform.

Si desea inicializar su Security Platform y el usuario con los valores avanzados, se recomienda que utilice el [Asistente de inicialización de Security Platform](#) y el [Asistente de inicialización del usuario de Security Platform](#).



- Este asistente requiere derechos administrativos, siempre y cuando no se haya inicializado aún Security Platform.
- Si Security Platform ya se encuentra inicializada, el asistente sólo realizará las tareas de configuración específicas del usuario, lo cual no requiere derechos administrativos.
- El uso de este asistente se puede controlar con la [política Control de inicialización rápida](#).
- Los pasos de inicialización de plataforma de este asistente sólo se encuentran disponibles si la [política Permitir inscripción de plataforma](#) se encuentra habilitada con la opción *Permitir Management Provider y asistente*, o si esta política no está configurada (se aplican las mismas condiciones si se inicia el asistente desde el [Ícono de notificación de la barra de tareas](#)). Tenga en cuenta que esta política sólo surte efecto si Security Platform no se inicializa antes.
- Los pasos de inicialización del usuario de este asistente sólo se encuentran disponibles si la [política Permitir inscripción del usuario](#) se encuentra habilitada con la opción *Permitir Management Provider y asistente*, o si esta política no está configurada (se aplican las mismas condiciones si se inicia el asistente desde el [Ícono de notificación de la barra de tareas](#)). Tenga en cuenta que esta política sólo surte efecto para los usuarios que aún no estén inicializados.
- Los pasos de inicialización de plataforma de este asistente no se encuentran disponibles en el [modo servidor](#), ya que Security Platform se inicializa automáticamente si el sistema cliente se

encuentra integrado a un Trust Domain con administración centralizada.

Pasos y páginas del asistente

Página/Paso	Comentario
1. Bienvenida	Selección de inicialización rápida o avanzada.
2. Valores	Configuración de Security Platform específica del usuario: Encriptación del sistema de archivos (EFS), Personal Secure Drive (PSD), Contraseña del usuario básico (si el usuario de Security Platform no se encuentra inicializado).
3. Resumen	Confirmación de valores y de los pasos del asistente requeridos.
4. Finalización	Introducción al estado de finalización del asistente. Acceso al archivo de protocolos y a los datos secretos generados.
5. Archivo de protocolos	Visualizar, imprimir y guardar archivo de protocolos.
6. Datos secretos	Visualizar los datos secretos generados.

Si su Trusted Platform no se encuentra actualmente habilitada, será notificado para que la habilite antes de configurar la plataforma (vea [Habilitación del Trusted Platform Module](#)).

Si su Trusted Platform ya tiene un propietario pero aún no está inicializada en el sistema operativo actual, se requerirá la autenticación de propietario (vea [Contraseña de propietario](#)).

Inicio de la aplicación

Si Security Platform aún no se encuentra inicializado:

Desde el [Ícono de notificación de la barra de tareas](#), haga clic en el elemento del menú [Inicialización de Security Platform](#).

Si Security Platform ya se encuentra inicializada y el usuario actual no está inicializado, o se ha inicializado pero las funciones EFS y PDS no están configuradas:

Desde el [Ícono de notificación de la barra de tareas](#), haga clic en el elemento del menú [Inicialización del usuario de Security Platform](#).



©Infineon Technologies AG

Infineon Security Platform Solution - Asistente para la inicialización rápida

Bienvenidos

Esta página del asistente le pregunta si desea realizar una inicialización rápida o una inicialización avanzada.

Inicialización rápida

La inicialización rápida, recomendada para la mayoría de los usuarios, combina la inicialización de usuario y de plataforma con ubicaciones de archivos de datos predeterminados y configuraciones de funciones predeterminadas. Los pasos específicos de la plataforma se realizan automáticamente sin que el usuario ingrese datos. Se generan automáticamente algunos datos secretos y archivos que se requieren para administración y emergencias.

Almacenamiento de datos secretos y archivos generados automáticamente

Se recomienda la utilización de un medio extraíble (por ejemplo, memoria USB) para almacenar [datos secretos y archivos](#) generados automáticamente. Si no se encuentra disponible ningún medio extraíble, la salida de datos debe ser almacenada en la unidad de disco duro local. Esto requiere protección de datos adicional. En consecuencia, deberá memorizar o guardar datos secretos adicionales que no necesitaría si almacenara los datos en un medio extraíble.

Inicialización avanzada

La inicialización avanzada, recomendada para los usuarios expertos, inicia el [Asistente de inicialización de Security Platform](#) para realizar los pasos de configuración específicos de la plataforma. Con la finalización del asistente se puede continuar con los pasos de configuración específicos del usuario por medio del [Asistente de inicialización del usuario de Security Platform](#). La inicialización avanzada permite la configuración avanzada de los datos secretos, las ubicaciones de archivos de datos y las funciones.

Elija este tipo de inicialización si desea utilizar la [Autenticación avanzada](#) o [BitLocker](#), o si desea crear un [Personal Secure Drive \(PSD\)](#) en un medio extraíble (por ejemplo, memoria USB).



©Infineon Technologies AG

Solución Infineon Security Platform - Asistente para la inicialización rápida

Configuraciones

Por medio de esta página se podrán configurar los valores de Security Platform específicos del usuario.



Disponibilidad de funciones:

- Esta página del asistente sólo se encuentra disponible si la política *Permitir inscripción del usuario* se encuentra habilitada con la opción *Permitir Management Provider y asistente*.
- EFS no se admite en ediciones de Windows Home.
- La configuración de EFS podría estar bloqueada por la política del usuario [Permitir configuración de EFS](#).
- La configuración de PSD podría estar bloqueada por la política del usuario [Permitir configuración de PSD](#).
- Para reconfigurar estas funciones, haga clic en [Herramienta de configuración - Configuraciones del usuario - Configurar...](#)

La siguiente tabla detalla las funciones de Security Platform.

Función	Explicación
<input checked="" type="checkbox"/> <i>Sistema de encriptación de archivos (EFS) basado en hardware</i>	<p>EFS forma parte de la tecnología de seguridad del sistema de archivos NTFS de Microsoft. Por medio de EFS se podrán encriptar archivos y carpetas. La solución Security Platform extiende la seguridad de EFS, protegiendo el acceso a las claves de encriptación de EFS con el Trusted Platform Module.</p> <p>Si tilda esta casilla de verificación el Asistente de inicialización rápida habilitará EFS, creará una carpeta encriptada <i>Documentos\Datos encriptados</i> o <i>Mis documentos\Datos encriptados</i> (dependiendo del sistema operativo), y creará un atajo de escritorio para esta carpeta.</p> <p>Aprenda más acerca de EFS</p>
<input checked="" type="checkbox"/> <i>Personal Secure Drive (PSD)</i>	<p>PSD es una unidad encriptada en su computadora. La misma luce como cualquier otra unidad del disco duro. Se puede acceder a los archivos y carpetas en el PSD como en cualquier otra unidad. La única diferencia es que el contenido del PSD</p>

	<p>está totalmente encriptado y sólo se puede acceder a él después de haber cargado explícitamente el PSD. La carga del PSD requiere la autenticación del usuario. Los datos del PSD se almacenan en el archivo imagen del PSD.</p> <p>Si tilda esta casilla de verificación, el Asistente de inicialización rápida creará un PSD y un atajo de escritorio para este PSD. El archivo de imagen PSD se creará en la partición del sistema, en la carpeta <i>Security Platform</i> (a menos que se fije la ubicación a través de la política de Ubicación de Archivo para Personal Secure Drive).</p> <p>Aprenda más acerca de PSD</p>
<p> <i>Contraseña de usuario básico</i></p>	<p>Por favor establezca la Contraseña de usuario básico que se requiere para utilizar las funciones de Security Platform.</p>

¿Cuándo se utiliza EFS o PSD?

La siguiente tabla realiza una comparación entre EFS y PSD. También provee consejos para cuándo se debe utilizar una u otra función.

Criterio	EFS	PSD
<i>Tipo de encriptación</i>	Con base en archivos y carpetas, es decir, se encriptan carpetas y archivos discretos.	Con base en dispositivos, es decir, se encriptan todos los archivos dentro de la unidad.
<i>Sistemas operativos soportados</i>	Sistemas operativos soportados por la solución Security Platform, excepto las ediciones de Windows Home.	Todos los sistemas operativos soportados por la solución Security Platform.
<i>Acceso y manejo de datos</i>	Siempre visible. Sólo es posible realizar encriptación y desencriptación después de la autenticación del usuario. La encriptación y desencriptación se bloquean después del cierre de sesión desde EFS. Además,	Sólo visible y accesible después de haber cargado explícitamente la unidad (requiere autenticación del usuario). El PSD puede ser explícitamente descargado. Además, se pueden establecer

	se pueden establecer derechos de acceso al sistema de archivos NTFS si desea compartir archivos.	los derechos de acceso al sistema NTFS.
<i>Recuperación de datos</i>	Por medio de Agentes de recuperación EFS.	<ul style="list-style-type: none"> • En sistemas operativos que soportan EFS: Por medio de Agentes de recuperación EFS. • En sistemas operativos que no soportan EFS: Por medio de Agentes de recuperación PSD.
<i>Compartición de datos</i>	Pueden ser compartidos entre múltiples usuarios al añadir el certificado del otro usuario.	Sin compartición de datos, único usuario.
<i>Ubicación de datos</i>	Unidades locales o carpetas Web, sistema de archivos NTFS.	Medios extraíbles o disco duro local.
<i>Copia de seguridad de datos</i>	Por medio de cualquier software o método para realizar copias de seguridad.	Por medio de Copia de seguridad de la solución Security Platform .
<i>Cuándo se utiliza EFS o PSD</i>	Si los datos a ser encriptados se encuentran ubicados en carpetas especiales (por ejemplo, <i>Mis Documentos</i> o carpetas de datos específicos de las aplicaciones.	<ul style="list-style-type: none"> • Si su sistema operativo es una edición de Windows Home y, por tanto, no admite EFS. • Si los datos a ser encriptados se encuentran ubicados en una unidad extraíble que desea utilizar en varias computadoras. En modo servidor, Personal Secure Drive en medios desmontables puede ser recorrido sin interrupciones. En modo independiente es necesario

migrar las credenciales y los valores de configuración, o se puede recuperar o añadir la copia de seguridad del archivo de imagen.

- Si los datos a ser encriptados se encuentran ubicados en un sistema de archivos FAT32.



La solución Infineon Security Platform - Asistente para la inicialización rápida

Resumen

La página del resumen detalla los pasos que serán realizados.

Los pasos requeridos dependen del estado actual del usuario y la plataforma. Por ejemplo, se pasan por alto los pasos específicos de la plataforma en una Security Platform ya inicializada, y sólo se realizan los pasos específicos del usuario.



Tenga en cuenta que la inicialización y configuración de Security Platform podrían tardar un tiempo. La creación de una unidad de PSD grande podría tardar un tiempo considerable.



La solución Infineon Security Platform - Asistente para la inicialización rápida

Finalización

La página de finalización detalla el resultado de todos los pasos de inicialización y configuración. Se puede encontrar información más detallada en el archivo de protocolo del asistente. Haga clic en *Detalles...* para acceder al archivo de protocolo.



El asistente podría haber creado datos secretos dependiendo del estado anterior del usuario y plataforma y de la selección del lugar para almacenar los resultados del asistente. Esto se necesita para administración y emergencias. Específicamente si no ha seleccionado un medio extraíble (por ejemplo, memoria USB) para almacenar los resultados del asistente, deberá imprimir, guardar o memorizar los datos secretos antes de finalizar el asistente. Para hacerlo, haga clic en *Detalles*.

Opciones avanzadas

Si desea cambiar los valores específicos del usuario o utilizar funciones adicionales, tilde **Continuar con opciones avanzadas**. En ese caso, se iniciará el [Asistente de inicialización del usuario](#) una vez que el asistente haya finalizado.



©Infineon

Technologies AG

La solución Infineon Security Platform - Asistente para la inicialización rápida

Protocolo del archivo

Este diálogo muestra en pantalla el protocolo para todos los pasos realizados por el asistente.

Elementos de diálogo	Explicación
<input type="checkbox"/> <i>Imprimir...</i>	<p>Haga clic aquí para imprimir el archivo de protocolos. Se puede decidir si se desean incluir los datos secretos generados requeridos para administración y emergencias en la impresión del protocolo .</p>
<input type="checkbox"/> <i>Guardar...</i>	<p>Haga clic aquí para guardar el archivo de protocolos. Se puede decidir si se desean incluir los datos secretos generados requeridos para administración y emergencias en el protocolo a ser guardado.</p> <p> Tenga en cuenta que ya se ha guardado automáticamente una versión del protocolo sin los datos secretos (<i>SpProtocol_<PCName>_<UserName>.txt</i> para usuarios locales) o (<i>SpProtocol_<PCName>_<UserName>.<DomainName>.txt</i> para usuarios del dominio). En este diálogo se puede visualizar la ruta del archivo de protocolos que fue guardado automáticamente.</p>
<input type="checkbox"/> <i>Exhibición</i>	<p>Haga clic aquí para visualizar los datos secretos generados.</p> <p> Tenga en cuenta que la cantidad y tipo de datos secretos depende del estado de usuario y plataforma anterior y también depende del lugar donde ha decidido almacenar los resultados del asistente. Si la plataforma había sido inicializada antes de iniciar el asistente, y además se había seleccionado un medio extraíble (por ejemplo, memoria USB) para almacenar los resultados del asistente, entonces ninguna clase de datos secretos fueron creados.</p>
	<p>Después de finalizar el asistente, ya no tendrá oportunidad de acceder a los datos secretos generados. Por lo tanto, asegúrese de haber impreso,</p>

guardado o archivado los datos secretos de algún modo antes de finalizar el asistente. Esto es particularmente importante si no se ha seleccionado un medio extraíble (por ejemplo, memoria USB) para almacenar los resultados del asistente.



©Infineon

Technologies AG

La solución Infineon Security Platform - Asistente para la inicialización rápida

Datos secretos

Este diálogo permite visualizar los datos secretos generados.



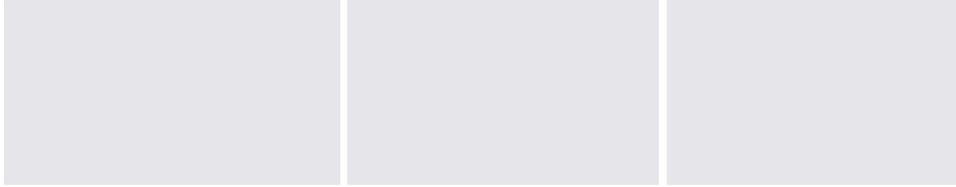
Si no ha seleccionado un medio extraíble (por ejemplo, memoria USB) para almacenar los resultados del asistente, deberá imprimir, guardar o memorizar todos los datos secretos generados. Los necesitará para realizar ciertas tareas cruciales relacionadas con administración y emergencias.

Tenga en cuenta que la cantidad y tipo de datos secretos depende del estado de usuario y plataforma anterior y también depende de dónde ha decidido almacenarlos.

La siguiente tabla ofrece detalles sobre los datos secretos generados y los archivos correspondientes. Las etiquetas **USB** y **HD** indican si los datos secretos o archivo en cuestión han sido creados y guardados, y si se ha seleccionado un medio extraíble (por ejemplo, memoria USB) o un disco duro (**HD**) para almacenar los resultados del asistente.

Tipo	Propósito	Extensión	Archivo correspondiente
Contraseña de propietario (USB, HD)	Requerida para realizar cruciales tareas administrativas de Security Platform.	Específico de la plataforma. Automáticamente creado durante los pasos de inicialización específicos de la plataforma si la plataforma no estaba aún inicializada cuando se inició el asistente.	Archivo de copia de contraseña de propietario Nombre de archivo: <i>SpOwner_<PC></i> , donde <i><PC></i> es el nombre de la plataforma. Sólo se crea y se selecciona si se ha seleccionado un medio extraíble (por ejemplo, memoria USB) para almacenar los resultados del asistente. En ese caso no se crea el archivo de copia de contraseña de propietario, ya que se ha seleccionado un medio extraíble. Archivo de copia de contraseña de propietario en medio USB (por ejemplo, memoria USB).
Contraseña para	Protege la	Específico de la	Combinación de

<p>Recuperación de emergencia/Tarjeta de seguridad para restablecimiento de la contraseña (HD)</p>	<p>combinación de Recuperación de emergencia/Tarjeta de seguridad para el restablecimiento de la contraseña que se necesita para realizar la Recuperación de emergencia y para restablecer la Contraseña del usuario básico.</p>	<p>plataforma. Automáticamente creado durante los pasos de configuración específicos de la plataforma si no se ha seleccionado un medio extraíble (por ejemplo, memoria USB) para almacenar los resultados del asistente y si la plataforma no había sido inicializada cuando se inició el asistente.</p>	<p>Recuperación de de seguridad para de la contraseña Nombre de archivo <i>SpToken_<PC>.2</i> donde <PC> es e plataforma Tenga en cuenta o seguridad no requ dedicada si está a medio extraíble (USB).</p>
<p>Secreto para el restablecimiento de la contraseña (USB, HD)</p>	<p>Un secreto personal del usuario que se requiere para restablecer su Contraseña de usuario básico.</p>	<p>Específico del usuario. Automáticamente creado durante los pasos de configuración específicos del usuario si el usuario no había sido inicializado cuando se inició el asistente.</p>	<p>Archivo del secr restablecimiento (USB) Nombre de archivo <i>SpPwdResetSecre</i> donde <PC> es e platatorma, y <U usuario (para usu combinación del nombre de domin dominio). Sólo se crea y se seleccionado un r ejemplo, memori. almacenar los res En ese caso no ne explícitamente el restablecimiento</p>



que puede utilizar
secreto para el re
contraseña desde
ejemplo, memori

Consejos generales para el manejo de datos secretos: Vea [Manejo de contraseñas](#).



©Infineon Technologies AG

Solución Infineon Security Platform - Asistente para la inicialización

Asistente para la inicialización de Infineon Security Platform

El asistente para la inicialización de Infineon Security Platform es utilizado para inicializar Security Platform y configurar sus funciones (copias de seguridad incluyendo restauración de emergencia, restablecimiento de contraseña, autenticación mejorada, BitLocker). Estas operaciones son requeridas para habilitar la funcionalidad de Infineon Security Platform y proveer las bases para todas las actividades futuras en Infineon Security Platform.

Si desea inicializar rápidamente su Security Platform y Usuario con las configuraciones predeterminadas, se recomienda que utilice el [Asistente para la inicialización rápida](#).

En lugar de inicializar una nueva Security Platform, también puede restaurar una Security Platform dañada seleccionando *Restaurar una Security Platform desde una copia de seguridad*.

Este es el primer asistente que debe ejecutarse para configurar una Infineon Security Platform



Disponibilidad del asistente:

- Este asistente está disponible sólo si el usuario actual tiene derechos de administración.
- Este asistente está disponible sólo si La política *Permiso de registración de plataforma* es habilitada con la opción *Permitir interfase y asistente de administración*, o si esta política no se encuentra configurada (las mismas condiciones son válidas si inicia este asistente desde el [icono de notificación de la barra de tareas](#)). Tenga en cuenta que esta política sólo surte efecto si Security Platform no se inicializa antes.
- Si el Security Platform ha sido inicializado con anterioridad, la política no estará en vigencia y este asistente puede utilizarse para configurar las funciones de Security Platform (las mismas condiciones son válidas si inicia este asistente desde el [icono de notificación de la barra de tareas](#)).
- El asistente no está disponible en el [modo servidor](#), ya que Security Platform se inicializa automáticamente si el sistema cliente está integrado en un Trust Domain con gestión centralizada.

Pasos del asistente

Paso	Comentario
1. Habilitar Trusted Platform Module	Solo si el Trusted Platform Module no se encuentra habilitado.
2. Inicializar o restaurar	Sólo si Security Platform todavía no esta inicializado.
3. Configuración de propiedad or Contraseña del propietario	Sólo si Security Platform todavía no esta inicializado. La contraseña del propietario puede ser activada o verificada dependiendo del estado de Security Platform.
4. Funciones	Copias de seguridad incluyendo restauración de emergencia, restablecimiento de contraseña, autenticación mejorada
5. Copia de seguridad	Solo si se seleccionó la función <i>Backup</i> .
6. Recuperación de emergencia	Solo si se seleccionó la función <i>Backup</i> .
7. Restablecimiento de contraseña	Solo si se seleccionó la función <i>Restablecimiento de contraseña</i> .
8. BitLocker	<p>Sólo si la función <i>BitLocker</i> fue seleccionada. Sólo si el estado de <i>BitLocker</i> es <i>Configurado</i>, <i>Requiere reconfiguración</i>, <i>Encriptando</i> o <i>Desencriptando</i>.</p> <p> • Esta función está sólo disponible si el sistema operativo admite la encriptación de unidad BitLocker (p.ej. para las ediciones Enterprise y Ultimate de Windows 7 y Windows Vista).</p> <p>• Esta página no está disponible en el modo servidor. Sin embargo puede configurar BitLocker a través del Applet del Panel de Control de Microsoft BitLocker.</p>

9. [Autenticación mejorada](#)

Solo si Security Platform ya se encontraba inicializada cuando comenzó el asistente.
Solo si se seleccionó la función *Autenticación mejorada*.

10. [Defensa de ataques por diccionario](#)

Sólo se encuentra disponible en Security Platforms con Infineon Trusted Platform Module 1.2.
Sólo si la función *Defensa de ataques por diccionario* ha sido seleccionada.

Inicio de la aplicación

Si Security Platform aún no se encuentra inicializado: Desde el [Ícono de notificación](#), de la barra de tareas, haga clic en el elemento del menú **Inicialización de Security Platform**. Se iniciará el [Asistente para la inicialización rápida](#) . En la página de Bienvenida seleccione **Inicialización avanzada**. Se iniciará el Asistente para la inicialización de Security Platform.

Si Security Platform ya se encuentra inicializado: Inicie el asistente para la inicialización de Security Platform por medio de la herramienta de configuración.

- Para configurar las funciones de Security Platform (copias de seguridad incluyendo restauración de emergencia, restablecimiento de contraseña, autenticación mejorada): [Herramienta de configuración - Avanzada - Configurar...](#)
- Para configurar solo la función de restablecimiento de contraseña: [Herramienta de configuración - Restablecimiento de contraseña - Configurar...](#)
- Para configurar solo la función de copia de seguridad: [Herramienta de configuración - Copia de seguridad - Configurar...](#)



La solución Infineon Security Platform - Asistente para la inicialización

Habilitado Trusted Platform Module

Es necesario habilitar el Trusted Platform Module para activar la funcionalidad principal. Sólo después de ello se puede inicializar el Security Platform y realizar las demás operaciones de configuración inicial. El procedimiento para habilitar Trusted Platform Module depende de la versión de Trusted Platform Module, el hardware de Security Platform y BIOS.

En los **sistemas Trusted Platform Module 1.2 que soportan la Interfaz de presencia física (PPI)**, dicha interfaz se utiliza para habilitar el Trusted Platform Module. Dependiendo del hardware y de la BIOS, esto se puede realizar sin la interacción del usuario, o puede requerir algunos pasos adicionales.

En **todos los demás sistemas** se debe reiniciar e ingresar a la BIOS del sistema. Aquí se encuentra disponible una descripción sobre cómo habilitar el chip:

En cualquier caso, el asistente detecta automáticamente cómo puede habilitarse el Trusted Platform Module en su sistema y lo guía según el caso.

La tabla a continuación le muestra cómo habilitar el Trusted Platform Module en diferentes tipos de Security Platform.

Tipo de Security Platform	Botón	Explicación
Trusted Platform Module 1.2 PPI debe ser reiniciado	<input type="checkbox"/> <i>Reiniciar</i>	Se reinicia el sistema. Al reiniciar, siga las instrucciones de la pantalla de inicio para habilitar el Trusted Platform Module.
Trusted Platform Module 1.2 PPI debe ser cerrado	<input type="checkbox"/> <i>Apagar</i>	Es sistema está apagado y necesita reiniciarse nuevamente de manera manual.

		Al inicio del sistema, siga las instrucciones de la pantalla de inicio para habilitar el Trusted Platform Module.
Trusted Platform Module 1.2 PPI no debe ser reiniciado ni cerrado	<input type="checkbox"/> <i>Habilitar</i>	La <i>Interfaz de presencia física</i> se utiliza para habilitar el Trusted Platform Module. No se requiere reinicio o apagado.  Dependiendo de su sistema, puede necesitar realizar algunos pasos adicionales para habilitar el Trusted Platform Module. Consulte su manual del sistema para más información.
Todos los demás tipos (por ejemplo, no se soportan Trusted Platform Module 1.1 y/o PPI)	<input type="checkbox"/> <i>Reiniciar</i>	El sistema se reinicia y el Trusted Platform Module debe habilitarse en la BIOS del sistema.
	Observación sobre el reinicio o apagado del sistema: Todas las aplicaciones están cerradas si indicaciones adicionales. Para prevenir una pérdida de información, todas las aplicaciones deben cerrarse antes de reiniciar el sistema.	



La Solución Infineon Security Platform - Asistente para la inicialización

Inicializar o restaurar Security Platform

Esta página de asistente pregunta si desea inicializar o restaurar una Security Platform.



Esta página del asistente no está disponible en el [modo servidor](#) ya que Security Platform se inicializa automáticamente si el sistema cliente está integrado a un Trust Domain con gestión centralizada, es decir, el administrador no tiene que realizar esta tarea.

Elemento de la página del asistente	Explicación
<input type="radio"/> <i>Inicialización de Security Platform</i>	Haga clic aquí si desea configurar una nueva Security Platform. En este caso se crearán una nueva plataforma y nuevas credenciales de usuario.
<input type="radio"/> <i>Restauración de Security Platform desde un archivo de copia de seguridad manual</i>	Haga clic aquí si desea restaurar una Security Platform luego de una falla, reemplazo o restablecimiento del hardware, medio de almacenamiento o Trusted Platform Module. Restauración de Security Platform reestablece el acceso a las funciones de Security Platform para todos los usuarios.



La Solución Infineon Security Platform - Asistente para la inicialización

Crear un Propietario de Security Platform.

Una vez que Trusted Platform Module esta habilitado, la propiedad debe ser configurada en una sola acción para asociar el chip lógico a la computadora para uso futuro. Durante esta operación se crea y almacena el propietario de Infineon Security Platform en el Trusted Platform Module, junto con el secreto de propietario de Infineon Security Platform. El mismo está protegido por la [Contraseña de propietario](#) que debe ser definida aquí. Puede escribir la Contraseña de propietario o generar una Contraseña de propietario aleatoria. Se puede guardar esta Contraseña de propietario en un archivo y utilizar este archivo de copia de seguridad con la Contraseña de propietario, o puede imprimirlo. Si ha elegido la opción de generar una Contraseña de propietario aleatoria, puede hacerla visible para memorizarla o anotarla. Se necesita la Contraseña de propietario o el archivo de copia de seguridad con la Contraseña de propietario para administrar la Security Platform.



Esta página del asistente no está disponible en el [modo servidor](#) ya que Security Platform se inicializa automáticamente si el sistema cliente está integrado a un Trust Domain con gestión centralizada, es decir, el administrador no tiene que realizar esta tarea.



Tomando propiedad por el asistente para la inicialización de Security Platform, este crea una nueva clave raíz de almacenamiento (SRK por sus siglas en inglés). Usualmente usted configura un propietario de Security Platform solo una vez, para una Trusted Platform Module específica. Desde que todos sus certificados de clave pública están relacionados a una clave raíz de almacenamiento (SRK por sus siglas en inglés) de Trusted Platform Module, no podrá utilizar estos certificados con una nueva SRK.

La siguiente tabla le muestra algunos consejos sobre cómo utilizar la página del asistente.

Elemento de la página del asistente	Explicación
 <i>Contraseña</i>	Establezca una Contraseña de propietario aquí. Se puede escribir de forma manual una Contraseña de propietario elegida por usted o se puede generar una

	<p>Contraseña de propietario aleatoria.</p> <p> Para garantizar que la Contraseña de propietario ingresada manualmente cumpla con los principales requisitos de calidad, se debe tener en cuenta un conjunto de reglas básicas para el pmanejo de contraseñas.</p>
<input checked="" type="checkbox"/> <i>Confirmar contraseña</i>	Ingrese nuevamente la contraseña para confirmar (no es necesario si ha generado una contraseña aleatoria).
<input type="checkbox"/> <i>Aleatoria</i>	<p>Haga clic aquí para generar una Contraseña de propietario aleatoria en vez de escribir una contraseña nueva. De este modo se asegurará de utilizar una contraseña segura que cumpla con los requisitos de complejidad y longitud de la misma.</p> <p> Asegúrese de desocultar, imprimir o guardar la contraseña aleatoria antes de continuar.</p>
<input type="checkbox"/> <i>En archivo...</i>	Haga clic aquí para guardar la nueva Contraseña de propietario en un archivo de copia de seguridad. Se podrá utilizar este archivo para la Autenticación de propietario en vez de escribir la contraseña.
<input type="checkbox"/> <i>Imprimir...</i>	<p>Haga clic en este botón para imprimir la Contraseña de propietario.</p> <p> Asegúrese de almacenar la impresión en una ubicación segura.</p>
<input checked="" type="checkbox"/> <i>Ocultar contraseñas</i>	Destilde esta casilla de verificación si desea ver las contraseñas.

 Tenga en cuenta que debido a la política [Habilitar seguridad estricta para campo de contraseña](#), podría no permitirse cortar, copiar, pegar y ver contraseñas en texto simple.



La Solución Infineon Security Platform - Asistente para la inicialización

Contraseña de propietario

Se requiere la [Contraseña de propietario](#) para realizar las cruciales tareas administrativas de Security Platform.

Esta página aparece en pantalla en el [Asistente para la inicialización de Security Platform](#) y en el [Asistente para la inicialización rápida](#), si ya existe la Contraseña de propietario pero todavía no se ha inicializado la Security Platform.

Este es el caso bajo estas circunstancias:

- Si la Contraseña de propietario ha sido establecida por medio de la aplicación [Trusted Platform Module \(TPM\) Management de Microsoft](#).
- Si el proceso de inicialización de Security Platform ha sido interrumpido tal vez por una pérdida de energía o alguna otra razón
- Si Security Platform es inicializada y tiene un propietario en otro sistema operativo (OS por sus siglas en inglés)
- Si Security Platform es inicializada en un sistema operativo (OS por sus siglas en inglés) y después el usuario inicializa Security Platform en otro entrando en la BIOS

Para autenticar, se puede escribir la contraseña o suministrar un archivo de Copia de seguridad de la contraseña de propietario.



Esta página del asistente no está disponible en el [modo servidor](#) ya que Security Platform se inicializa automáticamente si el sistema cliente está integrado a un Trust Domain con gestión centralizada, es decir, el administrador no tiene que realizar esta tarea.



Solución Infineon Security Platform - Asistente para la inicialización

Funciones de Security Platform

Con esta página usted puede configurar las funciones de Security Platform, e.j. copias de seguridad.



Esta página del asistente no está disponible en el [modo servidor](#), ya que el Trusted Computing Management Server realiza la tarea de configuración de las características de Security Platform, como ser *copia de seguridad*, *restablecimiento de la contraseña* y *autenticación mejorada*. La función *BitLocker* se puede configurar a través de Applet del Panel de Control de Microsoft.

La siguiente tabla explica todas las funciones de Security Platform.

Función	Explicación
<input checked="" type="checkbox"/> <i>Copia de seguridad automática (incluye recuperación de emergencia)</i>	<p>Seleccione esta función si desea configurar copias de seguridad automáticas de Security Platform. Configurar <i>Copias de seguridad</i> es altamente recomendado. De otro modo toda la información de usuario se perderá en caso de emergencia.</p> <p> Observe que no podrán desmarcar esta opción si la política Implementación de configuración de copias de seguridad incluyendo recuperación de emergencia está habilitada.</p>
<input checked="" type="checkbox"/> <i>Restablecimiento de la contraseña</i>	<p>Seleccione esta función si desea crear una tarjeta de restablecimiento de contraseña para todos los usuarios. Configurar <i>Restablecimiento de contraseña</i> es altamente recomendado. De otro modo las contraseñas de usuario básico no podrán ser restablecida.</p> <p> Observe que no podrán desmarcar esta opción si la política Implementación configuración de restablecimiento de contraseña esta habilitada.</p> <p>Esta función puede ser configurada una sola vez. La selección esta deshabilitada si <i>Restablecimiento de contraseña</i> ya está configurado.</p>

<input checked="" type="checkbox"/> <i>BitLocker</i>	<p>Tilde esta función si desea utilizar el cifrado de unidad BitLocker junto con el Trusted Platform Module para encriptar datos en su disco.</p> <p> Esta función está sólo disponible si el sistema operativo admite la encriptación de unidad BitLocker (p.ej. para las ediciones Enterprise y Ultimate de Windows 7 y Windows Vista).</p>
<input checked="" type="checkbox"/> <i>Autenticación mejorada</i>	<p>Seleccione esta función si desea habilitar la autenticación mejorada para todos los usuarios o si desea cambiar la selección de dispositivos de autenticación.</p> <p>Esta función esta solamente disponible si se instala al menos un plug-in de autenticación mejorada. Esta función no se encuentra disponible si Security Platform no ha sido inicializado antes de iniciar el asistente.</p>
<input checked="" type="checkbox"/> <i>Defensa de ataques de diccionario</i>	<p>Tilde esta función si desea configurar la cantidad de intentos de autenticación que deben permitirse para los diversos tipos de autenticación antes de que se tomen medidas de defensa de ataques por diccionario. Ver Configurar los valores de defensa de ataques por diccionario.</p> <p> Tenga en cuenta que esta función sólo se encuentra disponible en Security Platforms con un Infineon Trusted Platform Module 1.2 si la política Configurar el umbral de ataques por diccionario no se encuentra configurada. Esta función no se encuentra disponible si Security Platform no ha sido inicializado antes de iniciar el asistente.</p>



La Solución Infineon Security Platform - Asistente para la inicialización

Copia de seguridad

Con esta página usted puede configurar copias de seguridad automáticas de Security Platform. Vea [Copia de seguridad y restauración de datos de Security Platform](#).



En el [modo servidor](#) esta página no está disponible ya que las copias de seguridad automáticas son llevadas a cabo por el Trusted Computing Management Server, es decir que aquí no se requiere configuración explícita por parte del usuario.

A continuación se muestra una tabla con algunos consejos para utilizar esta página del asistente.

Elemento de la página del asistente	Explicación
<p> <i>Ubicación de copia de seguridad:</i> <input type="checkbox"/> <i>Examinar...</i></p>	<p>Las credenciales y la configuración de Security Platform serán guardados con regularidad en un archivo de copia de seguridad.</p> <p>Ingrese la ruta y el nombre del archivo o examine para buscarlo. Se creará un Archivo de copia de seguridad que consta de un archivo XML y de una carpeta con el mismo nombre, por ejemplo: archivo <code>SPSystemBackup.xml</code> y carpeta <code>SPSystemBackup</code>.</p> <p> Utilice la extensión *.xml.</p>
<p><input type="checkbox"/> <i>Programa...</i></p>	<p>Una copia de seguridad programada será creada. Haga clic aquí para ver y modificar la programación de las copias de seguridad.</p> <p> Por favor observe que las copias de seguridad automáticas son realizadas solamente si su computadora no esta apagada a la hora programada.</p> <p>Observe que la cuenta de usuario seleccionada para la copia de seguridad programada debe ser miembro del grupo "Administradores" o "Operadores de copias de seguridad".</p>



TPM

©Infineon Technologies AG

La Solución Infineon Security Platform - Asistente para la inicialización

Recuperación de emergencia

Con esta página se puede configurar la recuperación de emergencia que es parte de las copias de seguridad automáticas de Security Platform.



Disponibilidad de la página:

- Esta página esta solo disponible si ha seleccionado para configurar copias de seguridad automáticas de Security Platform.
- En el [modo servidor](#) esta página no está disponible ya que las copias de seguridad automáticas y restauraciones son llevadas a cabo por el Trusted Computing Management Server, es decir que aquí no se requiere configuración explícita por parte del usuario.

Elementos de la página del asistente



Observe que sus opciones en esta página de asistente pueden estar restringidas dependiendo de las [políticas del sistema](#).

La siguiente tabla le muestra algunos consejos sobre cómo utilizar la página del asistente.

Elemento de la página del asistente	Explicación
<input checked="" type="radio"/> <i>Crear una nueva tarjeta de seguridad de recuperación</i>	<p>Seleccione esta opción si desea crear una nueva tarjeta de seguridad para ser utilizada para recuperación de emergencia. La tarjeta de seguridad será guardada en la ubicación que haya especificado.</p> <p>Tendrá que establecer una nueva contraseña de tarjeta de seguridad.</p>
<input checked="" type="radio"/> <i>Utilizar la tarjeta de seguridad de recuperación existente</i>	<p>Seleccione esta opción si se reúnen las siguientes condiciones:</p> <ul style="list-style-type: none">• En caso de emergencia restaurar su sistema utilizando la tarjeta de seguridad de recuperación de emergencia que ha creado antes.• Esta tarjeta de seguridad y su contraseña son actualmente accesibles. <p>Tendrá que verificar la contraseña de la tarjeta de seguridad, es decir que necesita ingresar la contraseña por única vez.</p>
<input type="checkbox"/> <i>Ubicación del archivo</i> <input type="checkbox"/> <i>Examinar...</i>	<p>Si su política de configuración permite una especificación manual de la ubicación del archivo, puede cambiar el nombre de archivo y su ruta de acceso.</p> <p>Ingrese la ruta y el nombre del archivo o examine para buscarlo. Este archivo está en formato XML.</p> <p> Si ha seleccionado <i>Crear una nueva tarjeta de seguridad de recuperación</i>: La tarjeta de seguridad de recuperación de emergencia debería guardarse en una ubicación segura como un medio removible almacenado en un ambiente seguro. No guarde la tarjeta de seguridad de recuperación en su disco</p>

	<p>duro. De otro modo, en caso de falla del sistema o del disco duro, su tarjeta de seguridad no será accesible y se perderá información. Guarde la tarjeta de seguridad de recuperación en un medio de respaldo como un dispositivo de memoria o un disco compacto para prevenir la pérdida de esta y asegurarse que solo usted tiene acceso esta tarjeta de seguridad de recuperación.</p>
<p> Contraseña</p>	<p>Si ha seleccionado <i>Crear una nueva tarjeta de seguridad de recuperación</i>, necesita establecer una nueva contraseña de tarjeta de seguridad. Ingrese una contraseña para la tarjeta de seguridad de recuperación de emergencia. Tenga en cuenta los consejos generales referidos a las contraseñas.</p> <p>Si ha seleccionado <i>Usar la tarjeta de seguridad de recuperación existente</i>, necesita verificar la contraseña de la tarjeta de seguridad. Ingrese la contraseña de la tarjeta de seguridad existente.</p> <p>Si ha seleccionado <i>Usar el archivo de recuperación existente</i>, no necesita ingresar una contraseña.</p>
<p> Confirmar la contraseña</p>	<p>Si ha seleccionado <i>Crear una nueva tarjeta de seguridad de recuperación</i>, necesita confirmar su contraseña nueva. Ingrese de nuevo la contraseña para confirmar.</p>



La Solución Infineon Security Platform - Asistente para la inicialización

Restablecimiento de la contraseña

Con esta página usted puede crear una tarjeta de seguridad de restablecimiento de la contraseña para todos los usuarios.



Disponibilidad de la página:

- Esta página esta solamente habilitada, si ha seleccionado configurar el restablecimiento de las contraseñass.
- Esta página no está disponible en [modo servidor](#), ya que Trusted Computing Management Server administra esta tarea.

Elementos de la página del asistente



Observe que sus opciones en esta página de asistente pueden estar restringidas dependiendo de las [políticas del sistema](#).

La siguiente tabla le muestra algunos consejos sobre cómo utilizar la página del asistente.

Elemento de la página del asistente	Explicación
<input checked="" type="radio"/> <i>Creación de una nueva tarjeta de seguridad</i>	<p>Seleccione esta opción si desea crear una nueva tarjeta de seguridad para ser utilizada en el restablecimiento de la contraseña.</p> <p>La tarjeta de seguridad será guardada en la ubicación que haya especificado.</p> <p>Tendrá que establecer una nueva contraseña de tarjeta de seguridad.</p>
<input checked="" type="radio"/> <i>Uso de la tarjeta de seguridad existente</i>	<p>Seleccione esta opción si se reúnen las siguientes condiciones:</p> <ul style="list-style-type: none">• Desea restablecer contraseñas utilizando una tarjeta de seguridad que ya fue creada.• Esta tarjeta de seguridad y su contraseña son actualmente accesibles. <p>Tendrá que verificar la contraseña de la tarjeta de seguridad, es decir que necesita ingresar la contraseña por única vez.</p>
<input type="checkbox"/> <i>Ubicación de archivo</i> <input type="checkbox"/> <i>Examinar...</i>	<p>Si su política de configuración permite una especificación manual de la ubicación del archivo, puede cambiar el nombre de archivo y su ruta de acceso.</p> <p>Ingrese la ruta y el nombre del archivo o examine para buscarlo. Este archivo está en formato XML.</p> <p> Si ha seleccionado <i>Crear una nueva tarjeta de seguridad</i>: La tarjeta de seguridad de restablecimiento de la contraseña debería guardarse en una ubicación segura como un medio removible almacenado en un ambiente seguro. No guarde la tarjeta de seguridad en su disco duro. De otro modo, en caso</p>

	<p>de falla del sistema o del disco duro, su tarjeta de seguridad no será accesible y las contraseñas de usuario básico no podrán restablecerse. Guarde la tarjeta de seguridad en un medio de respaldo como un dispositivo de memoria o un disco compacto para prevenir la pérdida de esta y asegurarse que solo usted tiene acceso a la tarjeta de seguridad.</p>
<p> <i>Contraseña</i></p>	<p>Si ha seleccionado <i>Crear una nueva tarjeta de seguridad</i>, necesita establecer una nueva contraseña de tarjeta de seguridad. Ingrese una contraseña para la tarjeta de seguridad de restablecimiento de la contraseña. Tenga en cuenta los consejos generales referidos a las contraseñas.</p> <p>Si ha seleccionado <i>Usar la tarjeta de seguridad existente</i>, necesita verificar la contraseña de la tarjeta de seguridad. Ingrese la contraseña de la tarjeta de seguridad existente.</p> <p>Si ha seleccionado <i>Usar el archivo existente</i>, no necesita ingresar una contraseña.</p>
<p> <i>Confirmación de la contraseña</i></p>	<p>Si ha seleccionado <i>Crear una nueva tarjeta de seguridad</i>, necesita confirmar su contraseña nueva. Ingrese de nuevo la contraseña para confirmar.</p>



Solución Infineon Security Platform - Asistente para la inicialización

BitLocker

En esta página puede utilizar el cifrado de unidad BitLocker junto con el Trusted Platform Module para encriptar datos en su disco.



Disponibilidad de la página:

- Esta página está sólo disponible si el sistema operativo admite la encriptación de unidad BitLocker (p.ej. para las ediciones Enterprise y Ultimate de Windows 7 y Windows Vista).
- Esta página sólo se encuentra disponible si el estado de BitLocker es *Configurado*, *Requiere reconfiguración*, *Encriptando* o *Desencriptando* y si el usuario selecciona esta función.
- Esta página no aparece cuando el estado de BitLocker es "*No configurado*" ya que la configuración inicial de BitLocker requiere el reinicio del sistema. En este caso el Applet del panel de control de BitLocker se inicia automáticamente después de la finalización del Asistente para la inicialización.
- Esta página no está disponible en el [modo servidor](#).

Elementos de la página del asistente

La siguiente tabla le ofrece algunos consejos sobre cómo utilizar la página del asistente.

Configurar

Si hace clic en este botón se iniciará el Applet del panel de control de Microsoft BitLocker.



©Infineon

Technologies AG

La Solución Infineon Security Platform - Asistente para la inicialización

Autenticación mejorada

Con ésta página es posible habilitar la autenticación mejorada para todos los usuarios o cambiar la selección de dispositivos de autenticación.



Disponibilidad de la página:

- Esta página sólo se encuentra disponible en modo stand-alone si al menos un plug-in de autenticación avanzada se encuentra instalado.
- Esta página no está disponible en el modo [servidor](#) ya que Trusted Computing Management Server realiza la tarea de configurar la Autenticación mejorada a través de la política del servidor, es decir que el administrador no tiene que realizar esta tarea.

La siguiente tabla le muestra algunos consejos sobre cómo utilizar la página del asistente.

Elemento de la página del asistente	Explicación
<input type="checkbox"/> Lista de dispositivos de autenticación	<p>Marque el dispositivo/s de autenticación que desee habilitar para todos los usuarios de Security Platform. Una vez habilitado un dispositivo de autenticación, los usuarios pueden seleccionar este dispositivo para autenticarse.</p> <p> <ul style="list-style-type: none">• Si desea asegurarse que los usuarios de Security Platform realmente utilizan autenticación mejorada, debería habilitar la política de usuario Implementación de la autenticación mejorada.• En el modo stand-alone, si la política de proveedores de autenticación avanzada está en vigencia, sólo se puede configurar la lista de proveedores de autenticación avanzada permitidos mencionados en dicha política. Pero si la política no está configurada, todos los proveedores de autenticación avanzada registrados pueden ser configurados.</p>



©Infineon Technologies AG

La Solución Infineon Security Platform - Asistente para la inicialización de usuarios

Asistente para la inicialización de Infineon Security Platform

El Asistente para la inicialización de usuarios de Infineon Security Platform está diseñado para que los expertos inicialicen los Usuarios de Security Platform y configuren las funciones específicas del usuario (correo electrónico seguro, encriptación de archivos y carpetas con EFS y PSD, Autenticación avanzada). Este asistente debe ser iniciado para cada usuario de computadora que desee utilizar las Funciones personalizadas de Infineon Security Platform (es decir, la persona que será usuario de Infineon Security Platform).

Si desea inicializar rápidamente su usuario de Security Platform con las configuraciones predeterminadas, se recomienda que utilice el [Asistente para la inicialización rápida](#) .



Disponibilidad del asistente:

- Este asistente sólo se encuentra disponible si está habilitada la política *Permitir la inscripción de usuarios* con la opción *Permitir la interfaz de administración y el asistente*, o si dicha política no se encuentra configurada (las mismas condiciones son válidas si inicia este asistente desde el [icono de notificación de la barra de tareas](#)). Observe que esta política sólo se encuentra en vigencia para los usuarios que aun no estén inicializados.
- Si un usuario ha sido inicializado con anterioridad, la política no estará en vigencia y este asistente puede utilizarse para configurar las funciones específicas del usuario (las mismas condiciones son válidas si inicia este asistente desde el [icono de notificación de la barra de tareas](#)).
- En el [modo servidor](#), este asistente sólo está disponible si el usuario actual es un miembro del grupo de inscripción de usuarios.

Pasos del asistente

La siguiente tabla muestra los pasos del asistente para un usuario aún no inicializado. En caso de usuarios ya inicializados, sólo se realizan los pasos necesarios para una tarea especial del asistente (como sería, configurar una función específica del Usuario de Security Platform)

Paso	Comentario
1. Dispositivo de autenticación	<p>Sólo si el administrador de Security Platform habilitó al menos un dispositivo de autenticación.</p> <p>Sólo si el Usuario de Security Platform todavía no está inicializado. De otro modo esta página está disponible por medio de las Funciones de Security Platform.</p> <p> Si ya configuró la autenticación avanzada, pero su dispositivo de autenticación y Security Platform tienen distintas frases de contraseña de usuario básico, se le solicitará que sincronice su frase de contraseña de usuario básico.</p>
2. Contraseña de usuario básico	Sólo si el Usuario de Security Platform todavía no está inicializado.
3. Restablecimiento de la contraseña de usuario básico	Sólo si el administrador de Security Platform configuró la función de restablecimiento de la contraseña.
4. Funciones de Security Platform	Correo electrónico seguro, encriptación de archivos y carpetas con EFS y PSD, autenticación avanzada.
5. Solicitud de certificado	Sólo si se seleccionó <i>correo electrónico seguro</i> o <i>encriptación de archivos y carpetas</i> (EFS or PSD).
6. Configuración de correo electrónico seguro	Sólo si se selecciona <i>correo electrónico seguro</i> .
7. Certificado de encriptación	Sólo si se seleccionó <i>encriptación de archivos y carpetas</i> (EFS o PSD).

8. [Personal Secure Drive](#)

Solo si se seleccionó *encriptación de archivos y carpetas con Personal Secure Drive*

Inicio de la aplicación

Si el usuario actual aún no se inicializó: Desde el [Ícono de notificación de la barra de herramientas](#), haga clic en el elemento del menú Inicialización del usuario de Security Platform. Se iniciará el [Asistente para la inicialización rápida](#). En la página de Bienvenida seleccione la Inicialización avanzada. Se iniciará el Asistente para la inicialización de usuarios de Security Platform.

Si el usuario actual ya está inicializado: Inicie el asistente para la inicialización de usuarios por medio de la Herramienta de Configuración.

- Para configurar las funciones específicas del Usuario de Security Platform (e-mail seguro, encriptación de archivos y carpetas con EFS PSD, autenticación avanzada): [Herramienta de Configuración - Configuraciones del usuario - Configurar...](#)

[El Asistente para la inicialización rápida](#) se iniciará en vez del se iniciará en vez del Asistente para la inicialización de usuarios mientras las funciones del usuario no estén configuradas. En este caso, seleccione **Inicialización avanzada** en la página de Bienvenida.

- Para habilitar la función de restablecimiento de la contraseña para el usuario actual: [Herramienta de Configuración - Restablecimiento de la contraseña - Configurar...](#)
- Para crear un dispositivo de autenticación de la copia de seguridad: [Herramienta de Configuración - Copia de seguridad - Crear...](#)

Descripción de los parámetros de la línea de comando: Se puede iniciar el asistente por medio del explorador de Windows haciendo doble clic en el archivo *SpUserWz.exe* de la carpeta de instalación de la Solución Security Platform. Se permiten los siguientes parámetros de la línea de comando:

Parámetro	Comentario
<i>-forceinit</i> o <i>/forceinit</i>	Obliga a un usuario a reinicializar.  Se pierden todas las credenciales de usuario existentes. Utilice solamente este parámetro de la línea de comando si no dispone de un paquete de archivos de la

copia de seguridad.



Este parámetro de la línea de comandos no es soportado en el [modo servidor](#) como:

- El usuario no incurrirá en una situación en donde necesite utilizar este parámetro.
- No se espera que el usuario en un entorno Trust Domain utilice esto.



La Solución Infineon Security Platform - Asistente para la inicialización de usuarios

Dispositivo de autenticación

Esta página le permite seleccionar un dispositivo de autenticación.



Disponibilidad de la página: Esta página está disponible solamente si su administrador habilitó al menos un dispositivo de autenticación.

La siguiente tabla le muestra algunos consejos sobre cómo utilizar la página del asistente.

Elemento de la página del asistente	Explicación
<input type="checkbox"/> Lista de dispositivos de autenticación	<p>Seleccione el dispositivo de autenticación que desea utilizar. Si la política Imponer la autenticación avanzada no está habilitada, se puede seleccionar también la <i>contraseña</i>. Esto significa que no está utilizando ningún dispositivo de autenticación.</p> <p> No puede cambiar su selección de un dispositivo de autenticación a otro. Si desea hacerlo, debe primero cambiar a <i>Contraseña</i>. Puede cambiar al otro dispositivo de autenticación recurriendo nuevamente al asistente.</p>



Infineon Solución Security Platform - Asistente para la inicialización de usuario

Sincronizar la frase de contraseña de usuario básico

Por medio de esta página puede indicar la forma de sincronizar su frase de contraseña de usuario básico, si su dispositivo de autenticación y su Security Platform poseen distintas frases de contraseña.



Disponibilidad de la página: Esta página se muestra solamente, si se cumplen las siguientes condiciones:

- Configuró la autenticación avanzada.
- Se detectó que su dispositivo de autenticación y su Security Platform tienen diferentes frases de contraseña.

La siguiente tabla le muestra algunos consejos sobre cómo utilizar la página del asistente.

Página del asistente Elemento	Explicación
<input checked="" type="radio"/> Utilizar la frase de contraseña desde Security Platform, actualizar el dispositivo de autenticación	Seleccione esta opción si su dispositivo de autenticación se debe actualizar con la frase de usuario básico que utiliza actualmente su Security Platform. Esto es necesario si restableció su frase de contraseña de usuario básico sin actualizar su dispositivo de autenticación.
<input checked="" type="radio"/> Utilizar la frase de contraseña desde el dispositivo de autenticación, actualizar Security Platform	Seleccione esta opción para actualizar su Security Platform con la Frase de contraseña de Usuario básico la cual es utilizada por su dispositivo de autenticación. Esto es necesario si utiliza su dispositivo de autenticación en varios Security Platform, y cambió su frase de contraseña de usuario básico en otro.



La Solución Infineon Security Platform - Asistente para la inicialización de usuarios

Restauración de la contraseña de usuario básico

Por medio de esta página puede habilitar el restablecimiento de su contraseña de usuario básico en caso de emergencia (por ejemplo, si ha olvidado su contraseña de usuario básico actual).



Disponibilidad de la página: Esta página está disponible solamente si su administrador configuró el restablecimiento de la contraseña.

La siguiente tabla le ofrece algunos consejos sobre cómo utilizar la página del asistente.

Elemento de la página del asistente	Explicación
<input checked="" type="checkbox"/> <i>Permitir el restablecimiento de mi contraseña de usuario básico en caso de emergencia</i>	Tilde esta casilla de verificación para asegurarse de poder restablecer su contraseña de usuario básico en caso de emergencia.  Observe que no puede desmarcar esta casilla de verificación si ya ha activado la opción Restablecimiento de la contraseña, o si está habilitada la política Imponer la habilitación del restablecimiento de la contraseña .
 <i>Datos personales secretos</i> <input type="checkbox"/> <i>Examinar...</i>	Los datos personales secretos se escribirán a un archivo. Ingrese la ruta y el nombre del archivo o examine para buscarlo.  Guarde este archivo en un lugar seguro. Lo necesitará si necesita restablecer su contraseña de usuario básico en caso de emergencia.



La Solución Infineon Security Platform - Asistente para la inicialización de usuarios

Confirmar sus configuraciones (paso 1)

Su administrador de sistemas puede activar una función que le permita la recuperación de su clave de usuario básico. En este caso, se crearán entradas adicionales en el paquete de archivos de la copia de seguridad.

Nota: La clave de usuario básico se maneja siempre en modo protegido, aún en el proceso de recuperación.

El sistema ahora está listo para generar su clave de usuario básico. En caso de que la función de la copia de seguridad se encuentre activada, se crearán datos adicionales de recuperación de emergencia, que contienen la información necesaria para recuperar su clave.

Luego de hacer clic en el botón **Siguiente** se generará su clave de usuario básico.

Nota: No cierre la sesión, ni apague la máquina o desconecte el cable de alimentación mientras se esté efectuando esta operación.

Technologies AG



Solución Infineon Security Platform - Asistente para la inicialización de usuarios

Funciones de Security Platform

En esta página se pueden configurar las funciones de su Security Platform, por ejemplo, la encriptación de archivos y carpetas.



Disponibilidad de la página: Esta página está disponible solamente si sus políticas de usuario le permiten configurar al menos una opción.

Disponibilidad de funciones: Depende de su [configuración de las políticas de usuario](#).

La siguiente tabla explica todas las funciones de Security Platform.

Función	Explicación
<input checked="" type="checkbox"/> <i>Correo electrónico seguro</i>	<p>Encriptación de correo electrónico específico del usuario y/o firma para la prevención de lectura o modificación de sus correos electrónicos por parte de personas no autorizadas. El uso de esta característica garantiza que sólo el autor del mensaje de correo electrónico y los destinatarios especificados puedan descifrar y leer el mensaje o validar la identidad del remitente.</p> <p>Si opta por configurar esta función, puede solicitar un certificado para correo electrónico seguro. (Si elige configurar esta función, puede solicitar un certificado para correo electrónico seguro si se establece una dirección Web de una solicitud de certificado en sus configuración de la política). El asistente proveerá información sobre cómo configurar correo electrónico seguro. La configuración de su cliente de correo no forma parte de este asistente. Por lo tanto, su estado no se muestra aquí.</p>
<input checked="" type="checkbox"/> <i>Encriptación de archivos y carpetas - Certificado de encriptación</i>	<p>Seleccione esta función si desea visualizar o cambiar su Certificado de encriptación. Si opta por configurar esta función, se puede seleccionar un certificado. También se puede solicitar o crear un nuevo certificado.</p> <p>  El <i>Certificado de encriptación</i> sólo aparece en pantalla como una función separada del usuario si EFS o PSD ya están configurados. La página del Certificado de</p>

	<p>encriptación también aparece en pantalla durante la primera configuración de EFS o PSD.</p>
<p><input checked="" type="checkbox"/> <i>Encriptación de archivos y carpetas - Encrypting File System (EFS)</i></p>	<p>El sistema operativo incorpora la funcionalidad para la permitir la encriptación específica del usuario del contenido de archivos y carpetas en la computadora local utilizando el Encrypting File System (EFS) de Microsoft. Sólo el usuario que creó un archivo en estas carpetas puede acceder al contenido del mismo. Los demás usuarios deben obtener permisos de acceso a una carpeta EFS por medio de una operación administrativa explícita para poder utilizar los archivos contenidos en dicha carpeta.</p> <p> EFS no se admite en ediciones de Windows Home.</p>
<p><input checked="" type="checkbox"/> <i>Encriptación de archivos y carpetas con el Personal Secure Drive (PSD)</i></p>	<p>Personal Secure Drive ofrece la encriptación de archivos y carpetas de manera similar a EFS. A diferencia EFS, PSD lo admiten todos los sistemas operativos soportados por la solución Security Platform.</p> <p>Se provee un dispositivo lógico a los usuarios permitidos. Este dispositivo ofrece protección de acceso y encriptación para todo lo contenido en él. La encriptación es realizada automáticamente. No se puede acceder a un PSD por medio de su identificador UNC para conseguir datos legibles, y puede instalarse sólo en la computadora local. No es posible el acceso a la red.</p> <p>Podrá administrar los Personal Secure Drives si eligió configurar esta función.</p>
<p><input checked="" type="checkbox"/> <i>Autenticación mejorada</i></p>	<p>Seleccione esta función si desea ver o modificar sus configuraciones de autenticación. Si sus políticas lo permiten, puede seleccionar un dispositivo de autenticación o una autenticación por contraseña.</p> <p> Esta función está disponible solamente si su administrador habilitó al menos un dispositivo de autenticación. Esta función no está disponible si su cuenta de usuario no se inicializó previo al inicio del asistente.</p>

Reconfiguración de la función: En determinadas circunstancias especiales puede necesitar reconfigurar una función. Por ejemplo:

- Cuando el estado de *Encriptación de carpetas y archivos - Certificado de encriptación* es *requerido por la reconfiguración*, primero se debe resolver esto. Si el certificado de encriptación no es válido o ya no se encuentra disponible, se puede crear un nuevo certificado de encriptación o se pueden restaurar las credenciales del usuario. Este certificado es luego automáticamente reconfigurado por clave para su EFS y/o PSD configurado.
- Si el certificado de encriptación no se encuentra disponible y no tiene copia de seguridad de las credenciales del usuario, se debe crear un nuevo certificado de encriptación. Este nuevo certificado es luego automáticamente reconfigurado por clave para su EFS configurado. Pero este certificado no puede ser automáticamente reconfigurado por clave para su PSD configurado, por lo cual deberá borrar el PSD anterior y crear un nuevo PSD con este nuevo certificado de encriptación.
- Su certificado EFS o PSD ya no es válido y no está disponible. Sucede lo mismo con la encriptación de *archivos y carpetas por medio del Encrypting File System (EFS)*, si configuró tanto EFS como PSD y luego cambió su certificado PSD.
- Se realizó una restauración pero su PSD ya no se encuentra accesible (por ejemplo debido a que no se pudo ubicar el archivo de imagen de PSD).
- Configuró la *Autenticación avanzada*, pero su dispositivo de autenticación ya no está disponible o su dispositivo de autenticación y su Security Platform tienen Frases de contraseña de Usuario Básico diferentes.



La Solución Infineon Security Platform - Asistente para la inicialización de usuarios

Solicitud de certificado

Las funciones específicas del Usuario de Infineon Security Platform necesitan certificados para funcionar. Estos certificados permiten al usuario comprobar su identidad en un medio electrónico. Los certificados se generan fuera del software de Infineon Security Platform y tienen que ser transferidos al sistema por medio de mecanismos definidos.

	Disponibilidad de la página: Esta página está disponible sólo si se seleccionó al menos una función de seguridad y la política para la inscripción de certificados está habilitada (URL para iniciar desde el asistente para la inscripción de certificados). Contacte a su administrador para obtener información adicional.
Elemento de la página del asistente	Explicación
<input type="checkbox"/> <i>Solicitar certificado...</i>	El administrador de Infineon Security Platform establece en las políticas de Infineon Security Platform que se debe obtener un certificado y el método por el cual debe hacerse cuando el botón está activado. Al hacer clic en el botón, se conduce al usuario a una página aparte del asistente para la inscripción del certificado. Esta página es configurada por el administrador. Luego de completar el proceso de inscripción proceda con los siguientes pasos del asistente.

[Como inscribir certificados](#)



La Solución Infineon Security Platform - Asistente para la inicialización de usuarios

Configuración de correo electrónico seguro

El correo electrónico seguro es la encriptación del correo electrónico específico del usuario y/o la firma para la prevención de lectura o modificación de sus correos electrónicos por parte de personas no autorizadas. El uso de esta función garantiza que sólo el creador del correo electrónico y los destinatarios especificados puedan desencriptar y leer el mensaje, o validar la identidad del remitente.

La encriptación y el firmado de correo electrónico están disponibles en las aplicaciones de correo electrónico más populares. Si utilizará correo electrónico seguro, se lista la ayuda disponible para los clientes de correo electrónicos permitidos y aquí puede obtener información adicional.

Actualmente se encuentran permitidos los siguientes clientes de correo electrónico:

- Microsoft Windows Mail/Outlook Express
- Microsoft Outlook 2003
- Microsoft Outlook XP
- Microsoft Outlook 2000
- Mozilla Thunderbird

Para poder utilizar correo electrónico seguro, el cliente de correo electrónico debe configurarse para utilizar certificados digitales que estén protegidos con el Security Platform. Contacte a su administrador de sistemas para realizar una solicitud de certificado por medio de una entidad certificada apropiada, o realice una solicitud por medio de una entidad certificada en Internet.

Está disponible, por medio del botón correspondiente, una guía del usuario y una configuración detallada para cada cliente de correo electrónico.

Nota: Si todavía no dispone de un certificado digital que pueda utilizarse para el correo electrónico seguro, obténgalo antes de continuar con los pasos de configuración.

[Información detallada](#)

Technologies AG



Solución Infineon Security Platform - Asistente para la inicialización de usuarios

Certificado de encriptación

Esta página le permite seleccionar un certificado de encriptación para ser utilizado por [EFS](#) y/o [PSD](#). Cada certificado está identificado por su huella digital y siempre se asigna a un usuario de Infineon Security Platform sin ambigüedad.

Si no hay ningún certificado válido registrado actualmente, pero ya se encuentra disponible otro certificado apropiado, el asistente le ofrece seleccionar este certificado de modo automático. Si no se encuentra disponible ningún certificado de esta clase, el asistente le ofrece crear un nuevo certificado y seleccionarlo de modo automático.

Si no desea que el asistente cree y/o seleccione un certificado de modo automático, también lo puede realizar en modo manual.

La siguiente tabla le ofrece algunos consejos sobre cómo utilizar la página del asistente.

Elemento de la página del asistente	Explicación
 <i>Certificado actual</i>	Aquí puede encontrar información sobre el certificado de encriptación actualmente registrado (si ya había seleccionado un certificado con anterioridad).
 <i>Nuevo certificado</i>	Aquí puede encontrar información sobre el certificado de encriptación que será utilizado en el futuro (si es que se va a utilizar otro certificado distinto al certificado actual). Éste podría ser un certificado que será creado y/o seleccionado automáticamente por el asistente, o un certificado que ha sido creado y/o seleccionado de modo manual por medio del botón <i>Cambiar...</i>
 <i>Cambiar...</i>	Haga clic sobre este botón para crear y/o seleccionar un certificado de encriptación de modo manual. Aparecerá en pantalla el diálogo Selección de certificado .  Reconfiguración de claves para los datos

	<p>encriptados existentes: Por favor tenga en cuenta que aún se necesita el certificado de encriptación anterior para desencriptar los datos encriptados existentes. El proceso de reconfiguración de claves requerido para usar el nuevo certificado con los datos existentes depende de su sistema operativo:</p> <p>En los sistemas operativos que incluyen el asistente de reconfiguración de claves Sistema de archivos de encriptación Microsoft (por ejemplo, Windows 7 o Windows Vista), se debe realizar la reconfiguración de claves de modo manual.</p> <p>En todos los demás sistemas operativos se debe utilizar la herramienta de línea de comando "cipher.exe" o acceder a los archivos en cuestión para reconfigurar las claves de modo automático</p> <p>Se encuentra disponible más información en Microsoft TechNet (buscar "asistente de reconfiguración de claves" o "cipher.exe").</p>
<p> <i>Longitud clave para nuevos certificados</i></p>	<p>Aquí puede seleccionar la longitud de clave para los certificados de encriptación recientemente creados, por ejemplo <i>1024 bits</i> o <i>2048 bits</i>.</p>



La solución Infineon Security Platform - Asistente para la inicialización de usuarios

Configuración del Sistema de archivos de encriptación (EFS)

Por medio de esta página del asistente se podrá configurar un acceso fácil a los datos de EFS encriptados. También le permite revertir a Microsoft EFS sin protección de Security Platform.

La siguiente tabla le muestra algunos consejos sobre cómo utilizar la página del asistente.

Elemento de la página del asistente	Explicación
<input checked="" type="checkbox"/> <i>Carpeta EFS</i>	<p>Seleccione esta opción para crear una carpeta encriptada <i>Documentos\Datos encriptados</i> o <i>Mis Documentos\Datos encriptados</i> (dependiendo de su sistema operativo).</p> <p> Esta opción no se encuentra disponible siempre (p. ej. si ya ha creado antes la carpeta EFS o debido a la configuración de desktop.ini o a un tipo de sistema de archivos FAT32).</p>
<input checked="" type="checkbox"/> <i>Atajo de escritorio</i>	<p>Seleccione esta opción si desea acceder a su <i>carpeta EFS</i> por medio de un atajo de escritorio.</p> <p> Si destilda la casilla de verificación cuando ya había creado antes el <i>Atajo de escritorio</i>, el asistente borrará el atajo existente (siempre y cuando no haya sido renombrado o movido en el ínterin).</p>
<input type="checkbox"/> <i>Revertir...</i>	<p>Haga clic aquí para revertir a la funcionalidad de EFS predeterminada (Microsoft EFS) sin la protección de Security Platform.</p> <p>Luego de revertir a Microsoft EFS, la encriptación de archivos y carpetas funcionará de la siguiente manera:</p> <ul style="list-style-type: none">• Podrá acceder a todos sus datos encriptados, siempre que su clave privada y certificado EFS estén en condiciones de uso. Luego de revertir el

EFS, el primer acceso a un archivo encriptado con la Solución Security Platform requiere de su certificado EFS, de su clave privada y de su [autenticación del usuario](#). Una vez que se accedió a dicho archivo, el mismo se reencryptará automáticamente con el nuevo certificado de Microsoft EFS.

- Los archivos nuevos se encriptarán con el Microsoft EFS incluido en su sistema operativo (sin protección de Security Platform).

Recomendación: [Desencripte](#) los archivos EFS existentes si no puede asegurar que su clave privada y certificado EFS estarán en condiciones de uso, siempre que desee tener acceso a dichos archivos.



Este botón está disponible sólo si ya se ha configurado EFS anteriormente y se opta por configurarlo nuevamente.



©Infineon

La Solución Infineon Security Platform

Personal Secure Drive

Con las páginas del asistente del Personal Secure Drive se pueden cambiar las configuraciones de un Personal Secure Drive existente, borrar un Personal Secure Drive existente o crear un nuevo Personal Secure Drive. La configuración del Personal Secure Drive forma parte del [Asistente para la inicialización de usuarios](#). Aparecen en pantalla las páginas en cuestión si selecciona la función *Encriptación de archivos y carpetas con Personal Secure Drive (PSD)*.

Pasos y páginas del asistente

La siguiente tabla detalla los pasos y páginas del asistente relacionados con Personal Secure Drive.

Acción	Pasos/Páginas del asistente
Cambiar las configuraciones de un PSD existente	<ol style="list-style-type: none">1. Administración de sus Personal Secure Drives2. Cambio de configuración de su Personal Secure Drive
Borrar un PSD existente	<ol style="list-style-type: none">1. Administración de sus Personal Secure Drives2. Eliminación de su Personal Secure Drive
Crear un nuevo PSD	<ol style="list-style-type: none">1. Administración de sus Personal Secure Drives (sólo si existe al menos un PSD)2. Especificación de una etiqueta y una letra de unidad para su Personal Secure Drive3. Configuración de su Personal Secure Drive

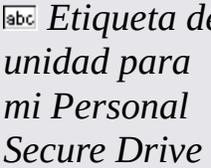


La Solución Infineon Security Platform

Especificación de una etiqueta y una letra de unidad para su Personal Secure Drive

Por medio de esta página se pueden configurar la etiqueta y la letra de unidad de su Personal Secure Drive, además de aprender a utilizar las opciones para cargar el PSD al inicio de sesión y para utilizar un atajo de escritorio.

La siguiente tabla le muestra algunos consejos sobre cómo utilizar la página del asistente.

Elemento de la página del asistente	Explicación
 <i>Mi Personal Secure Drive se mapeará a la unidad</i>	Para especificar la letra de unidad para su Personal Secure Drive, seleccione una letra que no utilice de la lista desplegable de letras disponibles (vea Administración de Personal Secure Drive).
 <i>Etiqueta de unidad para mi Personal Secure Drive</i>	Para especificar una etiqueta de unidad, ingrese la etiqueta en el campo provisto. La etiqueta no debe tener más de 32 caracteres de longitud. Por ejemplo, podría establecer la etiqueta como "Mi unidad segura".
<input checked="" type="checkbox"/> <i>Cargar mi Personal Secure Drive al inicio de sesión</i>	Seleccione esta opción si desea cargar su PSD al inicio de sesión.
<input checked="" type="checkbox"/> <i>Crear atajo de escritorio</i>	Seleccione esta opción si desea acceder a su PSD por medio de un atajo de escritorio. El nombre del atajo incluirá la letra de unidad y la etiqueta.



La Solución Infineon Security Platform

Configuración de su Personal Secure Drive

Al utilizar su Personal Secure Drive éste se parece y se comporta como cualquier otra unidad, pero no es una unidad física agregada a su computadora: es un archivo encriptado en una de sus unidades locales de la computadora. Al configurar su Personal Secure Drive, debe especificar cuán grande debe ser, y en qué unidad local se debe guardar.

La siguiente tabla detalla los indicios para utilizar la página del asistente.

Elementos de diálogo	Explicación
<p><input type="checkbox"/> <i>Espacio de almacenamiento</i></p>	<p>Espacio de almacenamiento para especificar el tamaño de la unidad, ingrese la cantidad de megabytes (MB) de memoria que requiera en el campo provisto o utilice las flechas hacia arriba y hacia abajo al costado derecho del campo para seleccionar el tamaño. Tenga en cuenta que también se soportan unidades locales con medios extraíbles (por ejemplo, memoria USB).</p> <p>La cantidad requerida de espacio en disco está reservada en esta unidad local para uso exclusivo de Personal Secure Drive. Por favor asegúrese de que haya suficiente espacio libre en la unidad local para su Personal Secure Drive.</p> <p> En el modo servidor, se recomienda la creación de un PSD en un medio extraíble si desea utilizarlo en más de una plataforma (ver Introducción al Personal Secure Drive). En este caso utilice una letra de unidad que esté disponible en todas las plataformas.</p>
<p><input type="checkbox"/> <i>Seleccione la unidad donde se guardará el archivo imagen PSD.</i></p>	<p>Seleccione una unidad donde se guardará el archivo imagen PSD.</p> <p> La selección de unidad se encuentra deshabilitada si está establecida la política de Ubicación de archivos para Personal Secure Drive.</p>

Tamaño de PSD máximo

El tamaño de su Personal Secure Drive no se puede cambiar luego de la configuración, así que asegúrese de que el tamaño asignado es lo suficientemente grande para cubrir sus necesidades.

Observe que no puede utilizar el tamaño máximo de la unidad, ya que el sistema de archivos utiliza algo de espacio. Esto depende del sistema operativo y puede ser significativo para tamaños de disco pequeños. Además, el almacenamiento de algunos datos PSD internos reduce levemente el tamaño de PSD máximo.

Observe también que el tamaño máximo de la unidad PSD está limitado:

- El tamaño máximo para la unidad PSD en unidades FAT16 es de 2GB
- El tamaño máximo para la unidad PSD en unidades FAT32 es de 4GB.
- El tamaño máximo para la unidad PSD en la partición del sistema se puede restringir mediante la política [*Espacio libre mínimo luego de la creación del PSD.*](#)



La Solución Infineon Security Platform

Administración de los Personal Secure Drives

Por medio de esta página se pueden cambiar las configuraciones de un Personal Secure Drive existente, borrar un Personal Secure Drive existente o crear un nuevo Personal Secure Drive. Esta página aparece en pantalla si se ha seleccionado la función *Encriptación de archivos y carpetas con Personal Secure Drive (PSD)* y si ya existe al menos un Personal Secure Drive. Tenga en cuenta que se debe ejecutar varias veces el asistente para realizar diferentes acciones o para crear varios Personal Secure Drives.

La siguiente tabla le muestra algunos consejos sobre cómo utilizar la página del asistente.

Página del asistente Elemento	Explicación
<input type="checkbox"/> <i>Personal Secure Drive (s) existente</i>	La lista detalla todos sus Personal Secure Drives y sus estados actuales. Se puede actualizar la lista con la tecla "F5". Si desea cambiar las configuraciones de un Personal Secure Drive existente o borrar un Personal Secure Drive existente, debe seleccionar la unidad en cuestión.
<input checked="" type="radio"/> <i>Cambiar las configuraciones del PSD seleccionado</i>	Seleccione esta opción si desea cambiar las configuraciones del Personal Secure Drive seleccionado (por ejemplo la letra de unidad, la etiqueta y las opciones para cargar el PSD al inicio de sesión y para utilizar un atajo de escritorio). El asistente continuará con la página Cambio de configuraciones del Personal Secure Drive .
<input checked="" type="radio"/> <i>Borrar el PSD seleccionado</i>	Seleccione esta opción si desea borrar el Personal Secure Drive seleccionado. El asistente continuará con la página Eliminación del Personal Secure Drive .
<input checked="" type="radio"/> <i>Crear un nuevo PSD</i>	Seleccione esta opción si desea crear un nuevo Personal Secure Drive. El asistente continuará con las páginas para crear un nuevo PSD .



TPM

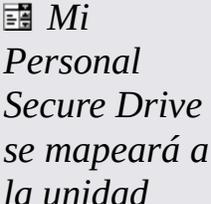
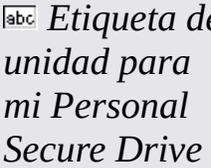
©Infineon Technologies AG

La Solución Infineon Security Platform

Cambio de configuración de su Personal Secure Drive

Por medio de esta página se pueden cambiar la etiqueta y la letra de unidad de su Personal Secure Drive, además de aprender a utilizar las opciones para cargar el PSD al inicio de sesión y para utilizar un atajo de escritorio.

La siguiente tabla le muestra algunos consejos sobre cómo utilizar la página del asistente.

Página del asistente Elemento	Explicación
	Para cambiar la letra de unidad para su Personal Secure Drive, seleccione una letra que no utilice de la lista desplegable de letras disponibles (vea Administración de Personal Secure Drive).
	Para cambiar la etiqueta de unidad, ingrese otra etiqueta en el campo provisto. La etiqueta no debe tener más de 32 caracteres de longitud. Por ejemplo, podría establecer la etiqueta como "Mi unidad segura".
<input checked="" type="checkbox"/> <i>Cargar mi Personal Secure Drive al inicio de sesión</i>	Seleccione esta opción si desea cargar su PSD al inicio de sesión.
<input checked="" type="checkbox"/> <i>Atajo de escritorio</i>	Seleccione esta opción si desea acceder a su PSD por medio de un atajo de escritorio. El nombre del atajo incluirá la letra de unidad y la etiqueta.  Si destilda la casilla de verificación cuando ya había creado un atajo de escritorio con anterioridad, el asistente borrará el atajo existente (siempre y cuando no haya sido renombrado o movido en el ínterin).



Technologies AG

La Solución Infineon Security Platform

Eliminación de su Personal Secure Drive

Si elige borrar su Personal Secure Drive, se le da la opción de crear una copia no encriptada de la unidad completa antes de borrarla permanentemente.

Nota: Al presionar **Siguiente**, borrará *permanentemente* su Personal Secure Drive - y ya *no* podrán recuperar los datos.

Para crear una copia no encriptada de su Personal Secure Drive antes de borrarlo, haga clic en el botón de radio *Deseo guardar una copia no encriptada de los contenidos de mi Personal Secure Drive antes de borrarlos permanentemente*, luego especifique la ubicación en la cual se van a guardar en un formato no encriptado.

Para borrar permanentemente su Personal Secure Drive sin crear una copia no encriptada, haga clic en el botón de radio *Deseo borrar permanentemente mi Personal Secure Drive sin guardar una copia no encriptada de su contenido*.



©Infineon

Technologies AG

La Solución Infineon Security Platform - Asistente para la migración

Asistente para la migración de Infineon Security Platform

El asistente para la migración de Infineon Security Platform se utiliza para transferir certificados y claves específicas del Usuario de Infineon Security Platform desde una Infineon Security Platform a otra por una vía segura.

Cada destino de migración debe ser autorizado por el Propietario de Infineon Security Platform antes de poder realizar la operación de exportación. Esto provee medios administrativos para mantener un registro de la distribución de los usuarios de Infineon Security Platform, aún en redes de gran escala.

La operación de migración debe realizarse por los usuarios de Infineon Security Platform y consiste de la exportación del Infineon Security Platform de origen y la correspondiente operación de importación en el Infineon Security Platform de destino. Nunca puede realizarse una migración para una cuenta diferente a la del usuario en sesión. Esto asegura la confiabilidad de Infineon Security Platform desde el punto de vista del usuario que lo utiliza.

No es posible realizar una operación de migración si el usuario actualmente en sesión no posee una clave de usuario básico o si Infineon Security Platform está deshabilitado (en forma permanente o temporal).



Disponibilidad del asistente:

- En el modo [stand-alone](#), este asistente sólo se encuentra disponible en un Security Platform inicializado.
- Este asistente no está disponible en el [modo servidor](#) ya que Trusted Computing Management Server realiza la tarea de migración de los certificados y claves específicos del usuario desde un Infineon Security Platform a otro, de manera segura.

Pasos del asistente

Paso	Comentario
1. Importar o exportar?	Especifique si desea importar sus claves y certificados desde una Security Platform o exportarlos hacia otra Security Platform.
2. Destino de la exportación	Especifique la computadora de destino de la migración (sólo cuando <i>Exportar</i> se ha seleccionado).
3. Ubicación del archivo a importar o Ubicación del archivo a exportar	Especifique la ubicación del archivo de datos de la migración.
4. Ingrese la contraseña o autenticación	Autentíquese para autorizar la migración.

Inicio de la aplicación

Inicie el asistente para la migración por medio de la Herramienta de Configuración: [Herramienta de Configuración - Migración - Exportar...](#) o [Herramienta de Configuración - Migración - Importar...](#)

Si desea exportar sus claves y certificados, seleccione *Esta es la plataforma de origen*.

Si desea importar sus claves y certificados, seleccione *Esta es la plataforma de destino*.



©Infineon Technologies AG

La Solución Infineon Security Platform - Asistente para la migración

Importar o exportar

Debe definirse la operación de migración para las claves de usuario. Es posible importar cualquiera de sus claves y certificados de otra Security Platform o exportarlos hacia otra Security Platform.



Esta página del asistente no está disponible en el [modo servidor](#), ya que la migración es llevada a cabo por Trusted Computing Management Server.

Elemento de la página del asistente	Explicación
⦿ <i>Importar</i>	Las siguientes operaciones importarán certificados y claves de usuarios específicos de Infineon Security Platform desde un archivo de migración a la Infineon Security Platform local. Debe conocerse la ubicación del archivo de migración.
⦿ <i>Exportar</i>	Las siguientes operaciones crearán un archivo de migración conteniendo claves y certificados del usuario actualmente en sesión en el Infineon Security Platform. El Propietario de Infineon Security Platform debe conocer y autorizar el Infineon Security Platform de destino.



©Infineon

La Solución Infineon Security Platform - Asistente para la migración

Especificación de la ubicación del archivo de importación

Se requiere el archivo de migración que contiene sus claves y certificados, el cual fue creado durante la operación de exportación.



Esta página del asistente no está disponible en el [modo servidor](#), ya que la migración es llevada a cabo por Trusted Computing Management Server.

Elemento de la página del asistente	Explicación
<input type="text"/> <i>Ubicación de archivo</i> <input type="checkbox"/> <i>Examinar...</i>	La información de la migración será leída de un archivo. Ingrese la ruta de acceso y el nombre del archivo de datos de migración o examine para buscarlo.  El migración está en formato XML.



La Solución Infineon Security Platform - Asistente para la migración

Especificar la ubicación del archivo de exportación

Las claves y certificados a ser migrados están guardados de forma segura en el archivo de migración. Este archivo, necesitado para completar la migración, puede importarse solo en una máquina autorizada por el propietario de la plataforma.



Esta página del asistente no está disponible en el [modo servidor](#), ya que la migración es llevada a cabo por Trusted Computing Management Server.

Elemento de la página del asistente	Explicación
<input type="text"/> <i>Ubicación de archivo</i> <input type="checkbox"/> <i>Examinar...</i>	La información de la migración será guardada en un archivo. Ingrese la ruta de acceso y el nombre del archivo de datos de migración o examine para buscarlo.
	La migración está en formato XML.



La Solución Infineon Security Platform - Asistente para la migración

Especifique el destino de la exportación

El propietario de Infineon Security Platform debe en primera instancia autorizar a cada Infineon Security Platform que se quiera utilizar como destino válido para una operación de migración. Se debe realizar esta operación en cada uno de los Infineon Security Platform de una red.



Esta página del asistente no está disponible en el [modo servidor](#), ya que la migración es llevada a cabo por Trusted Computing Management Server.

Elemento de la página del asistente	Explicación
<input type="checkbox"/> <i>Seleccione su Security Platform de destino</i>	<p>La lista de selección contiene todos los sistemas Infineon Security Platform que son destinos válidos para certificados y claves de usuario en el Infineon Security Platform local. Debe seleccionarse una de las entradas en la lista como destino para la operación de migración actual.</p> <p> Si no hay un destino disponible en la lista, debe detenerse el asistente para la migración de Infineon Security Platform utilizando el botón Cancelar . El Propietario del Infineon Security Platform local debe autorizar la migración para Infineon Security Platform local por medio de la Herramienta para la Configuración de Infineon Security Platform.</p>



©Infineon

Solución Infineon Security Platform - Asistente para la copia de seguridad

Asistente para la copia de seguridad de Infineon Security Platform

El asistente para la copia de seguridad de Infineon Security Platform se utiliza para llevar a cabo las operaciones para la copia de seguridad o de restauración de los [datos relacionados con Security Platform](#). Estas operaciones son necesarias para proteger los datos de pérdidas accidentales en caso de emergencia.

El archivo de copia de seguridad contiene la información de identificación de la computadora ("ID de plataforma") y la información de identificación del usuario ("ID de usuario"). Dicha información se utiliza para hacer corresponder el nombre de la máquina y el nombre de usuario con la máquina y usuario actuales durante el proceso de restauración.



Si el actual Clave básica de usuario es diferente del Clave básica de usuario que se va a recuperar, el proceso de recuperación sustituirá a las credenciales y a los valores instalados en la ubicación del destino. Por lo tanto se recomienda que restaure las credenciales de usuario a una cuenta de usuario en el sistema de destino que no haya llevado a cabo los pasos para la inicialización de usuarios de Security Platform.



En el [modo servidor](#), las copias de seguridad y restauraciones son llevadas a cabo por Trusted Computing Management Server, es decir que no se necesita ninguna configuración explícita. Si el Personal Secure Drive (PSD) ha sido configurado, se puede hacer una copia de seguridad y restaurar archivos imagen de Personal Secure Drive en forma manual.



Este icono de escudo sólo es visible para los usuarios con derechos administrativos bajo sistemas operativos con [Control de cuentas de usuario](#) (por ej. Windows 7 y Windows Vista).

Pasos del asistente

Escenario	Pasos del asistente	Explicación
Copia de seguridad manual	Configurar los valores de la copia de seguridad	Paso requerido.
	Configurar los valores de la copia de seguridad de PSD	Sólo si los Personal Secure Drives serán incluidos en la copia de seguridad.
Restauración	Configurar los valores de restauración	No se requieren si sólo se restaurarán los Personal Secure Drives.
	Confirmar computadora o seleccionar computadora	Sólo si su computadora no figura en los datos de la copia de seguridad. No se requieren si sólo se restaurarán los Personal Secure Drives.
	Seleccionar la tarjeta de seguridad de recuperación de emergencia	Sólo si posee derechos administrativos, si la copia de seguridad incluye datos de Recuperación de emergencia y si los datos de Recuperación de emergencia serán restaurados. No se requieren si sólo se restaurarán los Personal Secure Drives.
	Confirmar usuario	Sólo si se restaurarán credenciales y configuraciones para la cuenta del usuario actual, y si el usuario en los datos de copia de seguridad difiere del usuario actual.

		No se requieren si sólo se restaurarán los Personal Secure Drives.
	Seleccionar usuarios	Sólo si posee derechos administrativos y si se preparará la restauración para otros usuarios. No se requieren si sólo se restaurarán los Personal Secure Drives.
	Configurar los valores de restauración de PSD	Sólo si se restauran los Personal Secure Drives.

Tenga en cuenta que no se necesita utilizar el Asistente de copia de seguridad para realizar una Copia de seguridad del sistema, ya que la tarea de copia de seguridad programada y configurada por medio del Asistente de inicialización de Security Platform o del Asistente de inicialización rápida realiza de modo automático la Copia de seguridad del sistema.

Inicio de la aplicación

Copia de seguridad manual: Inicie el asistente para la copia de seguridad mediante la Herramienta de Configuración: [Herramienta de Configuración - Copia de seguridad - Copia de seguridad...](#)

Restauración manual: Inicie el asistente para la copia de seguridad mediante la Herramienta de Configuración: [Herramienta de Configuración - Copia de seguridad - Restaurar...](#)

Restauración incluyendo la recuperación de emergencia (Tarea administrativa): Primero inicie el asistente para la inicialización de Security Platform. Verifique [Restaurar un Security Platform desde un paquete de archivos de la copia de seguridad](#) en la página del asistente *Inicializar o restaurar un Security Platform*.

El asistente se inicia desde un globo de texto o desde el Icono de Notificación de la Barra de tareas: El asistente se inicia desde un globo de texto o desde el [Icono de Notificación de la Barra de tareas](#) de acuerdo a ciertos estados en los que se encuentre Security Platform (por ejemplo, al preparar la restauración del usuario actual por parte del administrador de Security Platform).



La Solución Infineon Security Platform - Asistente para la inicialización

Realizar copia de seguridad o restaurar

Seleccione una opción para crear una copia de seguridad o restaurar sus datos.

Elemento de la página del asistente	Explicación
<p> <i>Crear una copia de seguridad manual</i></p>	<p>Las operaciones siguientes crearán una copia de seguridad de sus datos de credencial desde un Infineon Security Platform local a un medio seguro de preferencia un medio extraíble como una unidad de memoria, un disco duro o el servidor. Se puede restaurar en caso de pérdida de datos. Se debe conocer la ubicación de la copia de seguridad.</p> <p> En el modo servidor, sólo puede realizar copias de seguridad de su Personal Secure Drive (PSD).</p>
<p> <i>Restaurar desde una copia de seguridad manual</i></p>	<p>Las operaciones siguientes restaurarán los datos que anteriormente se guardaron en una copia de seguridad al Infineon Security Platform. El usuario debe proveer la ubicación del archivo de copia de seguridad para el proceso de restauración.</p> <p> En el modo servidor, sólo puede restaurar su Personal Secure Drive (PSD).</p>
<p> <i>Restaurar desde una copia de seguridad del sistema</i></p>	<p>Las siguientes operaciones restaurarán al Infineon Security Platform los datos de credencial previamente guardados en copia de seguridad. Para el proceso de restauración el usuario debe ingresar la ubicación del archivo guardado. Si no cuenta con un Archivo de Copia de seguridad del sistema, también puede restaurarlo desde un archivo guardado manualmente. También se puede realizar una restauración de recuperación de emergencia.</p> <p> <ul style="list-style-type: none">• Este botón no se encuentra disponible si el usuario no cuenta con derechos</p>

administrativos.

- En el [modo servidor](#), este botón no está disponible ya que la copia de seguridad y restauración son llevadas a cabo por Trusted Computing Management Server.



La Solución Infineon Security Platform - Asistente para la copia de seguridad

Configuración de valores de copia de seguridad

Con esta página se puede especificar el paquetes de archivos de la copia de seguridad.



En el [server mode](#), Esta página no se encuentra disponible en el modo servidor, ya que la copia de seguridad es manejada por Trusted Computing Management Server.

La siguiente tabla le muestra algunos consejos sobre cómo utilizar la página del asistente.

Elemento de la página del asistente	Explicación
<input type="checkbox"/> <i>Grupo de archivos de la copia de seguridad.</i> <input type="checkbox"/> <i>Examinar...</i>	Y Sus credenciales y valores de Security Platform se guardarán en el paquete de archivos de copia de seguridad. Escriba la ruta y nombre de archivo o búsquelos.  El archivo de copia de seguridad es un archivo en formato XML.



La solución Infineon Security Platform - Asistente para la copia de seguridad

Configurar los valores de asistente para la copia de seguridad de Personal Secure Drive

Por medio de esta página se puede realizar la copia de seguridad de archivos imagen de un Personal Secure Drive. Los valores de PSD siempre se encuentran incluidos en la copia de seguridad si ha configurado un PSD, pero los archivos imagen deben ser explícitamente seleccionados para ser incluidos en la copia de seguridad.

La siguiente tabla le muestra algunos consejos sobre cómo utilizar la página del asistente.

Página del asistente Elemento	Explicación
<p> <i>Destino de la copia de seguridad del Personal Secure Drive predeterminado</i></p> <p> <i>Examinar...</i></p>	<p>Si desea realizar una copia de seguridad de uno o más archivos imagen del Personal Secure Drive, deberá especificar la ruta de destino predeterminada para los archivos imagen de copia de seguridad. Si desea realizar una copia de seguridad de varios archivos imagen para diferentes ubicaciones, deberá utilizar el botón <i>Cambiar...</i> para establecer las rutas de modo individual.</p> <p>Si no desea realizar ninguna copia de seguridad del Personal Secure Drive, se puede ignorar la selección de ruta.</p>
<p> <i>Seleccionar las Personal Secure Drives a ser incluidas en la copia de seguridad</i></p>	<p>La lista detalla todos los Personal Secure Drives configurados en la plataforma. Seleccionar las unidades a ser incluidas en la copia de seguridad. Asegúrese de que se haya especificado un archivo imagen de copia de seguridad válido para cada unidad seleccionada, y de que haya suficiente espacio libre en la carpeta de destino.</p> <p>Si no desea realizar ninguna copia de seguridad del archivo imagen del Personal Secure Drive, asegúrese de que ningún Personal Secure Drive esté tildado.</p>

	<p>Menú de contexto: Haga clic con el botón derecho sobre la lista para desplegar el menú de contexto con todas las acciones admitidas.</p>
<input type="checkbox"/> <i>Cambiar...</i>	<p>Haga clic sobre este botón para cambiar la ubicación de la copia de seguridad y/o el nombre de archivo del archivo imagen de la copia de seguridad. Aparecerá en pantalla un diálogo. Realice los cambios allí y cierre nuevamente el diálogo.</p> <p> No cambie la extensión de archivo *.fsb del archivo imagen de copia de seguridad.</p>



La Solución Infineon Security Platform - Asistente para la copia de seguridad

Configurar los valores de restauración

Por medio de esta página puede especificar e paquete de archivos de copia de seguridad para restarurar. Si posee derechos de administración, también puede especificar una razón para la restauración.



Disponibilidad de la página: En el [modo servidor](#) esta página no está disponible ya que las copias de seguridad y restauraciones son llevadas a cabo por el Trusted Computing Management Server, es decir que no es necesaria una configuración explícita.

La siguiente tabla le muestra algunos consejos sobre cómo utilizar la página del asistente.

Elemento de la página del asistente	Explicación
<ul style="list-style-type: none">⦿ <i>Disco duro dañado o datos perdidos</i>⦿ <i>Nueva Trusted Platform Module</i>⦿ <i>Nuevo Security Platform a inicializar</i>	<p>Dependiendo del estado de Security Platform se selecciona una de las siguientes razones de restauración:</p> <ul style="list-style-type: none">• <i>Disco duro dañado o datos perdidos:</i> Security Platform posee un propietario. Este estado ocurre por lo general, si se inicializó la Solución de Security Platform y se encuentra lista para utilizar, pero algunos datos ya no se pueden acceder.• <i>Nueva Trusted Platform Module:</i> Security Platform no posee un propietario, pero ya existen una configuración anterior de Security Platform ó credenciales. Este estado ocurre por lo general, si se instaló Security Platform anteriormente, y luego se reemplazó el Trusted Platform Module ó se restableció desde la BIOS.• <i>Nuevo Security Platform a inicializar:</i> Security Platform no posee un propietario. No se pudieron

	<p>encontrar credenciales ó alguna configuración anterior de Security Platform.</p> <p>Este estado ocurre por lo general, si ejecutará una restauración sobre una PC, sobre la cual no se instaló anteriormente la Solución de Security Platform.</p> <p>Advierta que no puede cambiar esta selección.</p> <p> La razón de restauración sólo se muestra a los usuarios con derechos de administración.</p>
<p> <i>Especifique la ruta y el nombre de archivo del paquete de archivos de copia de seguridad a restaurar</i></p> <p> <i>Examinar...</i></p>	<p>Necesita especificar el paquete de archivos desde el que desea restaurar.</p> <p>Ingrese la ruta y el nombre del archivo o examine para buscarlo.</p> <p> El archivo de copia de seguridad está en formato XML.</p>



La Solución Infineon Security Platform - Asistente para la copia de seguridad

Configurar los valores de restauración de Personal Secure Drive

Por medio de esta página se pueden restaurar los Personal Secure Drives. Se puede utilizar la copia de seguridad de un archivo imagen de un PSD para un PSD ya configurado, o se puede configurar un nuevo PSD para utilizar este archivo imagen restaurado.

La siguiente tabla le muestra algunos consejos sobre cómo utilizar la página del asistente.

Elemento de la página del asistente	Explicación
<p><input type="text"/> <i>Ubicación de la copia de seguridad del Personal Secure Drive predeterminado</i></p> <p><input type="button" value="Examinar..."/></p>	<p>Si desea restaurar uno o más Personal Secure Drives, deberá especificar la ruta predeterminada de las copias de seguridad de los archivos imagen de PSD a ser restaurados. Esta ruta será considerada la ruta de restauración predeterminada para todos los archivos imagen de PSD. Si desea restaurar varios archivos imagen desde diferentes ubicaciones, deberá utilizar el botón <i>Cambiar...</i> para establecer las rutas de modo individual.</p> <p>Si no desea restaurar ningún Personal Secure Drive, se puede ignorar la selección de ruta.</p>
<p><input type="checkbox"/> <i>Seleccionar las Personal Secure Drives a ser restauradas</i></p>	<p>La lista detalla todos los Personal Secure Drives configurados en la plataforma. Seleccione las unidades a ser restauradas y asegúrese de que se haya especificado una copia de seguridad de archivo imagen válido para cada unidad seleccionada.</p> <p>La lista podría incluir unidades con estados diferentes:</p> <ul style="list-style-type: none">• Personal Secure Drives que son totalmente funcionales (es decir, se encuentran disponibles los valores PSD y el archivo imagen). Quizás querría por ejemplo restaurar una unidad totalmente

funcional si ha borrado por error algunos archivos en su PSD, y la copia de seguridad del archivo imagen contiene estos archivos. Tenga en cuenta que los datos actuales de su PSD serán sobrescritos en su totalidad en ese caso.

- Personal Secure Drives con archivo imagen faltante (por ejemplo si acaba de restaurar los valores de PSD desde un Grupo de archivos de copia de seguridad, pero el archivo imagen aún tiene que ser restaurado). En ese caso deberá restaurar la copia de seguridad del archivo imagen antes de poder acceder a los datos del PSD.
- Personal Secure Drives para los cuales no se encuentra disponible una clave aplicable. En ese caso se puede restaurar una copia de seguridad del archivo imagen que utiliza la clave esperada. Pero considere recuperar primero los credenciales y valores de configuración, después puede no necesitar recuperar el archivo de imagen.

Si no desea restaurar ningún Personal Secure Drive, asegúrese de que ningún Personal Secure Drive esté tildado.

Menú de contexto: Haga clic con el botón derecho sobre la lista para desplegar el menú de contexto con todas las acciones admitidas.

Agregar...

Haga clic sobre este botón para añadir otro Personal Secure Drive a la lista de unidades. De este modo podrá restaurar un Personal Secure Drive desde una copia de seguridad de un archivo imagen sin tener copia de seguridad de los valores correspondientes. Aparecerá en pantalla un [diálogo](#) desde donde podrá configurar todos los valores de PSD relevantes.

Cambiar...

Haga clic sobre este botón para establecer o cambiar los valores de restauración del Personal Secure Drive seleccionado.

Por ejemplo, se debe hacer esto en los siguientes casos:

- No se pudo encontrar ninguna copia de seguridad del archivo imagen adecuado en la ubicación de copia de seguridad del PSD predeterminado.
- Se pudo encontrar una copia de seguridad del archivo imagen adecuado en la ubicación de copia de seguridad del PSD predeterminado, pero usted desea seleccionar otra copia de seguridad de archivo imagen válido.
- El estado local del PSD seleccionado requiere que se cambie el destino del archivo imagen o la letra de unidad.

Aparecerá en pantalla un [diálogo](#) desde donde podrá configurar todos los valores de PSD relevantes.



La Solución Infineon Security Platform - Asistente para la copia de seguridad

Cambiar valores de restauración/Añadir Personal Secure Drive

Por medio de este diálogo se podrán establecer o cambiar las configuraciones de un Personal Secure Drive o añadir otro Personal Secure Drive a ser restaurado. Sólo se habilitan los controles requeridos dependiendo de la acción a ser realizada.

La siguiente tabla le muestra algunos consejos sobre cómo utilizar este diálogo:

Elemento de la página del asistente	Explicación	Cambiar	Añadir
<input type="text"/> <i>Ruta de la copia de seguridad del archivo imagen</i> <input type="button" value="Examinar..."/>	Especifique la ruta de la copia de seguridad del archivo imagen a ser restaurado.	Debe ser establecido si no encuentra ninguna copia de seguridad del archivo imagen adecuado en la ubicación de copia de seguridad del PSD predeterminado. De lo contrario se puede cambiar la ruta.	Debe ser establecido
<input type="listbox"/> <i>Unidad de destino del archivo imagen</i>	Seleccione la unidad donde se restaurará el archivo imagen de PSD.	Debe ser establecido si no es posible restaurar la copia de seguridad del archivo imagen a la unidad de destino almacenada en las	Debe ser establecido

		configuraciones locales. De lo contrario la unidad de destino no puede ser cambiada.	
 <i>Letra de unidad</i>	Para especificar la letra de unidad para su Personal Secure Drive, seleccione una letra que no utilice de la lista desplegable de letras disponibles (vea Administración de Personal Secure Drive).	Debe ser establecido si no es posible utilizar la letra de unidad almacenada en las configuraciones locales. De lo contrario la letra de unidad no puede ser cambiada.	Debe ser establecido
 <i>Etiqueta de unidad</i>	Para especificar la etiqueta de unidad, ingrese la etiqueta en el campo provisto. La etiqueta no debe tener más de 32 caracteres de longitud. Por ejemplo, podría establecer la etiqueta como "Mi unidad segura".	No se puede cambiar	Debe ser establecido
<input checked="" type="checkbox"/> <i>Cargar al iniciar sesión</i>	Seleccione esta opción si desea cargar su PSD al inicio de sesión.	No se puede cambiar	Opcional
<input checked="" type="checkbox"/> <i>Crear atajo de escritorio</i>	Seleccione esta opción si desea acceder a su PSD por medio de un atajo de escritorio. El nombre del atajo incluirá la letra de unidad y la etiqueta.	No se puede cambiar	Opcional



TPM

©Infineon Technologies AG

La Solución Infineon Security Platform - Asistente para la copia de seguridad

Confirmar computadora

Esta página le pide confirmación para restaurar la computadora desde los datos de la copia de seguridad especificada a su computadora.



Disponibilidad de la página:

- Esta página sólo aparece si los datos de la copia de seguridad especificada contiene datos para otra computadora diferente de la suya.
- En el [modo servidor](#), esta página no está disponible ya que la copia de seguridad y restauración son llevadas a cabo por Trusted Computing Management Server.

La tabla a continuación le muestra algunos consejos sobre cómo utilizar la página del asistente.

Elemento de la página del asistente	Explicación
<i>Su computadora: Nombre de la computadora / ID de la plataforma</i>	Aparece el nombre de su computadora y el ID de plataforma. Observe que el nombre de la computadora pudo cambiar desde que se realizó la copia de seguridad, ya que puede renombrarse. Es por ello que también se muestra el ID de la plataforma.
<i>Computadora en los datos de la copia de seguridad: Nombre de la computadora / ID de la plataforma</i>	Aparece el nombre de la computadora y el ID de plataforma para la computadora en la que se realizó la copia de seguridad.



©Infineon

La Solución Infineon Security Platform - Asistente para la copia de seguridad

Seleccionar computadora

Por medio de esta página puede seleccionar la computadora a restaurar.



Disponibilidad de la página:

- Esta página sólo aparece si los datos de la copia de seguridad especificada contiene datos para varias computadoras pero no para la suya.
- En el [modo servidor](#), esta página no está disponible ya que la copia de seguridad y restauración son llevadas a cabo por Trusted Computing Management Server.

La tabla a continuación le muestra algunos consejos sobre cómo utilizar la página del asistente.

Elemento de la página del asistente	Explicación
 <i>Su computadora: Nombre de la computadora / ID de la plataforma</i>	Aparece el nombre de su computadora y el ID de plataforma.  Observe que el nombre de la computadora pudo cambiar desde que se realizó la copia de seguridad, ya que puede renombrarse. Es por ello que también se muestra el ID de la plataforma.
 <i>Computadora en los datos de la copia de seguridad: Nombre de la computadora / ID de la plataforma</i>	Aparece el nombre de la computadora y el ID de plataforma para las computadoras en las que se realizaron las copias de seguridad. Seleccione una de estas computadoras para restaurar.



La Solución Infineon Security Platform - Asistente para la inicialización

Seleccione la tarjeta de seguridad de recuperación de emergencia

Si el proceso de restauración incluye la recuperación de emergencia, entonces necesita especificar una tarjeta de seguridad para recuperación de emergencia. Con esta página usted puede especificar esta tarjeta.

Los datos de la recuperación de emergencia en este paquete de archivos sólo se pueden utilizar en combinación con una tarjeta de seguridad de recuperación que esté protegida con una contraseña independiente. Esta tarjeta de seguridad se escribió a un archivo cuando el administrador de Security Platform configuró los datos de recuperación de emergencia para todos los usuarios.



Disponibilidad de la página:

- Esta página sólo aparece si el administrador de Security Platform intenta restaurar las credenciales y configuraciones de la plataforma desde un archivo de copia de seguridad creado automáticamente.
- Esta página sólo aparece si se necesita la recuperación de emergencia (es decir, la razón de la restauración es la inicialización de un *nuevo Trusted Platform Module* o un *nuevo Security Platform*).
- En el [modo servidor](#), esta página no está disponible ya que la copia de seguridad y restauración son llevadas a cabo por Trusted Computing Management Server.

La siguiente tabla le muestra algunos consejos sobre cómo utilizar la página del asistente.

Elemento de la página del asistente	Explicación
Ubicación de archivo Examinar...	Ingrese la ruta y el nombre del archivo o examine para buscarlo. Este archivo está en formato XML.
Contraseña	Ingrese una contraseña para la tarjeta de seguridad de recuperación de emergencia.



©Infineon Technologies AG

La Solución Infineon Security Platform - Asistente para la copia de seguridad

Confirmar usuario

Esta página le pide confirmación para restaurar el usuario desde los datos de la copia de seguridad especificada a la cuenta de usuario actual.



Disponibilidad de la página:

- Esta página aparece a los usuarios sin derechos administrativos si los datos de la copia de seguridad contienen información para otro usuario diferente a la cuenta de usuario actual.
- En el [modo servidor](#), esta página no está disponible ya que la copia de seguridad y restauración son llevadas a cabo por Trusted Computing Management Server.

La tabla a continuación le muestra algunos consejos sobre cómo utilizar la página del asistente.

Elemento de la página del asistente	Explicación
<i>Su cuenta de usuario: Nombre de usuario / ID de usuario</i>	Aparecen el nombre de usuario y el ID del usuario de la cuenta de usuario actual. Observe que el nombre del usuario pudo cambiar desde que se realizó la copia de seguridad, ya que puede renombrarse. Es por ello que también se muestra el ID de usuario.
<i>Usuario en los datos de la copia de seguridad: Nombre de usuario / ID de usuario</i>	Aparece el nombre y el ID de usuario para aquel que realizó la copia de seguridad.



©Infineon

La Solución Infineon Security Platform - Asistente para la copia de seguridad

Seleccionar usuarios

Esta página le pide seleccionar los usuarios a restaurar a partir de los datos de la copia de seguridad.



Disponibilidad de la página:

- Esta página aparece al administrador si los usuarios en los datos de la copia de seguridad especificada no pueden mapearse automáticamente a los usuarios en su computadora.
- En el [modo servidor](#), esta página no está disponible ya que la copia de seguridad y restauración son llevadas a cabo por Trusted Computing Management Server.

La tabla a continuación le muestra algunos consejos sobre cómo utilizar la página del asistente.

Elemento de la página del asistente	Explicación
 <i>Nombre del usuario actual</i>  <i>Usuario desde los datos de la copia de seguridad</i>	Aquí se muestra la cuenta del usuario actual. Si desea restaurar su cuenta de usuario actual, haga clic sobre la flecha que se encuentra junto al campo de texto y seleccione de la lista el usuario a restaurar.
 <i>Nombre de usuario</i>  <i>Usuario desde los datos de la copia de seguridad</i>	Aquí se muestran otras cuentas de usuario válidas de quienes han accedido a esta computadora al menos una vez. Para agregar otros usuarios que no aparecen en la lista, haga doble-clic en "<AGREGAR USUARIO>". Si desea preparar la restauración de otros usuarios, haga clic para el usuario de cada computadora sobre la flecha que se encuentra junto al campo de texto y seleccione de la lista el usuario a restaurar.
	 Se muestra una celda explicativa para cada uno de estos usuarios luego de su próximo inicio de sesión, solicitando que completen la restauración. Así mismo, estos usuarios contarán con una entrada al menú de notificación de la barra de tareas para completar la

restauración.



©Infineon Technologies AG

Solución Infineon Security Platform - Asistente para el restablecimiento de la contraseña

Asistente para el restablecimiento de la contraseña de Infineon Security Platform

El asistente para el restablecimiento de las contraseñas de Infineon Security Platform se utiliza para restablecer las contraseñas de usuario básico. El restablecimiento de una contraseña de usuario básico involucra pasos administrativos y de usuario. Mediante el Asistente para la reconfiguración de la contraseña se pueden realizar tanto los pasos administrativos como los del usuario.



Disponibilidad del asistente:

- En el modo [stand-alone](#), este asistente sólo se encuentra disponible en un Security Platform inicializado.
- En [modo servidor](#), no hay disponibles tareas administrativas en este asistente, ya que Trusted Computing Management Server administra esta tarea.



Este icono de escudo sólo es visible para los usuarios con derechos administrativos bajo sistemas operativos con [Control de cuentas de usuario](#) (por ej. Windows 7 y Windows Vista).

Pasos del asistente

Pasos administrativos: Las páginas del asistente para preparar el restablecimiento de la contraseña para un usuario específico están hechas para los administradores de Security Platform o el equipo de ayuda de escritorio. Se necesita una contraseña específica que protege la tarjeta de seguridad de restablecimiento. Si la contraseña de usuario básico del administrador debe ser restablecida, entonces el asistente continuará con los pasos de usuario.

Pasos del usuario: Las páginas del asistente para restablecer la contraseña de usuario actual presuponen que el restablecimiento de la contraseña para este usuario se ha preparado antes.

Paso	Comentario
1. Seleccione la tarjeta de seguridad de restablecimiento de contraseña	Tarea administrativa
2. Seleccionar el usuario cuya contraseña se desea restablecer	Tarea administrativa
3. Mostrar y guardar el código de autorización de restablecimiento	Tarea administrativa (disponible solo si el usuario seleccionado no es el usuario actual)
4. Facilite secretos para el restablecimiento de su contraseña de usuario básico	Tarea del usuario
5. Establezca la nueva contraseña de usuario básico	Tarea del usuario  Si configuró la autenticación avanzada, pero su dispositivo de autenticación no se encuentra disponible o no funciona, puede pasar por alto la actualización de su dispositivo con la nueva frase de contraseña de usuario básico.

Inicio de la aplicación

Inicie el asistente para el restablecimiento de la contraseña de Infineon Security Platform por medio de la Herramienta de Configuración:
[*Herramienta de Configuración - Restablecimiento de contraseña*](#)



©Infineon Technologies AG

La Solución Infineon Security Platform - Asistente para el restablecimiento de la contraseña

Preparar o realizar el restablecimiento de la contraseña

Esta página de la asistente pregunta si desea realizar los pasos administrativos para el restablecimiento de la contraseña o los pasos de usuario.

Elemento de la página de la asistente	Explicación
<p> <i>Preparar y proveer el código de autorización para el restablecimiento de la contraseña para un usuario específico.</i> <i>Preparar y restablecer la cuenta de administrador actual en un solo paso.</i></p>	<p>Realice los pasos administrativos para el restablecimiento de la contraseña. Si la contraseña de usuario básico de la administrador debe ser restablecida, entonces el asistente continuará con los pasos de usuario.</p> <p> Este elemento de la página asistente no está disponible en modo servidor, ya que Trusted Computing Management Server administra esta tarea.</p>
<p> <i>Restablecer mi contraseña (El restablecimiento de la contraseña ya está preparado para mi cuenta de usuario)</i></p>	<p>Realice los pasos de usuario para el restablecimiento de la contraseña.</p>

 Esta página se mostrará solamente si el asistente no ha sido iniciado por medio de la Herramienta de Configuración de Security Platform.



La Solución Infineon Security Platform - Asistente para el restablecimiento de la contraseña

Seleccionar el usuario cuya contraseña se desea restablecer

Esta página del asistente le permitirá seleccionar el usuario cuya contraseña se desea restablecer.



Disponibilidad de la página: Esta página no está disponible en [modo servidor](#), ya que Trusted Computing Management Server administra esta tarea.

Elemento de la página del asistente	Explicación
 Usuarios	La lista muestra todos los usuarios de Security Platform que tienen habilitada la funcionalidad de restablecimiento para sus contraseñas de usuario básico (vea Asistente para la inicialización rápida o Asistente de inicialización del usuario). Por favor seleccione el usuario cuya contraseña se desea restablecer.



Esta página es parte de los pasos administrativos de restablecimiento de la contraseña.



La Solución Infineon Security Platform - Asistente para el restablecimiento de la contraseña

Seleccionar la tarjeta de seguridad de restablecimiento de la contraseña

Este asistente le pregunta por la tarjeta de seguridad para el restablecimiento de la contraseña.



Disponibilidad de la página: Esta página no está disponible en [modo servidor](#), ya que Trusted Computing Management Server administra esta tarea.

Elemento de la página del asistente	Explicación
 <i>Restablecer de la ubicación de la tarjeta de seguridad</i>	Ingrese la ruta de acceso y el nombre de archivo de la tarjeta de seguridad para el restablecimiento de la contraseña que fue creada en el momento en que la información de restablecimiento de la contraseña fue configurada para todos los usuarios. (consulte Asistente para la inicialización).
 <i>Examinar...</i>	Haga clic aquí para buscar la tarjeta de seguridad para el restablecimiento de la contraseña.
 <i>Contraseña</i>	Ingrese la contraseña que protege la tarjeta de seguridad para el restablecimiento de la contraseña que fue especificada cuando la información del restablecimiento de la contraseña fue configurada para todos los usuarios. Nota: La "tarjeta de seguridad de restablecimiento de la contraseña" es necesaria para restablecer "contraseñas de usuario básico". Este archivo está protegido con otra "contraseña" específica.



La página es parte de los pasos administrativos de restablecimiento de la contraseña.



©Infineon Technologies AG

La Solución Infineon Security Platform - Asistente para el restablecimiento de la contraseña

Mostrar y guardar el código de autorización de restablecimiento

Esta página de asistente muestra el código de autorización de restablecimiento que autoriza a un usuario a restablecer su contraseña de usuario básica.



Disponibilidad de la página: Esta página no está disponible en [modo servidor](#), ya que Trusted Computing Management Server administra esta tarea.

Elemento de la página del asistente	Explicación
 <i>Restablecer el código de autorización</i>	Esta cadena de código debe ser otorgada al usuario que necesita restablecer su contraseña de usuario básico. Será requerida para el restablecimiento de la contraseña.
<input type="checkbox"/> <i>Guardar en el archivo...</i>	Con este botón puede guardar el código de autorización de restablecimiento en un archivo. Puede dar este archivo al usuario y este puede leer el código en el archivo. Si el usuario no está en línea (tal vez no pueda entregarle el archivo), entonces necesita entregarle la información y el encabezado como esta mostrado (e.j. por teléfono). En este caso de el usuario necesitará ingresar el código de autorización de restablecimiento manualmente.
 <i>Suma de verificación</i>	La suma de verificación asiste al usuario en el ingreso manual del código de autorización de restablecimiento. La suma de verificación de la cadena ingresada será mostrada al usuario. Si esta suma de verificación corresponde con la que se pasó junto con el código de autorización de restablecimiento, entonces se ingresó la cadena de código correctamente.



Esta página es parte de los pasos administrativos de restablecimiento de contraseña. El código de autorización de restablecimiento debe ser otorgado al usuario que necesita restablecer su contraseña de usuario básico. Esta página no será mostrada si la contraseña de usuario básico que debe ser restablecida es la

de su propia cuenta. En este caso el asistente continúa con los pasos de usuario y usted puede restablecer de inmediato su propia contraseña de usuario básico.



©Infineon Technologies AG

La Solución Infineon Security Platform - Asistente para el restablecimiento de la contraseña

Suministrar datos secretos para el restablecimiento de su contraseña de usuario básico

La página del asistente lo consulta para proveer datos secretos para restablecer su contraseña de usuario básico: su "secreto personal" y el "código de autorización de restablecimiento"

Elemento de la página del asistente	Explicación
<input type="checkbox"/> <i>Secreto personal</i>	<p>Su secreto personal fue creado durante la habilitación de la funcionalidad de restablecimiento para su contraseña de usuario básico. (vea Asistente para la inicialización rápida o Asistente para la inicialización de usuarios).</p> <p>Puede escribir el Secreto personal en forma manual o suministrar el archivo de Secreto personal.</p>
<input type="checkbox"/> <i>Obtener desde archivo...</i>	<p>Si ha guardado el Secreto personal en archivo, haga clic en este botón para suministrar el archivo de Secreto personal.</p>
<input checked="" type="checkbox"/> <i>Ocultar secreto</i>	<p>Destilde esta casilla si desea dejar el secreto visible en texto simple.</p> <p> La opción dentro del campo Secreto personal podría estar restringida en función de la política del sistema Habilitar seguridad estricta de campo de contraseña.</p>
	<p>Nota: Los siguientes elementos de página no se mostrarán si ya ha preparado el restablecimiento de la contraseña para su cuenta de usuario. En este caso no es necesario el código de autorización de restablecimiento.</p>
<input type="checkbox"/> <i>Restablecer el código de autorización</i>	<p>Esta cadena de código fue suministrada por su administrador de Security Platform o por el equipo de ayuda de escritorio. Puede leer el código de autorización de restablecimiento desde un archivo o ingresarlo directamente.</p>
<input type="checkbox"/> <i>Obtener</i>	<p>Haga clic en este botón si le fue suministrado un archivo con</p>

<i>desde el archivo...</i>	el código de autorización de restablecimiento. De otro modo tendrá que escribir la cadena de código.
<input type="checkbox"/> <i>Obtener desde servidor...</i>	<p>Este elemento del asistente sólo está disponible en el modo servidor. Haga clic en este botón para obtener del servidor el código de autorización de restablecimiento.</p> <p> El sistema cliente debe estar integrado en un Trust Domain con gestión centralizada.</p>
<input type="checkbox"/> <i>Suma de verificación</i>	<p>La suma de verificación lo asiste en el ingreso manual del código de autorización de restablecimiento. Si la suma de verificación mostrada corresponde con la que se le dió junto con el código de autorización de restablecimiento, entonces se ingresó la cadena de código correctamente.</p>

 Esta página es parte de los pasos para el usuario de restablecimiento de la contraseña. Si la contraseña de usuario básico a restablecerse es la de su propia cuenta, esta página será mostrada luego de que halla realizado los pasos administrativos.

La Solución Infineon Security Platform - Asistente para la importación de PKCS #12

Asistente para la importación de Infineon Security Platform PKCS #12

El asistente para la importación de Infineon Security Platform PKCS #12 se utiliza para importar archivos de Personal Information Exchange a Security Platform.

Los archivos de Personal Information Exchange (PKCS #12) tienen la extensión ".pfx" o ".p12". Un archivo PKCS #12 creado para usted contiene su certificado y su clave privada. También puede contener una cadena de certificación, es decir, todos los certificados de la entidad certificada (CA) necesarios para validar su certificado. Para mantener la seguridad, se protege la clave privada de un archivo PKCS #12 por medio de una contraseña.

Diferencias con el asistente para la importación de certificados de Microsoft

PC sin Security Platform: los archivos PKCS #12 se importan utilizando el *Asistente para la importación de certificados de Microsoft*. Su clave privada está asegurada por software.

PC con Security Platform: Los archivos PKCS #12 se importan utilizando el *Asistente para la importación de Security Platform PKCS #12*. Su clave privada está asegurada por Trusted Platform Module. De esta manera se mejora la protección de su clave privada.

Pasos del asistente

Paso	Comentario
1. Archivo PKCS #12 a importar	Especifique el archivo que desea importar
2. Opciones	Configure las opciones de importación PKCS #12

Inicio de la aplicación

Para iniciar el asistente para la importación de Infineon Security Platform PKCS #12 haga clic en **Importar...** en el visor de certificados de Security Platform. Se puede ejecutar el visor de certificados de Security Platform desde la herramienta de configuración ([Herramienta de configuración - Configuración del usuario - Administrar...](#)).



©Infineon

Technologies AG

La Solución Infineon Security Platform - Asistente para la importación de PKCS #12

Archivo PKCS #12 a importar

Esta página del asistente le pide que especifique el archivo PKCS #12 que desea importar.

Elemento de la página del asistente	Explicación
 <i>Nombre del archivo</i>	Puede ingresar o pegar la ruta de acceso aquí, por ejemplo: D:\certificates\MyPKCS12file.pfx o D:\certificates\MyPKCS12file.p12.
<input type="checkbox"/> <i>Examinar</i>	Haga clic aquí para examinar en busca del archivo PKCS #12 en lugar de ingresar o pegar la ruta de acceso.
 <i>Ingrese la contraseña que protege el archivo</i>	Para mantener la seguridad, se protege la clave privada de un archivo PKCS #12 por medio de una contraseña. Ingrese aquí la contraseña.



La Solución Infineon Security Platform - Asistente para la importación de PKCS #12

Opciones

Esta página del asistente le pide que configure las opciones de importación de PKCS #12.

Elemento de la página del asistente	Explicación
<input type="checkbox"/> <i>Depósito de certificados</i>	El archivo PKCS #12 se guardará en depósito determinado de certificados, por ejemplo <i>Personal</i> . Aquí se muestra el depósito de certificados.
<input type="checkbox"/> <i>Examinar...</i>	<p>Haga clic aquí si desea cambiar el depósito de certificados.</p> <p> Puede importar un certificado en cualquier depósito de certificados. En la mayoría de los casos, los certificados se importan al depósito <i>Personal</i> o al <i>Trusted Root Certification Authorities</i>, dependiendo de si el certificado es para usted o si es un certificado de una entidad certificada raíz.</p> <p>Recomendación: Si va a importar su propio certificado, elija el depósito de certificados <i>Personal</i>.</p>
<input checked="" type="checkbox"/> <i>Si el archivo PKCS #12 así lo estipula, incluya la cadena completa del certificado</i>	<p>Un archivo PKCS #12 puede contener no sólo su certificado, sino una cadena de certificados completa. Una cadena de certificados contiene todos los certificados de la entidad certificada (CA) necesarios para validar su certificado.</p> <p>Tilde esta casilla de verificación si desea importar la cadena de certificados completa (si así lo estipula el archivo PKCS #12 especificado).</p> <p> Si se importa la cadena de certificados completa, los certificados de la entidad certificada se alojarán automáticamente en los depósitos de certificados apropiados.</p> <p>Ejemplo: Está por importar un PKCS #12 incluyendo su propio</p>

	<p>certificado y clave privada, un certificado CA intermedio y un certificado CA raíz confiable. Ha seleccionado el depósito de certificado <i>Personal</i>.</p> <ul style="list-style-type: none">→ Su certificado se guardará en el depósito de certificados <i>Personal</i>.→ El certificado CA intermedio se guardará en el depósito de certificados <i>Intermediate Certification Authorities</i>.→ El certificado CA raíz confiable se guardará en el depósito de certificados <i>Trusted Root Certification Authorities</i>.
<input checked="" type="checkbox"/> <i>Habilitar nivel alto de protección de la clave privada</i>	<p>Tilde esta casilla de verificación si desea asegurarse de que su clave privada no se utilice sin su consentimiento.</p> <p>Si activa el <i>nivel alto de protección de la clave privada</i>, se le pedirá ingresar su contraseña cada vez que utilice su clave privada.</p>



Infineon Solución Security Platform - Icono de Notificación de la Barra de tareas

Icono de Notificación de la Barra de tareas de Security Platform

El Icono de Notificación de la Barra de tareas es un punto de ingreso sensible al estado para las tareas administrativas de Security Platform. A través de este ícono puede acceder al Menú de Notificación de la Barra de tareas. Además, los globos de texto y los cuadros de ayuda lo asisten por medio de información sensible al estado.

Icono de Notificación de la Barra de tareas

Este ícono aparece en el Área de Notificación de la Barra de tareas (TNA por sus siglas en inglés). Es un punto de acceso sensible al estado para las distintas tareas administrativas de Security Platform.

El estado actual de Security Platform se puede conocer a través de la apariencia visual de este ícono:



Security Platform se encuentra listo para usar.

Security Platform se encuentra inicializado, pero deshabilitado o



temporalmente deshabilitado. El usuario actual puede habilitar el Security Platform.

Security Platform no se encuentra inicializado para el



usuario actual.

Security Platform se encuentra deshabilitado o temporalmente deshabilitado,



o bien falló la auto evaluación. El usuario actual no puede cambiar este estado del Security Platform.



Security Platform no está inicializado.

Menú de Notificación de la Barra

Este menú se muestra luego de que el usuario hace clic en el Icono de Notificación de la Barra de tareas.

Le suministra tareas administrativas sensibles al estado, como

de tareas	<p>ser:</p> <ul style="list-style-type: none"> • Inicialización de Security Platform • Inicialización de usuario de Security Platform • Administración de Security Platform • Ayuda acerca de la elección de distintas tareas <p> No todos los elementos del menú están disponibles en el modo servidor.</p>
Globos de texto	<p>Los globos de texto le informan sobre los cambios de estado y le sugieren que realice ciertas operaciones de acuerdo a estados específicos de Security Platform.</p> <p> En el modo servidor, las tareas que no requieren la interacción del usuario son realizadas por Trusted Computing Management Server. No están disponibles las celdas de descripción relacionadas con estas tareas.</p>
Cuadros de ayuda	<p>Se muestra una breve información de estado en forma de cuadro de ayuda al momento en que el usuario pasa el ratón sobre el Icono de Notificación de la Barra de tareas.</p>



Solución Infineon Security Platform - Icono de Notificación de la Barra de tareas

Opciones del Menú de Notificación de la Barra de tareas

Dependiendo del estado actual del Infineon Security Platform y del estado de los usuarios que se encuentran actualmente en una sesión activa, el Menú de Notificación de la Barra de tareas le ofrece distintas opciones.

Por medio del menú contextual se pueden ejecutar todas las herramientas del Infineon Security Platform permitidas para el usuario en sesión actual. Si el usuario en sesión actual no tiene permiso para ejecutar una herramienta de la solución, el elemento no se encuentra en el menú.



Este icono de escudo sólo es visible para los usuarios con derechos administrativos bajo sistemas operativos con [Control de cuentas de usuario](#) (por ej. Windows 7 y Windows Vista).

La tabla a continuación lista todos los elementos del menú.

Elementos del menú	Explicación
<i>Administrar Security Platform</i>	<p>Ejecute la Herramienta de Configuración de Infineon Security Platform.</p> <p> Bajo sistemas operativos con control de cuentas de usuario, la herramienta de configuración se inicia sin privilegios elevados.</p>
<i>Inicialización de Security Platform</i>	<p>Ejecute el Asistente para la inicialización de Infineon Security Platform.</p> <p>Este elemento del menú está disponible cuando aún no se ha realizado la configuración de Infineon Security Platform. Esta entrada figura en gris si la política <i>Permitir la inscripción de la plataforma</i> está desactivada (esta política está en vigencia si el Security Platform no se inicializa antes).</p> <p> Este elemento del menú no está disponible en el modo servidor, ya que Security Platform se inicializa</p>

	automáticamente si el sistema cliente está integrado en un Trust Domain con gestión centralizada.
<i>Inicialización de usuario de Security Platform</i>	<p>Ejecute el Asistente para la inicialización de Infineon Security Platform.</p> <p>Este elemento del menú está disponible cuando el usuario en sesión actual aún no se ha configurado como usuario de Infineon Security Platform. Esta entrada está deshabilitada si el Security Platform no se encuentra inicializado y la política <i>Permitir la inscripción de usuarios</i> está deshabilitada (esta política está en vigencia sólo para usuarios que aún no están inicializados).</p> <p> Este elemento del menú no está disponible en el modo servidor si el usuario actual no es un miembro del grupo de inscripción de usuarios.</p>
<i>Habilitación de la copia de seguridad de sus funciones de Security Platform</i>	<p>Incluya sus claves y credenciales en las copias de seguridad automáticas. Se le pedirá que se autentifique en el Security Platform. Este elemento de menú está disponible si el administrador de Security Platform ha configurado la Copia de seguridad, pero el usuario en sesión actual aún no habilitó esta función.</p> <p> En el modo servidor, este elemento del menú no está disponible ya que la copia de seguridad y restauración son llevadas a cabo por Trusted Computing Management Server.</p>
<i>Habilitación de la función de restablecimiento de la contraseña</i>	<p>Habilite la función de restablecimiento de la contraseña para su cuenta de usuario. Este elemento del menú está disponible si el administrador de Security Platform ha</p>

	configurado el Restablecimiento de la contraseña , pero el usuario actual aún no configuró esta función.
<i>Personal Secure Drive - Cargar</i> o <i>Personal Secure Drive -</i> <LetraUnidad.Etiquetaunidad> - Cargar	Cargue su Personal Secure Drive. ve. Si ha instalado más de un PSD, entonces el menú listará todas las unidades (<LetraUnidad.Etiquetaunidad>). Este elemento del menú se encuentra disponible si ha configurado por lo menos un PSD (el cual no está actualmente cargado).
<i>Personal Secure Drive -</i> Descargar o <i>Personal Secure Drive -</i> <LetraUnidad.Etiquetaunidad> - Descargar	Descargar su Personal Secure Drive. Si ha instalado más de un PSD, entonces el menú listará todas las unidades (<LetraUnidad.Etiquetaunidad>). Este elemento del menú se encuentra disponible si ha configurado por lo menos un PSD (el cual está actualmente cargado).
<i>Personal Secure Drive - Cargar</i> al iniciar la sesión o <i>Personal Secure Drive -</i> <LetraUnidad.Etiquetaunidad> Cargar al iniciar la sesión	Especifique si desea cargar su PSD automáticamente después del inicio de sesión en Windows. Si ha instalado más de un PSD, entonces el menú listará todas las unidades (<LetraUnidad.Etiquetaunidad>). Si aparece una tilde aquí, entonces su PSD será cargado. Haga clic aquí para añadir/quitar la tilde. Este elemento del menú se encuentra disponible si ha configurado por lo menos un PSD (el cual está actualmente cargado)
<i>Personal Secure Drive -</i> Crear/Administrar	Crear, cambiar o borrar unPersonal Secure Drive por medio del Asistente de inicialización del usuario .
<i>Personal Secure Drive -</i> Descargue all	Descargue todos los Personal Secure Drives que están actualmente cargados.

<p><i>Cierre de sesión desde el EFS (Encrypting File System)</i></p>	<p>Haga clic aquí para cerrar la sesión desde el EFS. Esto implica que deberá autenticarse nuevamente para acceder a sus datos protegidos de EFS.</p> <p>Este elemento de menú está disponible si anteriormente se ha autenticado para acceder a algún dato protegido por EFS.</p>
<p><i>Cambiar la contraseña de usuario básico</i></p>	<p>Haga clic aquí para cambiar su contraseña de usuario básico.</p> <p>Si su contraseña de usuario básico caducó, ese elemento del menú se encuentra disponible. La caducidad de la contraseña de usuario básico se puede establecer con la política de usuario <u>Período máximo de la contraseña de usuario básico. Sincronizar la frase de contraseña de usuario básico</u>.</p>
<p><i>Sincronizar la frase de contraseña de usuario básico</i></p>	<p>Haga clic aquí para sincronizar su frase de contraseña de usuario básico para el dispositivo de autenticación y de Security Platform.</p> <p>Si su dispositivo de autenticación y su Security Platform poseen distintas frases de contraseña de usuario básico, este elemento del menú se encuentra disponible. Las razones pueden ser:</p> <ul style="list-style-type: none"> • <u>Restableció</u> su frase de contraseña de usuario básico sin actualizar su dispositivo de autenticación. • Utiliza su dispositivo de actualización en varias Security Platform, y cambió su frase de contraseña de usuario básico en otro. Reconfigurar las funciones del usuario
<p><i>Reconfigurar las opciones de usuario</i></p>	<p>Haga clic aquí para reconfigurar las funciones de Security Platform. Este elemento del menú está disponible, si su PSD o EFS requiere reconfiguración. Las</p>

razones pueden ser:

- Su certificado EFS o PSD ya no es válido y no está disponible. Sucede lo mismo con la *encriptación de archivos y carpetas por medio del Encrypting File System (EFS)*, si configuró tanto EFS como PSD y luego cambió su certificado PSD.
- Se realizó una recuperación, y su PSD no se puede cargar más (p.ej. porque la letra de la unidad está siendo usada).

Deshabilitar transitoriamente el Security Platform hasta el próximo inicio del sistema

Haga clic aquí para suspender la ejecución de Infineon Security Platform hasta que se reinicie el sistema. Aquellas aplicaciones diseñadas para utilizar Security Platform ya no podrán utilizar los datos protegidos por medio de Trusted Platform Module, incluyendo los datos protegidos de EFS y Personal Secure Drive, entre otros. El acceso a los datos protegidos se restaura una vez rehabilitado el Security Platform. Este elemento del menú está disponible si Infineon Security Platform se encuentra inicializado y habilitado. Observe que esta función sólo está disponible en Security Platforms con un Trusted Platform Module 1.2.

Habilitar el funcionamiento de Security Platform

Para los administradores, este elemento de menú está disponible en un Security Platform inicializada en el modo independiente, si el propietario ha deshabilitado el Security Platform. Se requiere la contraseña de propietario para habilitar el Security Platform. Este elemento del menú también está disponible para los usuarios en un Security Platform con una versión de Trusted

	<p>Platform Module inferior a la 1.2, si el usuario ha deshabilitado temporalmente el Security Platform. En este caso, el usuario tiene que reiniciar el sistema.</p> <p> Este elemento del menú no está disponible en el modo servidor, ya que Security Platform se inicializa automáticamente si el sistema cliente está integrado en un Trust Domain con gestión centralizada.</p>
<p><i>Restauración del Security Platform</i></p>	<p>Restaurar las credenciales y la configuración del Security Platform desde un paquete de archivos de la copia de seguridad. Este elemento del menú está disponible para un administrador si el Security Platform no se inicializó o se inicializó en otro sistema operativo, o si cambió el propietario de la plataforma.</p> <p> En el modo servidor, este elemento del menú no está disponible ya que la copia de seguridad y restauración son llevadas a cabo por Trusted Computing Management Server.</p>
<p><i>Restauración de las funciones del Security Platform</i></p>	<p>Restaurar sus credenciales de usuario y la configuración desde un paquete de archivos de la copia de seguridad. Este elemento de menú está disponible si su clave de usuario básico no se puede cargar, por ejemplo si no puede utilizar las funciones del Security Platform.</p> <p> En el modo servidor, este elemento del menú no está disponible ya que la copia de seguridad y restauración son llevadas a cabo por Trusted Computing Management Server.</p>
<p><i>Credenciales / configuraciones</i></p>	<p>Se obtiene una copia de trabajo local de sus</p>

del usuario – Solicitar copia de trabajo local

configuraciones y credenciales de usuario desde Trusted Computing Management Server. Bloquee cualquier modificación proveniente de otras computadora siempre que no haya aceptado o desechado sus cambios locales (es decir, el estado de la sesión del usuario en modo servidor se fija a "Lectura/escritura permanente").



Este elemento del menú sólo está disponible en el [modo servidor](#).

Realice esta acción antes de llevar su plataforma offline, si desea cambiar sus credenciales o configuraciones de usuario sin contar con una conexión de red a Trusted Computing Management Server. Un ejemplo típico es el cambio o reconfiguración de su contraseña de usuario básico en un ordenador portátil que se encuentra offline.

Precondiciones:

- El usuario actual se ha inicializado en modo servidor.
- Su plataforma está conectada a Trusted Computing Management Server.
- No hay una copia de trabajo local activa en la misma plataforma (es decir, el estado de la sesión del usuario en la misma plataforma no es "Lectura/Escritura permanente").

Si hay un acceso actual para escritura para sus credenciales de usuario, o sus credenciales de usuario no están actualizadas, se le informará que no puede solicitar una copia de trabajo local en la actualidad. En el primer caso, espere durante un tiempo breve e inténtelo de nuevo. En el

	<p>segundo caso, aparecerá un globo para actualizar sus credenciales de usuario.</p> <p>Detalles sobre los estados de sesión de usuario.</p>
<p><i>Credenciales / configuraciones del usuario – Aceptar cambios locales</i></p>	<p>Remite los cambios de sus credenciales o configuraciones de usuario al Trusted Computing Management Server. Vuelve a permitir cambios desde otras plataformas.</p> <p> Este elemento del menú sólo está disponible en el modo servidor.</p> <p>Realice esta acción cuando su plataforma vuelva a estar online, después de haber cambiado sus credenciales o configuraciones de manera local.</p> <p>Precondiciones:</p> <ul style="list-style-type: none">• El usuario actual se ha inicializado en modo servidor.• Su plataforma está conectada a Trusted Computing Management Server.• Hay una copia de trabajo local activa (es decir, el estado de la sesión de usuario en esta plataforma es "Lectura/Escritura permanente").
<p><i>Credenciales / configuraciones de usuario – Desechar los cambios locales</i></p>	<p>Desecha los cambios de sus credenciales o configuraciones. Vuelve a permitir cambios desde otras plataformas.</p> <p> Este elemento del menú sólo está disponible en el modo servidor.</p> <p>Realice esta acción cuando su plataforma vuelva a estar online, y no ha cambiado sus credenciales y configuraciones en ningún aspecto, o cuando desea revertir los cambios</p>

	<p>realizados.</p> <p>Precondiciones:</p> <ul style="list-style-type: none">• El usuario actual se ha inicializado en modo servidor.• Su plataforma está conectada a Trusted Computing Management Server.• Hay una copia de trabajo local activa (es decir, el estado de la sesión de usuario en esta plataforma es "Lectura/Escritura permanente").
<p><i>Actualizar las configuraciones y credenciales del usuario</i></p>	<p>Realice esta tarea para actualizar sus configuraciones y credenciales en la plataforma actual.</p> <p> Este elemento del menú sólo está disponible en el modo servidor.</p> <p>Precondiciones:</p> <ul style="list-style-type: none">• El usuario actual se ha inicializado en modo servidor.• Su plataforma está conectada a Trusted Computing Management Server. <p>Detalles sobre la actualización de las configuraciones y credenciales del usuario</p>
<p><i>Restaura</i></p>	<p>Actualice el Ícono de notificación de la barra de tareas y el Menú de notificación de la barra de tareas.</p>
<p><i>Borrar el Caché de autenticaciones</i></p>	<p>Revierta el efecto de Recordar la <i>contraseña para todas las aplicaciones</i>, el cual ha sido establecido en el diálogo de autenticación de la Contraseña para usuario básico. De este modo se le notificará para que realice una nueva autenticación cuando sea necesario.</p>

	 Este elemento del menú sólo se encuentra disponible si con anterioridad se ha tildado <i>Recordar la contraseña para todas las aplicaciones</i> en el diálogo de autenticación de la Contraseña del usuario básico.
<i>Habilitar Infineon TPM Strong Cryptographic Provider</i>	Se debe generar una clave para habilitar Infineon TPM Strong Cryptographic Provider . Haga clic aquí para autorizar la generación de la clave.
<i>Ayuda</i>	Se ha iniciado la ayuda de Infineon Security Platform.
Diversos elementos del menú para la ayuda contextual	Aparece la ayuda específica contextual para el estado actual de la plataforma y las acciones de usuario necesarias.



Infineon Solución Security Platform - Icono de Notificación de la barra de tareas

Deshabilitación de Trusted Platform Module

El Trusted Platform Module se puede deshabilitar de dos maneras diferentes.

- **Deshabilitación transitoria**

Esta operación deshabilita el chip hasta que el sistema vuelva a reiniciarse.
Un cambio en el usuario registrado no afecta el estado del chip.

- **Deshabilitación permanente**

Esta operación desactiva el chip físicamente. Si Infineon Security Platform ya está configurado, esta operación se puede realizar por medio de la [Herramienta de Configuración de Infineon Security Platform](#).

La rehabilitación de Infineon Security Platform se realiza por medio de la misma Herramienta de Configuración. Si Infineon Security Platform no está configurado, se debe habilitar el chip en la BIOS del sistema.



©Infineon

Technologies AG

Infineon Solución Security Platform - Icono de Notificación de la barra de tareas

Deshabilitación temporaria de Infineon Security Platform

Se habilita un mecanismo para desactivar el Infineon Security Platform hasta que el sistema vuelva a reiniciarse. La deshabilitación temporaria permanece activa si el usuario de Infineon Security Platform simplemente cierra y vuelve a iniciar su sesión.

En este estado todas las funciones de Infineon Security Platform e Trusted Platform Module se encuentran bloqueadas.



©Infineon

Technologies AG

Solución Infineon Security Platform - Icono de Notificación de la Barra de tareas

Habilitación de Infineon Security Platform

Para habilitar Security Platform, vaya a **Avanzado** en la herramienta de configuración y haga clic en **Habilitar...** (ver [Configuración avanzada](#)). Tenga en cuenta que el [Propietario de Security Platform](#) es el único que puede realizar esta acción, dado que se requieren derechos de administración y la contraseña del propietario.

Tras la habilitación de Security Platform, realice la configuración inicial de Security Platform y de los usuarios por medio del [Asistente para la inicialización rápida](#) (recomendado para la mayoría de los usuarios), o por medio del [Asistente de inicialización](#) y del [Asistente para la inicialización de usuarios](#) (recomendado para usuarios expertos).



Technologies AG

La solución Infineon Security Platform - Administración de política

Administración de política de Infineon Security Platform

Con el editor de políticas de grupo local puede administrar las configuraciones relativas a la seguridad de Infineon Security Platform:

Políticas del sistema	Configuraciones de seguridad para la computadora
Políticas de usuario	Configuraciones de seguridad para los usuarios en la computadora
 En modo servidor , las Políticas se configuran en todo el dominio mediante un administrador de dominios a través de Trusted Computing Management Server.	

Restricciones y precondiciones



- Solo un administrador puede cambiar las políticas de usuario y del sistema.
- El Editor de política del grupo local no está disponible en ediciones de Windows Home.

Cómo registrar las Políticas de Security Platform

Las Políticas de Security Platform se registran automáticamente (archivo de plantilla administrativa **IfxSpPol.admx**) en los sistemas operativos que soportan el formato de política ADMX (por ejemplo, Windows Vista y Windows 7).

En los demás sistemas operativos se deben realizar los siguientes pasos para registrar las Políticas de Security Platform de modo manual (archivo de plantilla administrativa **IfxSpPol.adm**) antes de poder acceder a las políticas desde la [Herramienta de configuración](#):

1. Iniciar Editor de políticas de grupo local (gpedit.msc)
2. Hacer clic con el botón derecho sobre **Plantillas administrativas de Configuración de computadora** o **Configuración del usuario**.
3. En el menú de contexto, haga clic en **Añadir/Quitar plantillas...** .
Aparece en pantalla el diálogo "Añadir/Quitar plantillas".
4. Haga clic en **Añadir**.
Aparece en pantalla el diálogo del explorador "Plantillas de la política".
5. Seleccione la plantilla **IfxSpPol.adm**, y haga clic en **Abrir** para añadir la plantilla "Security Platform".
6. Haga clic en **Cerrar** para registrar la nueva plantilla administrativa.

Cómo editar las políticas de sistema y de usuarios

1. Iniciar la [Herramienta de configuración](#) desde el [Icono de notificación de la barra de tareas](#).

En los sistemas operativos con Control de la cuenta del usuario (por ejemplo, Windows 7 y Windows Vista), haga clic en  **Administrar Security Platform**.

En los demás sistemas operativos, haga clic en **Administrar Security Platform**.

2. Para editar las Políticas del sistema, haga clic en **Sistema...** en la lengüeta **Avanzado**.

Para editar las Políticas del usuario, haga clic en **Usuario...** en la lengüeta **Avanzado**.

El Editor de políticas de grupo local ha sido iniciado. Muestra en pantalla las Políticas del sistema de Infineon Security Platform o las Políticas del usuario.

Mas información

En la introducción de Microsoft Group Policy y en Microsoft Technet hay información disponible sobre las políticas del sistema y las políticas del usuario. Para obtener la información necesaria en la Ayuda de Microsoft, minimice todas las ventanas abiertas para visualizar el entorno de escritorio de Windows. Después pulse F1 y busque la palabra clave apropiada.



©Infineon Technologies AG

Infineon La Solución Security Platform - Administración de política

Políticas de sistema de Infineon Security Platform

El software solución Infineon Security Platform admite las siguientes configuraciones de política de computadora.



En [modo servidor](#), las Políticas del Sistema se configuran en todo el dominio por un administrador de dominios a través de Trusted Computing Management Server. Tenga en cuenta que las configuraciones que sólo son válidas para el modo de servidor se describen en el archivo de plantilla administrativa suministrado por Trusted Computing Management Server.



Valor predeterminado: Si una política no ha sido explícitamente establecida (e.j. el Editor de política del grupo local muestra el estado **No configurado**), entonces el software solución Security Platform implícitamente aplica un valor por predeterminado.

Todas las configuraciones de las versiones

Configuraciones que son válidas tanto para la versión en modo servidor como para la versión en modo stand-alone.

Política	Explicación	Valor predeterminado
<i>Preparar la inscripción de TPM</i>	<p>Habilitado: El Trusted Platform Module se prepara automáticamente para habilitarse en las plataformas no inicializadas que tienen un Trusted Platform Module deshabilitado y que soportan la Interfaz de Presencia Física (PPI). Se guiará a los usuarios para que completen la habilitación.</p> <p>Deshabilitado: El Trusted Platform Module no está preparado para habilitarse automáticamente.</p>	Deshabilitado
<i>Permitir a los administradores el uso remoto de la clave de plataforma</i>	<p>Habilitado: Un administrador puede utilizar claves de plataforma no solo de forma local sino también remotamente.</p> <p>Deshabilitado: No se puede utilizar las claves de plataforma en forma remota. Por problemas de privacidad, el acceso a estas claves está restringido según lo acordado por Trusted Computing Group (TCG). De esta manera todas las claves que permitirían la identificación de su Security</p>	Deshabilitado

	<p>Platform están ocultas para el acceso remoto. Esta política requiere que todas las computadoras sean miembros de dominios confiables. Esto sólo es relevante para los sistemas operativos que soporten la asociación de dominios.</p> <p> Observe que la administración y operación de Security Platform no está restringida por esta política.</p>	
<p><i>Permitir la lectura de la memoria TPM NV no protegida</i></p>	<p>Determina quien puede leer la memoria No-Volátil (NV) no protegida, almacenada en un Trusted Platform Module 1.2. La memoria NV puede contener datos sensibles.</p> <p>Habilitado: Especifique si sólo los administradores locales, los administradores locales y remotos, todos los usuarios locales o todos los usuarios pueden leer datos NV no protegidos.</p> <p>Deshabilitado: Ningún usuario puede leer datos NV no protegidos.</p> <p> Esta política sólo es válida para Security Platforms con un Trusted Platform Module 1.2.</p> <p>Observe que la administración y operación de Security</p>	<p>Permitido/administradores locales</p>

	Platform no se ve restringida por esta configuración.	
<p><i>Configuración del límite para el ataque de diccionario</i></p>	<p>Determina la cantidad de intentos de autenticación permitidos para Trusted Platform Module antes de que se tomen medidas de defensa de ataques por diccionario.</p> <p>Habilitado: Especificar cuántos intentos de autenticación deben permitirse para las claves (por ejemplo, las utilizadas para la autenticación del usuario de Security Platform), los propietarios y para el acceso a datos sellados (por ejemplo, los utilizados por Windows BitLocker en combinación con PIN) antes de que se tomen medidas de defensa de ataques por diccionario.</p> <p>Deshabilitado: No se puede configurar el límite para el ataque de diccionario. Se encuentran activos los valores predeterminados.</p> <p> Esta política sólo es relevante para Security Platforms con un Infineon Trusted Platform Module 1.2. Se debe establecer antes de inicializar Security Platform. Los cambios posteriores a esta política sólo tendrán efecto después de la próxima</p>	<p>Habilitado</p> <p>Propietario: 3 intentos Clave: 5 intentos Datos: 10 intentos</p>

configuración del [nivel de defensa](#).

Si esta política no está configurada, entonces se pueden establecer los mismos valores de forma separada para cada plataforma en modo independiente mediante Intialization Wizard (ver [Configurar Diccionario de valores de defensa contra ataques](#)). En este caso no es necesario redefinir ningún nivel de defensa para que los valores de configuración sean eficaces.

Observe que todos los usuarios de Security Platform comparten la cantidad de intentos de autenticación permitidos. Téngalo presente si existen múltiples usuarios en paralelo en el sistema (por ejemplo, al utilizar Fast User Switching).

[Detalles sobre el ataque de diccionario](#)

Habilitar seguridad severa del campo de contraseña

Habilitado: La posibilidad de cortar, copiar, pegar y ver la contraseña en texto claro no está disponible en los campos de contraseña.

Deshabilitado: La posibilidad de pegar está disponible en los campos de contraseña. Además, la

Deshabilitado

	<p>función de cortar y pegar está disponible cuando la contraseña está visible e texto claro.</p>	
<p><i>Purgar claves al ingresar en estados de ahorro de energía.</i></p>	<p>Habilitado: Las claves de Security Platform son purgadas antes de que la computadora entre en uno de los estados de ahorro de energía Stand by (S3) o Hibernación (S4). Por lo tanto, el nivel de seguridad durante el período del estado de ahorro de energía aumenta. Al volver del estado de ahorro de energía, las funciones de Security Platform necesitarán una nueva autenticación de usuario.</p> <p>Deshabilitado: Las claves de Security Platform no son purgadas.</p>	<p>Habilitado</p>
<p><i>Proveedores de autenticación avanzados</i></p>	<p>Habilitado: Ingrese el ID de clase (CLSID) de un proveedor de autenticación avanzada, o múltiples CLSIDs separados por punto y coma. Sólo los proveedores especificados aquí serán aceptados para utilizar la autenticación avanzada en los sistemas clientes que aun no se han configurado. Si no conoce ningún ID de</p>	<p>Comportamiento igual al de deshabilitado.</p>

	<p>clase de un proveedor de autenticación avanzada, contáctese con el fabricante de proveedores de autenticación avanzada. Ejemplo de ID de clase: {76D8D888-B5AC-49FC-9408-8A45D37F3AC6}</p> <p>Deshabilitado: No se pueden especificar proveedores de autenticación avanzada. No se puede utilizar la autenticación avanzada en sistemas clientes que no han sido configurados aun.</p>	
<p><i>Permitir a los administradores a tomar dominio remoto</i></p>	<p>Habilitado: No se requiere de la presencia local de un administrador al tomar posesión de una computadora. Esta funcionalidad puede ser particularmente útil cuando se realiza la configuración de clientes en redes grandes.</p> <p>Deshabilitado: No está permitido tomar dominio remotamente.</p> <p> Esta política requiere que todas las computadoras sean miembros de dominios confiables. Esto sólo es relevante para los sistemas operativos que soporten la asociación de dominios.</p>	<p>Deshabilitado</p>
<p><i>Permitir a los</i></p>	<p>Determina quien puede leer la</p>	<p>Deshabilitado</p>

*administradores
la recuperación
remota de la
clave pública*

clave pública Storage Root Key's(SRK) almacenada en un Trusted Platform Module. La clave pública SRK requiere de protección especial, ya que mediante ella se puede identificar al Security Platform.

Habilitado: Un administrador puede recuperar la clave pública SRK no solo a nivel local sino también remotamente.

Deshabilitado: No esta permitido la recuperación remota de una clave publica SRK.



El paso de migración [Autorización y exportación automática](#) requiere que esta opción este habilitada en la computadora destino de la migración.

Esta política requiere que todas las computadoras sean miembros de dominios confiables.

Esta configuración solo es relevante para los sistemas operativos que soportan la asociación de dominios.

Configuraciones de la versión en modo Stand-alone

Configuraciones que son válidas sólo para la versión en modo stand-alone.

Política	Explicación
<i>Contraseñas de propietario - Longitud mínima de contraseña</i>	<p>Habilitado: Ingrese la longitud mínima deseada para la contraseña de propietario, por ejemplo, 6. La longitud mínima de contraseña es válida para las contraseñas de propietario que más tarde se configuran o modifican.</p> <p>Deshabilitado: La longitud mínima de la contraseña es de 6 caracteres.</p> <p> Este parámetro se aplica sólo a las contraseñas de propietario configuradas en un Security Platform individual.</p> <p>Detalles en el manejo de contraseñas</p>
<i>Contraseñas de propietario - La contraseña debe reunir los requerimientos de complejidad</i>	<p>Habilitado: Se implementan requisitos de complejidad de contraseña para contraseñas de propietario que más tarde se configuren o modifiquen.</p> <p>Deshabilitado: No se imponen requerimientos de complejidad de contraseña.</p> <p> Este parámetro se aplica sólo a las contraseñas de propietario configuradas en un Security Platform individual. Los requisitos de complejidad para contraseñas de propietario configuradas por medio de Trusted Computing Management Server los establece la política homónima de Trusted Computing Management Server. Detalles en complejidad de contraseñas</p>
<i>Permitir registro de plataforma</i>	<p>Habilitar/permitir interfase y asistente para la administración: El administrador esta habilitado para utilizar el asistente de inicialización de Security Platform y la interfase management provider para la inicialización.</p> <p>Habilitar/permitir la interfase proveedora de la administración solamente: El administrador puede solo</p>

	<p>invocar la interfase management provider pero no puede ejecutar el asistente para la inicialización de Security Platform.</p> <p>Deshabilitado: Security Platform no permite que el administrador lleve a cabo ninguna función.</p>
<p><i>Implementación de la configuración de la copia de seguridad incluyendo restauración de emergencia</i></p>	<p>Habilitado: La configuración de las copias de seguridad automáticas (incluyendo las restauraciones de emergencia) es obligatorio en el proceso de inicialización de Security Platform.</p> <p>Si Security Platform ha sido inicializado sin configurar las copias de seguridad automáticas, no hay ninguna imposición para configurar las copias de seguridad automáticas.</p> <p>Deshabilitado: No hay ninguna imposición para configurar las copias de seguridad automáticas. Las copias de seguridad pueden ser configuradas luego de la inicialización de Security Platform por medio de Herramienta de configuración - Copia de seguridad - Configuración....</p>
<p><i>Localización del archivo de copia de seguridad</i></p>	<p>Habilitado: Ingrese la ruta de acceso incluyendo el nombre de archivo, e.j. \\BackupServer\SecurityPlatformShare\SPSystemBackup.xml La ruta de destino será implementada cuando la función de copia de seguridad sea configurada. Se creará un Archivo de copia de seguridad que consta de un archivo XML y de una carpeta con el mismo nombre, por ejemplo: archivo SPSysystemBackup.xml y carpeta SPSysystemBackup.</p> <p>Si la función de copia de seguridad ha sido configurada, entonces la ruta de acceso de la copia de seguridad existente se mantiene hasta que no se realice una reconfiguración.</p> <p> Asegúrese de ingresar una ruta válida que sea accesible por todas las PCs de Security Platform. De otro modo, la configuración de la copia de seguridad fallará.</p> <p>Deshabilitado: La ruta de destino de la copia de seguridad puede ser libremente especificada cuando se configura la función de copia de seguridad.</p>

Implementar copia de seguridad del sistema automáticamente

Habilitado: El archivo de copia de seguridad del sistema se actualizará inmediatamente una vez realizados cambios significativos a los datos de Security Platform.



Precondiciones: Se deben [configurar](#) las copias de seguridad automáticas. También se debe permitir acceso a escritura del archivo de copia de seguridad del sistema.

Deshabilitado: El archivo de copia de seguridad del sistema no se actualizará inmediatamente una vez realizados cambios significativos a los datos de Security Platform. Se configuran copias de seguridad automáticas y se permite el acceso a escritura del archivo de copia de seguridad, el archivo se actualizará con próxima copia de seguridad del sistema programada.

Uso de la clave pública de la Tarjeta de Recuperación de emergencia del archivo

Habilitado: Ingrese una ruta de acceso que incluya el nombre del archivo público, por ej.

\\NombreServidor\NombreCarpeta\NombreArchivo.xml.

Esta ruta será implementada cuando se configure la recuperación de emergencia.

Si la restauración de emergencia ha sido configurada en una computadora de Security Platform, esta configuración no tendrá ningún efecto en esa computadora.



Asegúrese de ingresar una ruta válida que sea accesible por todas las computadoras de Security Platform. De otro modo, la configuración de la restauración de emergencia fallará.

Deshabilitado: La tarjeta de seguridad para la recuperación de emergencia se puede crear o seleccionar al configurar la recuperación de emergencia.

[Detalles de la configuración de recuperación de emergencia ¿Cómo se crea un archivo de almacenamiento de clave pública a partir de un archivo de tarjeta de seguridad?](#)

Implementación de la configuración

Habilitado: La configuración del restablecimiento de contraseña es obligatorio en el proceso de inicialización de Security Platform.

<p><i>del restablecimiento de contraseña</i></p>	<p>Si Security Platform ha sido inicializado sin configurar el restablecimiento de contraseña, no hay ninguna imposición para configurarlo.</p> <p>Deshabilitado: No hay ninguna imposición para configurar el restablecimiento de contraseña. El restablecimiento de contraseñas puede ser configurado luego de la inicialización de Security Platform por medio de Herramienta de configuración - Restablecimiento de contraseña - Configurar....</p>
<p><i>Uso de la clave pública de la Tarjeta de restablecimiento de contraseña del archivo</i></p>	<p>Habilitado: Ingrese una ruta de acceso que incluya el nombre del archivo público, por ej. \\NombreServidor\NombreCarpeta\NombreArchivo.xml. Esta ruta será implementada cuando se configure el restablecimiento de contraseña. Si el restablecimiento de contraseña ha sido configurada en una computadora de Security Platform, esta configuración no tendrá ningún efecto en esa computadora.</p> <p> Asegúrese de ingresar una ruta válida que sea accesible por todas las computadoras de Security Platform. De otro modo, el restablecimiento de contraseña fallará.</p> <p>Deshabilitado: La tarjeta de seguridad de restablecimiento de la contraseña se puede crear o seleccionar al configurar el restablecimiento de la contraseña.</p> <p>Detalle del restablecimiento de contraseña ¿Cómo se crea un archivo de almacenamiento de clave pública a partir de un archivo de tarjeta de seguridad?</p>

Configuraciones de versiones de productos previos

Configuraciones que son válidas sólo para versiones de productos anteriores.

Política	Explicación	Valor predeterminado
<i>Localización del archivo de restauración de seguridad</i>	<p>Esta configuración es solo relevante para las versiones mas antiguas del software de solución Security Platform.</p> <p>En las versiones mas antiguas, la ubicación del archivo de recuperación de emergencia puede ser establecido explícitamente durante la inicialización de Security Platform. Con esta política, la ubicación del archivo puede ser implementada.</p> <p>En la versión actual, la ubicación del archivo es establecido automáticamente .</p>	---
<i>Iniciar URL desde el asistente para registro de certificado</i>	Consulte políticas de usuario .	Deshabilitado



La solución Infineon Security Platform - Administración de política

Políticas de usuario de Infineon Security Platform

El software solución Infineon Security Platform admite las siguientes configuraciones de políticas de usuario.



En [modo servidor](#) las Políticas de Usuario se configuran en todo el dominio por un administrador de dominio a través de Trusted Computing Management Server. Tenga en cuenta que las configuraciones que sólo son válidas para el modo de servidor se describen en el archivo de plantilla administrativa suministrado por Trusted Computing Management Server.



Valor predeterminado: Si una política no ha sido explícitamente establecida (e.j. el Editor de política del grupo local muestra el estado **No configurado**), entonces el software solución Security Platform implícitamente aplica un valor por predeterminado.

Todas las configuraciones de las versiones

Configuraciones que son válidas tanto para la versión en modo servidor como para la versión en modo stand-alone.

Política	Explicación	Valor predeterminado
<i>Contraseña de usuario básico - Longitud mínima de contraseña</i>	<p>Habilitado: Ingrese la longitud mínima de la contraseña de usuario básico que desee, e.j. 6. La longitud mínima de la contraseña es válida para las contraseñas de usuario básico que serán establecidas o cambiadas posteriormente.</p> <p>Deshabilitado: La longitud mínima de la contraseña es de 6 caracteres.</p> <p>Detalles en el manejo de contraseñas</p>	Habilitado caracteres
<i>Contraseña de usuario básico - La contraseña debe reunir los requerimientos de complejidad</i>	<p>Habilitado: Los requerimientos de complejidad de contraseñas son impuestos para las contraseñas de usuario básico que serán establecidas o cambiadas posteriormente.</p> <p>Deshabilitado: No se imponen requerimientos de complejidad de contraseña.</p> <p>Detalles en complejidad de contraseñas</p>	Deshabilitado
<i>Contraseña de usuario básico - Período máximo de la contraseña de usuario básico</i>	<p>Determina el período de tiempo (en días) en que se puede utilizar la contraseña de usuario básico antes de que el sistema solicite su cambio.</p> <p>Habilitado:</p> <ul style="list-style-type: none">• <i>Perodo máximo de la contraseña de usuario básico:</i> Ingrese el período máximo deseado para la contraseña de usuario básico, por ejemplo 42 días.• <i>Advertencia de caducidad de la contraseña de usuario básico:</i> Indique con cuántos días de anticipación de debe notificar al usuario antes de que expire la contraseña de usuario básico, por ejemplo 7 días.	Deshabilitado

	<p>Deshabilitado: No existe un período máximo para la contraseña de usuario básico, o sea las contraseñas no caducan.</p>	
<p><i>Frase de contraseña de usuario básico - Longitud mínima de frase de contraseña</i></p>	<p>Habilitado: Ingrese la longitud mínima de la frase de contraseña de usuario básico que desee, e.j. 20. La longitud mínima de la frase de contraseña es válida para todas las frases de contraseñas de usuario básico que serán establecidas o cambiadas posteriormente.</p> <p>Deshabilitado: La longitud mínima de la frase de contraseña es de 20 caracteres.</p> <p> Esta política es solo relevante si es utilizada la autenticación mejorada</p> <p>Detalles en autenticación mejorada</p>	<p>Habili caracte</p>
<p><i>Frase de contraseña de usuario básico - La frase de contraseña debe reunir los requerimientos de complejidad</i></p>	<p>Habilitado: Los requerimientos de complejidad son impuestos para las frases de contraseñas de usuario básico que serán establecidas o cambiadas posteriormente.</p> <p>Deshabilitado: No serán impuestos requerimientos de complejidad.</p> <p> Esta política es solo relevante si es utilizada la autenticación mejorada</p> <p>Detalles en complejidad de contraseñas Detalles en autenticación mejorada</p>	<p>Desha</p>
<p><i>Inicialización rápida de control</i></p>	<p>Habilitado/Permitir: Se pueden utilizar el Asistente de inicialización rápida o el Asistente de inicialización Security Platform y el Asistente de inicialización del usuario para inicializar plataformas y usuarios.</p> <p>Habilitado/Imponer: El Asistente para la inicialización rápida deberá utilizarse para inicializar las plataformas o los usuarios. Las demás funciones disponibles (EFS, PSD) deben ser configuradas en</p>	<p>Habili</p>

	<p>un principio con el Asistente de inicialización rápida.</p> <p>Deshabilitado: El Asistente de inicialización rápida no se puede utilizar para inicializar plataformas y usuarios. En su lugar se debe utilizar el Asistente de inicialización de Security Platform y el Asistente de inicialización del usuario.</p>	
<p><i>Permiso de usuario para deshabilitar temporalmente la función de Security Platform</i></p>	<p>Habilitado: El usuario de Infineon Security Platform puede desactivar las funciones activas de Security Platform hasta que la computadora se reinicie la próxima vez.</p> <p>Deshabilitado: La capacidad de deshabilitar temporalmente Infineon Security Platform no está disponible en la interfaz de usuario del software de solución Security Platform</p> <p> Esta política sólo es relevante para Security Platforms con un Infineon Trusted Platform Module 1.1.</p> <p>Cuando un usuario cierra la sesión y otro usuario diferente inicia una sesión, las funciones desactivadas de Security Platform permanecen desactivadas hasta que se reinicie la computadora.</p>	Habili
<p><i>Permitir la configuración de correo electrónico seguro</i></p>	<p>Habilitado: El usuario está autorizado a configurar la función de Security Platform <i>Correo electrónico seguro</i>.</p> <p>Deshabilitado: El usuario no puede configurar esta función, pero puede ser utilizada una configuración previa.</p>	Habili
<p><i>Permiso de configuración de EFS</i></p>	<p>Habilitado: El usuario tiene permitido configurar la función de Security Platform <i>Encriptación de archivo y encriptación de carpeta con Encrypting File System (EFS)</i>.</p> <p>Deshabilitado: El usuario no puede configurar esta</p>	Habili

	<p>función, pero puede ser utilizada una configuración previa.</p> <p> EFS no se admite en ediciones de Windows Home.</p>	
<i>Permiso de configuración de PSD</i>	<p>Habilitado: El usuario tiene permitido configurar la función de Security Platform <i>Encriptación de archivo y carpeta con el Personal Secure Drive (PSD)</i>.</p> <p>Deshabilitado: El usuario no puede configurar esta función, pero puede ser utilizada una configuración previa.</p>	Habili
<i>Implementación del permiso de restablecimiento de la contraseña</i>	<p>Habilitado: Habilitar el restablecimiento de contraseña es obligatorio en el proceso de inicialización de usuario. Si Security Platform ha sido inicializado sin habilitar el restablecimiento de contraseña, no hay ninguna imposición para habilitar el restablecimiento de contraseña.</p> <p>Deshabilitado: No hay ninguna imposición para habilitar el restablecimiento de contraseña. El restablecimiento de contraseñas puede ser habilitado luego de la inicialización de usuario por medio de Herramienta de configuración - Restablecimiento de contraseña - Permitir....</p>	Desha
<i>Implementar la autenticación avanzada</i>	<p>Habilitado: Los usuarios de Security Platform deben utilizar autenticación mejorada (con frase de contraseña de usuario básico).</p> <p>Deshabilitado: Los usuarios de Security Platform pueden decidir si quieren utilizar autenticación mejorada (con frase de contraseña de usuario bsico) o autenticación de contraseña (con contraseña de usuario básico).</p> <p> Esta política sólo es relevante si al menos se ha</p>	Desha

	<p>habilitado un dispositivo de autenticación para todos los usuarios. Si ya se inicializó Security Platform sin seleccionar un dispositivo de autenticación, no hay ninguna imposición para utilizar la Autenticación avanzada.</p> <p>Detalles en autenticación mejorada</p>	
<p><i>Habilitar almacenamiento de contraseña de usuario básico</i></p>	<p>Habilitado: La contraseña de usuario básico puede ser almacenada en el software de Infineon Security Platform , esto reduce el numero de ingresos de contraseñas durante el proceso de inicio de sesión actual. Esto minimiza el numero de contraseñas consultadas al usuario.</p> <p>Deshabilitado: El diálogo de contraseña de usuario básico no ofrece la posibilidad de almacenar temporalmente la contraseña de usuario básico.</p>	<p>Habili</p>
<p><i>Iniciar URL desde el asistente para registro de certificado</i></p>	<p>Habilitado: Esta característica especifica la dirección de red que será utilizada por el Asistente para la inicialización de Infineon Security Platform para recuperar los certificados utilizando el explorador de red.</p> <p>La página en la cual obtener un certificado sólo está disponible en el asistente para la inicialización de usuarios, si esta configuración esta habilitada y al menos un Security Platform se seleccionó para su configuración.</p> <p>Deshabilitado: La página para obtener un certificado no esta disponible en el asistente para la inicialización de Security Platform.</p> <p>Notas:</p> <ul style="list-style-type: none"> • Esta configuración esta también admitida como política de sistema para ser compatible con las primeras versiones del software de solución Security Platform. • Recomendación: Utilice esta configuración como política de usuario. 	<p>Desha</p>

	<ul style="list-style-type: none"> • Mientras esta configuración sea independiente de uso del certificado, hay también al respecto una política de usuario especial para certificados EFS (<i>Tipo y registración de certificado EFS</i>). 	
<p><i>Tipo y registración de certificado EFS</i></p>	<p>Habilitado: Puede restringir el tipo de certificado EFS. También puede habilitar la inscripción de certificados externos EFS especificando la dirección de red de la entidad certificada.</p> <p>1. tipo de certificado EFS: Especifique si desea permitir todos los tipos de certificados (certificados de dominio, externos y auto firmados) o solo ciertos tipos de certificados. Esta restricción será aplicada cuando los usuarios van inscribir o seleccionar los certificados</p> <ul style="list-style-type: none"> • Certificado de dominio: Un certificado inscripto por una entidad certificada dentro de su dominio. • Certificado externo: Un certificado inscripto por medio de una entidad certificada externa accesible por medio de la WWW. • Certificado auto firmado: Un certificado creado en su propia computadora. <p>2. URL de solicitud de certificado: Ingrese la dirección de red de solicitud de certificado de la entidad certificada a ser utilizada para la inscripción de certificado EFS, e.j. https://www.companyname.com/foldername. Esta ruta destino será utilizada cuando se necesite un certificado EFS de una entidad certificada externa (CA por sus siglas en inglés).</p> <ul style="list-style-type: none"> • La ruta de solicitud de certificado es opcional. • Los usuarios no podrán solicitar certificados EFS externos si no especifica una ruta aquí. 	<p>Desha</p>

	<ul style="list-style-type: none"> • Si desea habilitar los certificados EFS externos, entonces ingrese una ruta válida que sea accesible por todas las computadoras de Security Platform. De otro modo la inscripción de certificados EFS fallará. <p>Deshabilitado: El tipo de certificado EFS no está restringido. No está establecida la dirección Web a utilizar para recuperar los certificados EFS, es decir que los usuarios no podrán solicitar certificados EFS externos.</p> <p>Notas:</p> <ul style="list-style-type: none"> • Observe que certificados EFS no son utilizados solamente para EFS, sino también para PSD. • Mientras esta configuración es válida solamente para certificados EFS (para ser utilizado para EFS o PSD), hay también una política que es independiente de la utilización del certificado (<i>Inicio de URL desde el asistente para registración de certificado</i>). <p>Como inscribir y seleccionar certificados EFS.</p>	
<i>Advertencia de expiración de certificado EFS</i>	<p>Habilitado: Los usuarios de Security Platform serán notificados por un diálogo antes que expire el certificado EFS. Especifique cuando debería tener lugar esta notificación, por ejemplo 14 días antes desde la expiración del certificado.</p> <p>Deshabilitado: No hay notificación de la expiración de certificado.</p>	Los usuarios serán notificados antes de la expiración del certificado.
<i>Período de validez de los certificados EFS auto-assinados</i>	<p>Habilitado: Especifique el período de tiempo en que los certificados auto-firmados EFS serán válidos.</p> <p>Deshabilitado: El período de validez es de 10 años.</p>	Habilitado: El período de validez es de 10 años.
<i>Ubicación del archivo para Personal Secure</i>	<p>Habilitar la unidad predeterminada PSD: Esto establece el dispositivo en el cual serán creados los archivos de imagen de Personal Secure Drive.</p>	Deshabilitado: No se establece la unidad predeterminada PSD.

<p><i>Drive</i></p>	<p>Ingrese una letra de unidad válida en el campo de edición, incluyendo dos puntos pero sin ninguna ruta adicional (por ejemplo, C:). Si la letra de unidad es inválida, los usuarios no podrán crear archivos de imagen de Personal Secure Drive.</p> <p>Deshabilitado: El usuario puede elegir la unidad en que serán creados los archivos de imagen de Personal Secure Drive.</p>	
<p><i>Espacio mínimo libre después de la creación de PSD</i></p>	<p>Habilitado: Si un PSD es guardado en la unidad de sistema (donde se encuentra el sistema operativo actual), se definirá una cantidad de espacio libre a dejarse luego de la configuración PSD. Especifique cuanto espacio debe ser dejado en la unidad de sistema luego de la configuración PSD.</p> <p>Deshabilitado: No hay restricciones concernientes la espacio en la partición de sistema luego de la creación PSD.</p> <p><u>Ejemplo:</u> La política esta habilitada y establecida a 5000 MB. El tamaño mínimo de la unidad de PSD es 20 MB para Windows 7 y Windows Vista, y 10 MB para el resto de sistema operativos.</p> <ul style="list-style-type: none"> • Asumiendo que el espacio libre antes de la creación de PSD es de 5050 MB, entonces el espacio máximo de PSD debería ser de 50 MB. • Asumiendo que el espacio libre sea de 5000 MB, entonces no podrá crear PSD en la unidad de sistema. 	<p>La política habilitada establecida a 5000 MB.</p>
<p><i>Permiso de importación de clave para usuario</i></p>	<p>Habilitado: Los usuarios de Security Platform tienen permitido importar claves privadas dentro de Security Platform. Observe que esas claves privadas son importadas junto con los certificados por medio de Visor de certificados y selección de certificados.</p> <p>Deshabilitado: Los usuarios de Security Platform no tienen permitido importar claves privadas dentro</p>	<p>Habilitado</p>

	de Security Platform.	
<p><i>Implementación de protección fuerte de clave privada para llaves de firma MS-CAPI</i></p>	<p>Habilitado: Todas las claves utilizadas en forma exclusiva para las operaciones de firmado por la interfase MS-CAPI están protegidas por una fuerte protección privada. En este caso la clave está protegida por su propia contraseña que debe ser ingresada siempre que la clave sea utilizada para una operación de firmado.</p> <p>Deshabilitado: Las claves de firmado no están protegidas en forma especial.</p> <p> Esta contraseña específica puede ser almacenada para evitar la entrada repetitiva. Desde que esta contraseña no está relacionada con la clave de usuario básica, el mecanismo de almacenamiento utilizado para las contraseñas de usuario básico no afecta esta contraseña.</p>	<p>Desha</p>
<p><i>Creación de la Clave del usuario básico no migrable</i></p>	<p>Habilitado/A pedido: Se les solicitará a los usuarios la creación de una Clave de usuario básico no migrable cuando utilicen Infineon TPM Strong Cryptographic Provider por primera vez. Tenga en cuenta que Strong Cryptographic Provider requiere una Clave de usuario básico no migrable.</p> <p>Habilitado/Automático: La Clave de usuario básico no migrable es creada automáticamente para los nuevos usuarios durante la inicialización del usuario. La Clave de usuario básico no migrable es creada a pedido para los usuarios que ya se encuentran inicializados.</p> <p>Deshabilitado: No se puede crear una Clave de usuario básico no migrable; es decir, no se puede utilizar Infineon TPM Strong Cryptographic Provider.</p>	<p>Habili pedido</p>

Configuraciones de la versión en modo Stand-alone

Configuraciones que son válidas sólo para la versión en modo stand-alone.

Política	Explicación	Valor predeterminado
<i>Evento de alerta de copia de seguridad</i>	<p>Habilitado: Los usuarios de Security Platform serán notificados por un diálogo, si la copia de seguridad de credenciales de usuario específico y claves han fallado (por ejemplo, debido a que la ubicación de la copia de seguridad no es accesible) Especifique cada cuanto debería mostrarse esta notificación, por ejemplo cada 2 días luego de la falla de la copia de seguridad, hasta la próxima copia de seguridad exitosa.</p> <p>Deshabilitado: No hay notificación de la falla de la copia de seguridad.</p>	Los usuarios son notificados diariamente.
<i>Permiso de registración de usuario</i>	<p>Habilitar/permitir interfase y asistente para la administración: Los usuarios se pueden inicializar por medio de la interfaz Management Provider, el Asistente para la inicialización rápida o el Asistente para la inicialización de usuarios.</p> <p>Habilitar/permitir la interfase proveedora de la administración solamente: El usuario puede solo invocar la interfase proveedora de administración pero no puede ejecutar las herramientas de solución Security Platform.</p> <p>Deshabilitado: Security Platform no permite que el usuario lleve a cabo ninguna función.</p>	Habilitar/permitir interfase y asistente para la administración



TPM
©Infineon Technologies AG

La Solución Infineon Security Platform

Servicios de integración de Security Platform

Los servicios de integración de Security Platform le permite a las aplicaciones estándar utilizar la funcionalidad del Trusted Platform Module. Esto es posible para aplicaciones que admitan Microsoft Crypto-API o PKCS #11 Crypto-API, Microsoft Cryptography Next Generation (CNG) API, o PKCS #11 Crypto-API.

La tabla siguiente lista todos los componentes de los servicios de integración disponibles:

Nombre del proveedor	Explicación	Crypto-API	Aplicaciones/servicios admitidos (ejemplos)
Infineon TPM Cryptographic Provider(Usuario CSP, sin soporte AES)	Utilizado para los certificados de usuario. Para utilizar claves privadas de certificados se requiere	Microsoft Crypto-API	<ul style="list-style-type: none"> • Encriptación de archivos y carpetas con EFS y PSD. • Correo electrónico seguro (S/MIME) con Outlook y Windows Mail/Outlook Express • Autenticación de cliente SSL/TLS con Internet Explorer • Inscripción de certificados mediante certificado snap-in de Microsoft y entidades certificadas públicas (CA por sus siglas en inglés) que admitan Internet Explorer • Macros firmadas en Microsoft Office • Punto de control
Infineon TPM RSA and AES Cryptographic Provider (Usuario CSP, incluyendo soporte AES. No disponible bajo Windows 2000.)	Autenticación de usuarios . La clave privada de certificados de usuario es migrable, ej. esta puede transferirse a otro Trusted Platform Module.		

			<p>VPN utilizando Microsoft Crypto-API</p> <ul style="list-style-type: none"> • Aplicaciones cliente confiables utilizando Microsoft Crypto-API • Firma digital y encriptación de archivos Adobe • Autenticación de usuarios con EAP-TLS
<p>Infineon TPM PKCS #11 Provider (También llamado "TPM Cryptoki Token")</p>		<p>PKCS #11 Crypto-API</p>	<ul style="list-style-type: none"> • Correo electrónico seguro (S/MIME) con Mozilla Thunderbird • Autenticación de cliente SSL/TLS con Mozilla Firefox • Inscripción de certificados mediante entidades certificadas públicas (CA por sus siglas en inglés) soportando Mozilla Firefox • Inscripción de certificados mediante Sun CA basada en servidor certificado. • Acceso a la red seguro y acceso remoto seguro con RSA SecurID • Aplicaciones de

			cliente confiables utilizando la interfase PKCS #11
Infineon TPM Strong Cryptographic Provider (sin soporte AES)	Utilizado para los certificados de usuario. Se requiere la Autenticación del usuario cada vez que se utilice la clave privada del certificado. La clave privada del Certificado del usuario no es migrable, es decir, relacionada al Trusted Platform Module.	Microsoft Crypto-API	<ul style="list-style-type: none"> • Especialmente destinado para la autenticación del usuario en un VPN
Infineon TPM Platform Cryptographic Provider (Platform CSP)	Utilizado para los certificados de computadora. No se requiere autorización dedicada para utilizar clave privada de certificados, desde que la clave privada de certificados de computadora esta protegida por Trusted Platform Module. La clave privada de certificados de	Microsoft Crypto-API	<ul style="list-style-type: none"> • Autenticación IEEE 802.11 EAP-TLS entre cliente WLAN y servidor RADIUS (en la fase TLS handshake), en la empresa administrada en el lado del cliente en la WLAN • Autenticación IEEE 802.1X EAP-TLS en LANs cableadas entre cliente y servidor RADIUS (en la fase TLS handshake), en la empresa

	<p>computadora no es migrable, ej. fuera de los límites de Trusted Platform Module.</p> <p>Par utilizar la plataforma CSP, debe ser un administrador o miembro del grupo de administradores.</p>		<p>administrada del lado del cliente</p> <ul style="list-style-type: none"> • Autenticación de computadoras IPsec en el lado del cliente VPN
<p>Infineon TPM Key Storage Provider (KSP)</p>	<p>Key Storage Provider restringido. Provee acceso solamente a otros Infineon TPM Cryptographic Service Providers. Soporta solamente operaciones de firma y descriptación, pero no la creación de un par de claves TPM RSA.</p>	<p>Microsoft Cryptography Next Generation (CNG) API</p>	<ul style="list-style-type: none"> • Microsoft .NET 3.0 • Para más ejemplos, vea otros Cryptographic Service Providers.

Para otras aplicaciones admitidas, por favor contacte al soporte de su producto.



La Solución Infineon Security Platform

Servicios de Security Platform

Los servicios de Security Platform le proveen una pila de software compatible con Trusted Computing Group (TCG).

La pila de software TCG (TSS por sus siglas en inglés) contiene los siguientes módulos):

- Proveedor de servicio TSS (TCG Software Stack)
- Servicio de núcleo TSS
- Librería de controladores de dispositivos TSS

La pila de software TCG es una parte integral de la plataforma compatible con TCG, y le provee funciones que las aplicaciones y sistemas operativos avanzados pueden utilizar.



Recomendación:

Contacte el soporte de su producto para verificar si hay disponible actualizaciones de firmware para su Trusted Platform Module.



La solución Infineon Security Platform

Server Integration Services

El componente *Server Integration Services* se comunica con Trusted Computing Management Server. Permite la integración de Security Platform con el Trusted Computing Management Server (vea [modo servidor](#)).

Es un componente interno sin ninguna interfaz de usuario gráfica. Client Side Control Agent es un componente principal de Server Integration Services.

Nombre del componente	Explicación
<i>Client Side Control Agent</i>	Sincroniza el estado de la plataforma y las credenciales del usuario con el Trusted Computing Management Server (ver estados de sesión de usuario).

Si Server Integration Services no está incluido en su versión del software Infineon TPM Professional Package, contáctese con su proveedor para obtenerlo.

Para saber cómo instalar Server Integration Services, lea *ReadmeServerIntegrationServices.txt*. Para identificar la versión instalada, verifique la versión de *Client Side Control Agent* mencionada en *Más detalles* de la [Herramienta de configuración](#).



La Solución Infineon Security Platform

Uso de las funciones de Security Platform en sus aplicaciones

La Solución Infineon Security Platform soporta la [Funcionalidad de clave pública provista por Windows 2000/Windows XP](#) y la [Funcionalidad PKI basada en el estándar PKCS #11](#). Este soporte abarca la cadena de procesos completa de [inscripción](#) de [certificados digitales](#), la configuración de las aplicaciones disponibles que utilizan certificados, y la administración de las funciones específicas del Usuario de Infineon Security Platform.

Las aplicaciones que utilizan certificados digitales son:

- [Personal Secure Drive \(PSD\)](#)
- [Sistema de encriptación de archivos \(EFS por sus siglas en inglés\)](#)
- [Correo electrónico seguro](#)
- [Macros firmadas en Microsoft Word](#)
- [Conexiones seguras de red](#)



©Infineon

Solución Infineon Security Platform

Certificados e infraestructura de claves públicas (PKI, por sus siglas en inglés)

Antes de poder utilizar las características de Security Platform en sus aplicaciones, necesita solicitar uno o más certificados. Si no utiliza certificados autofirmados o certificados de una entidad certificada (CA por sus siglas en inglés) en su dominio, necesita tener acceso a una infraestructura de clave pública (PKI por sus siglas en inglés).

Los certificados se administran con el [Visor de certificados/selección de certificados de Security Platform](#).



Los siguientes temas proveen información básica concernientes a los certificados y PKI, los cuales son diseñados especialmente para los administradores.

[Certificados digitales](#)

[Infraestructura de clave pública en sistemas operativos Windows](#)

[Infraestructura de claves públicas en PKCS #11](#)



©Infineon

Technologies AG

Infineon Security Platform Solution

Certificados digitales

Los certificados digitales son credenciales electrónicas que confirman la identidad de una persona o empresa. Básicamente, un certificado digital asocia la identidad del propietario del certificado digital a un par de claves electrónicas que pueden utilizarse para firmar información digital.

Un certificado digital debe contener la información siguiente:

- Clave pública del propietario
- Nombre del propietario
- Fecha de caducidad del certificado digital
- Número de serie del certificado digital
- Nombre de la entidad emisora del certificado
- Certificado digital de la entidad emisora del certificado digital

Además de esta información, un certificado digital también puede incluir otros datos proporcionados por el usuario, tales como:

- Dirección postal
- Dirección de correo electrónico (en algunas aplicaciones, este campo es obligatorio)
- Información básica de registro (como el país, la edad, el sexo, etc.)

Suele ser otra entidad de confianza, denominada entidad emisora de certificados (CA), quien se encarga de emitir y administrar los certificados digitales. El proceso para [obtener un certificado](#) puede generalizarse para un gran número de entidades emisoras de certificados. Hay bastantes entidades emisoras de certificados que atienden al número creciente de certificados digitales mediante la emisión de certificados que pueden utilizarse para fines que van desde el correo electrónico seguro a las comunicaciones seguras en Internet o en una intranet.



©Infineon

La Solución Infineon Security Platform

Obtención de un certificado digital de una entidad certificada pública

Para utilizar la tecnología de clave pública de Microsoft, primero necesita obtener un **ID Digital**. Debido a la creciente demanda de IDs digitales, un gran número de entidades certificadas comerciales (CA por sus siglas en inglés) como VeriSign y Thawte, ofrece certificados digitales que se pueden utilizar para varios propósitos como el correo electrónico seguro y la firma de macros.

Las CAs emiten distintos tipos de certificados, incluyendo los siguientes:

- Certificados personales para que firmen digitalmente el correo electrónico las personas e intercambien información segura sobre una red pública.
- Certificados de autenticación de clientes y de servidores, que se utilizan para transmitir información de forma segura entre clientes y servidores.
- Certificados de edición de software, que se utilizan para las empresas de software comercial que firman digitalmente su software.

Las CAs también pueden emitir otros tipos de certificados. Cada CA tiene su propia Declaración de prácticas de certificados (CPS por sus siglas en inglés) la cual forman las bases sobre las que operan estas CAs. Es buena idea visitar el sitio Web de alguna CA y leer su CPS antes de decidir desde cual obtendrá su certificado.

Cuando selecciona una CA, considere las siguientes cuestiones:

- ¿La CA es una entidad confiable que opera con prácticas de certificación que cubre sus necesidades y lo hace de una forma eficiente en su región?
- ¿La CA es conocida? ¿La mayoría de las personas reconocen su CA como confiable y de buena reputación? Si selecciona una CA con una reputación cuestionable, los usuarios pueden rechazar su certificado.
- ¿La CA requiere información detallada de su persona para verificar sus credenciales?
- ¿La CA tiene algún sistema para recibir solicitudes de certificado en línea, tales como las solicitudes que se generan por un servidor de gestión de claves? Tal sistema le puede ahorrar mucho tiempo y acelerar el proceso de solicitud, obtención e instalación de certificados.
- ¿El costo del servicio de la CA concuerda con sus requerimientos?

Una vez que decidió de que CA comercial va a obtener su certificado, debe enviar una solicitud a esa CA. Muchas CA admiten procedimientos de

inscripción en línea.



Seleccione una de los [Cryptographic Service Providers](#) que se entregaron con la Solución Security Platform para utilizarse para su certificado.

Una vez que se procesó su solicitud, recibirá instrucciones sobre cómo instalarlo y utilizarlo.



©Infineon

Technologies AG

Solución Infineon Security Platform

Infraestructura de clave pública (PKI) en sistemas operativos Windows

El sistema operativo de Microsoft Windows 2000 introdujo una infraestructura de clave pública integral (PKI) en la plataforma de Windows. Dicha infraestructura mejora los servicios criptográficos de clave pública basados en Windows que fueron introducidos durante los últimos años, suministrando un conjunto integrado de servicios y herramientas administrativas para la creación, puesta en funcionamiento y administración de aplicaciones basadas en claves públicas.

Esto significa que los desarrolladores de aplicaciones pueden aprovechar los mecanismos de seguridad de secreto compartidos o los mecanismos de seguridad basados en claves públicas, según conveniencia. Más aún, las empresas también podrán administrar sus entornos y aplicaciones con herramientas y políticas constantes en toda la organización.

El PKI no reemplaza los mecanismos existentes de autorización y confianza de dominio de Windows basados en el controlador de dominio (DC) y Kerberos Key Distribution Center (KDC). En cambio, el PKI trabaja con estos servicios y provee mejoras que permiten a las aplicaciones escalar fácilmente a los requisitos de Internet y Extranet. La infraestructura de clave pública cumple con la necesidad de integridad y confidencialidad y autenticación e identificación distribuida y escalable ofreciendo una red de servicios, tecnología, protocolos y estándares que le permiten poner en funcionamiento y administrar sistemas de seguridad de la información fuertes y escalables. Las estaciones de trabajo y los servidores que corren bajo Windows 2000 o Windows NT4 ofrecen uniformemente asistencia para la creación, puesta en funcionamiento y administración de aplicaciones basadas en claves públicas.

Entre los componentes básicos de una infraestructura de clave pública están los certificados digitales, las listas de revocaciones de certificados y las entidades emisoras de certificados. Los administradores de empresas deben asegurarse de que se encuentra una infraestructura de clave pública montada antes de comenzar a utilizar los servicios criptográficos de clave pública en sus redes.

En Microsoft TechNet encontrará más información sobre los conceptos de Microsoft PKI y sobre los servicios de certificados.

Para configurar una PKI dentro de una organización deben llevarse a cabo los pasos siguientes:

- Configuración del Active Directory
- Instalación de una entidad certificada
- Cambio de plantilla del certificado de usuario
- Inscripción de certificados

Este documento ofrece una introducción a algunos de los elementos enumerados anteriormente y le presenta vínculos que proveen más información sobre estos temas.



©Infineon

Technologies AG

La Solución Infineon Security Platform

Configuración de Active Directory

Active Directory es el servicio de directorio utilizado por Microsoft Windows 2000. Constituye la base de las redes distribuidas de Windows 2000. Active Directory facilita el almacenamiento seguro, estructurado y jerárquico de la información sobre los elementos en las redes de una empresa, como ser, sus usuarios, computadoras, servicios, etc.

Active Directory debe estar instalado en el dominio en el que se desea configurar una PKI, ya que toda la información relacionada a la ubicación y políticas de la entidad certificada, los certificados y las listas de revocación se almacenan en el Active Directory.

Una vez que ha instalado un Active Directory para su dominio, necesitará agregarle usuarios. Puede utilizar el snap-in "Active Directory Users and Computers" para agregar, mover, borrar y modificar las propiedades de elementos como usuarios, contactos, grupos, etc.

En Microsoft TechNet encontrará más información sobre Active Directory.

El siguiente paso en la configuración de una PKI es la instalación de una entidad certificada.



Technologies AG

La Solución Infineon Security Platform

Instalación de una entidad certificada

Una entidad certificada (CA por sus siglas en inglés) es un servicio que emite los certificados necesarios para ejecutar una infraestructura de clave pública (PKI por sus siglas en inglés). Estos certificados usualmente se emiten a quienes lo solicitan basados en un conjunto de criterios ya establecidos. Una CA garantiza la validez de la unión entre la clave pública del sujeto y la información de la identidad del mismo que se almacena en el certificado que se emite. Una CA puede ser comercial externa, o puede ser una que ejecuta su empresa. (Ya que una CA es un punto importante de confianza en una empresa, la mayoría de las organizaciones eligen tener una CA propia).

La infraestructura de clave pública de Windows 2000 asume un modelo de CA jerárquico que se caracteriza por su escalabilidad, fácil administración, y soporte para certificados emitidos por CAs comerciales de terceros.

Windows 2000 soporta dos tipos de servicios de CA: empresarial o independiente. La diferencia primordial entre los dos servicios de CA radica en la manera en que emiten los certificados. Una CA independiente emite certificados sin autenticar al solicitante y usualmente requiere que un administrador de CA apruebe las solicitudes basado en alguna información adicional.

Una CA empresarial requiere la existencia de un dominio de Windows 2000 y autentifica al solicitante basado en su información de sesión de dominio. Por otro lado, una CA empresarial utiliza plantillas de certificados para distinguir entre los diferentes tipos que existen basándose en el uso pretendido. Los usuarios pueden obtener diferentes tipos de certificados basados en sus derechos de acceso dentro de un dominio y el propósito por el cual desean utilizar los certificados.

Debe instalar una CA empresarial si pretende emitir certificados sólo a usuarios o computadoras dentro de una organización que es parte de un dominio de Windows 2000. Debe instalar una CA independiente si va a emitir certificados a usuarios o computadoras que se encuentran fuera de un dominio de Windows 2000.

Nota: Una CA empresarial tienen un módulo de políticas especial que asegura la forma en que se procesan y emiten los certificados. La información de la política que utilizan estos módulos de políticas se almacenan en un objeto CA en el Active Directory. Por lo tanto debe tener un Active Directory y un servidor DNS completamente funcional antes de configurar una CA empresarial.

Refiérase a las instrucciones de Microsoft TechNet sobre el modo de instalación de una entidad certificada para su dominio.

El próximo paso en la configuración de un PKI es cambiar la Plantilla de certificado de usuario para habilitar la utilización de los [Cryptographic Service Providers](#) que se entregan con la Solución Security Platform.



©Infineon

Technologies AG

La Solución Infineon Security Platform

Cambio de plantilla del certificado de usuario

Al utilizar el Asistente de solicitud de certificado, el usuario puede seleccionar sólo uno de los Cryptographic Service Providers (CSP), que se encuentran almacenados en el directorio activo para la plantilla de certificado apropiada. Para habilitar los [Cryptographic Service Providers](#) que se entregaron con la Solución Security Platform para una solicitud de certificado de usuario, se debe modificar la plantilla de certificado de usuario correspondiente.

Cómo edita la plantilla de certificado de usuario que se encuentra almacenada en el Active Directory?

1. **Instalación de ADSI Edit**

La plantilla de certificado de usuario se puede modificar por medio de Active Directory Services Interface Editor (ADSI editor). Este editor es un Microsoft Management Snap-in el cual es parte de las herramientas de soporte que se encuentran ubicadas en la carpeta Support\Tools en el CD del sistema operativo de Windows 2000 Server. Para instalar las herramientas, haga doble clic sobre el icono de Setup en esa carpeta. Para más información sobre la instalación y utilización de Windows 2000 Support Tools y Support Tools Help, vea el archivo Readme.doc en la carpeta Support\Tools en el CD del sistema operativo de Windows 2000 Server. Para más información sobre la utilización de ADSI Edit, vea Microsoft Windows 2000 Resource Kit Tools Help.

2. **Ejecutar ADSI Edit**

Adsiedit.msc (el MMC snap-in para ADSI Edit) automáticamente intenta cargar el dominio actual en el cual el usuario inició sesión. Si la computadora se encuentra instalada en un grupo de trabajo o no inició sesión en un dominio, ocurre repetidamente el mensaje de error "El dominio especificado no existe". Para evitar problemas en esta situación, abra mmc.exe, agregue el ADSI Edit snap-in manualmente, realice las conexiones que sean apropiadas con las credenciales necesarias, y luego guarde el archivo de consola. Le da su propia consola predeterminada que funciona con ADSI Edit.

3. **Seleccione la plantilla de certificado de usuario**

En Adsiedit.msc los nodos siguientes deben modificarse para extender una plantilla de certificado:

CN=<nombre de plantilla>, CN=Plantillas de certificado, CN=Servicios de clave pública, CN=Servicios, CN=Configuración, DC=<nombre de dominio>.

4. **Modificar la plantilla de certificado de usuario**

Haga clic con el botón derecho sobre la entrada **CN=Usuario** y en menú que aparece haga clic sobre el elemento del menú **Propiedades**.

Seleccione la propiedad para ver: *pKIDefaultCSPs*.

Editar atributo:

Agregar el siguiente texto: *<n>,Infineon TPM Cryptographic Provider* (en donde *<n>* es el número posterior en la lista de **valores**).

Ejemplo: La lista de **valores** ya tiene dos elementos:

1,Microsoft Enhanced Cryptographic Provider v1.0

2,Microsoft Base Cryptographic Provider v1.0

Agregar el siguiente texto:

3,Infineon TPM Cryptographic Provider

Haga clic sobre **Agregar** y luego en **Aplicar** para almacenar el cambio de la plantilla de certificado.

La entidad certificada (CA por sus siglas en inglés) ahora está lista para comenzar la inscripción de usuarios para los certificados de Security Platform.

Nota: Si desea utilizar los [Cryptographic Service Providers](#) que se entregaron con la Solución Security Platform dentro de otras plantillas, los pasos que se requieren son similares a los que se describieron arriba para Active Directory.



La Solución Infineon Security Platform

Inscripción de certificados

Los certificados actúan como un mecanismo para obtener confianza en la relación entre una clave pública y la entidad que es dueña de la correspondiente clave privada. Un certificado es una declaración que está firmada digitalmente por el emisor, que garantiza que la clave pública dada pertenece al sujeto que tiene en posesión dicho certificado. Los certificados generalmente llevan información sobre la identidad de la entidad que tiene acceso a la clave privada correspondiente a la clave pública que se menciona en el certificado.

Un usuario asociado a uno de los [Cryptographic Service Providers](#) que se entregan con la Solución Security Platform se puede inscribir por medio de

- Certificar un Snap-In que se ejecuta en Microsoft Management Console o
- La aplicación Web provista por los sistemas operativos Microsoft Windows Server.



©Infineon

Technologies AG

La Solución Infineon Security Platform

Inscripción de certificados por medio de Microsoft Management Console

Este método se aplica sólo si la computadora local y la entidad certificada (CA por sus siglas en inglés) se encuentran dentro del mismo dominio de Windows.

1. Ejecute el Microsoft Management Console Certificates Snap-In
Ejecute de Microsoft Management Console y agregue el Certificate Snap-In para administrar los certificados para mi cuenta de usuario.
2. Llamar al asistente para la solicitud de certificado
Haga clic con el botón derecho sobre el medio de almacenamiento lógico **Personal** y ejecute el **Asistente para la solicitud de certificado** por medio de un clic sobre **Solicitar nuevo certificado....**
3. Procesar la solicitud de certificado
Haga clic sobre **Siguiente** para proceder.
4. Seleccione el tipo de certificado **Usuario** y tilde el elemento **Avanzado**. Se requiere para asociar el certificado a uno de los [Cryptographic Service Providers](#) que se entregan más tarde con la solución Security Platform.

Haga clic sobre **Siguiente** para proceder.

5. Seleccione uno de los Cryptographic Service Providers que se entregaron con la solución Security Platform para usar con el certificado solicitado. La longitud de la clave se establece automáticamente a la longitud de clave predeterminada del CSP.



Si los Cryptographic Service Providers que se entregaron con la solución Security Platform no aparece en la lista, asegúrese de que se modificó la plantilla de certificado de usuario.

Haga clic sobre **Siguiente** para proceder.

6. Seleccione la entidad certificada a la que desea enviar la solicitud.
Haga clic sobre **Siguiente** para proceder.

7. Ingrese un nombre y una descripción para el nuevo certificado.
Haga clic sobre **Siguiente** para proceder.
8. Complete la solicitud de certificado al hacer clic sobre **Terminar**.

Se muestra una confirmación que indica que la solicitud del certificado se realizó exitosamente.



©Infineon Technologies AG

La Solución Infineon Security Platform

Inscripción de certificados por medio de navegadores Web

Las secciones a continuación describen la inscripción de certificados utilizando el Microsoft CA estándar, como puede instalarse en los sistemas operativos servidores de Microsoft Windows (por ejemplo: Microsoft Windows Server 2003).

Las entidades certificadas (CA por sus siglas en inglés) públicas pueden utilizar diferentes interfaces Web.

1. **Ejecutar Internet Explorer** Ejecute su Internet Explorer y abra su página de inicio de la entidad certificada empresarial.
Seleccione **Solicitar un certificado** y haga clic sobre **Siguiente** para proceder.
2. **Procesar la solicitud de certificado**
Seleccione **Solicitud de certificado de usuario** y haga clic sobre **Siguiente** para proceder.



Si selecciona **Solicitud avanzada** su solicitud es más flexible y se pueden seleccionar o establecer una gran variedad de parámetros. Usualmente esta opción se debe utilizar para seleccionar uno de los [Cryptographic Service Providers](#) que se entregaron con la solución Security Platform.

Haga clic sobre **Más opciones** para permitir la asociación del Cryptographic Service Provider con el certificado que solicitó.

Si hace clic sobre **Enviar** los siguientes valores predeterminados se utilizan para la solicitud del certificado:

<i>CSP:</i>	<i>MS Base Cryptographic Provider V1</i>
<i>Longitud de clave:</i>	<i>Predeterminado de CSP</i>
<i>Protección fuerte de clave privada:</i>	<i>No</i>
<i>Nombre del contenedor:</i>	<i>Un GUID aleatorio</i>

El certificado se asocia al *MS Base Cryptographic Provider V1*.

Seleccione uno de los Cryptographic Service Providers que se entregaron

con la solución Security Platform para utilizar por el certificado solicitado. La longitud de la clave se establece automáticamente a la longitud predeterminada de clave del CSP y el nombre del contenedor es un GUID aleatorio.



Si los Cryptographic Service Providers que se entregaron con la solución Security Platform no aparece en la lista, asegúrese de que se modificó la plantilla de certificado de usuario.

Complete la solicitud del certificado haciendo clic sobre **Enviar**.

Se muestra una confirmación que indica que la solicitud del certificado se realizó exitosamente.

El certificado recibido se puede instalar en su sistema al hacer clic sobre **Instalar este certificado**.



©Infineon Technologies AG

Infineon Security Platform Solution

Infraestructura de clave pública (PKI) en PKCS #11

El estándar PKCS #11 define una interfaz común para la creación, utilización y administración de certificados y claves de cifrado. Cada implementación de esta interfaz ofrece una aproximación específica a la tecnología subyacente, ya que en el estándar PKCS #11 no se hace referencia alguna al identificador de cifrado que lleva a cabo la funcionalidad principal. Existen soluciones en el mercado que están basadas en software y en tarjetas inteligentes o en módulos criptográficos de hardware especializados. Cada biblioteca compatible con PKCS #11 implementa su propio modo para incluir estos dispositivos y utilizarlos para generar y gestionar datos relevantes para el cifrado.

Puesto que el estándar PKCS #11 define una interfaz independiente de la plataforma, existen diferentes soluciones de una gran variedad de fabricantes. Este estándar es compatible con muchas plataformas y sistemas operativos.

Las bibliotecas compatibles con PKCS #11 ofrecen su funcionalidad mediante una interfaz bien definida. En función del objetivo principal de la implementación, es posible que una biblioteca PKCS #11 sea compatible solamente con un subconjunto de la interfaz definida.

Para crear una PKI, las aplicaciones que utilizan un módulo PKCS #11 deben tener acceso a un almacén permanente que permite guardar los certificados y las claves privadas del usuario de forma segura y fiable. En el estándar PKCS #11 no se hace referencia alguna a este mecanismo de almacenamiento. Puesto que se trata de un mecanismo que se utiliza habitualmente, los servicios de directorio han resultado ser un modo útil de ofrecer la funcionalidad solicitada. Para acceder a estos servicios de directorio se suele utilizar el protocolo LDAP (Lightweight Directory Access Protocol).

Windows 2000 y Windows XP no contienen ninguna biblioteca PKCS #11 nativa; por lo tanto, esta característica debe agregarse mediante productos de otros fabricantes. El software Infineon Security Platform Solution incluye una biblioteca que implementa la interfaz PKCS #11, la cual utiliza Trusted Platform Module para realizar las operaciones de cifrado más delicadas, como la generación de claves.

En el mismo sistema se encuentran varias implementaciones independientes del estándar. Normalmente las aplicaciones que utilizan estas bibliotecas deben configurarse en un paso extra para acceder correctamente a los módulos respectivos.

No obstante, las aplicaciones basadas en PKCS #11 deben implementar todas las tareas administrativas necesarias para ofrecer los datos necesarios para gestionar la funcionalidad de PKCS #11.

Los programadores de aplicaciones pueden beneficiarse de toda la funcionalidad de los mecanismos de seguridad basados en clave pública mediante el uso de diferentes módulos de implementación PKCS #11, sin necesidad de modificar la plataforma ni el sistema del software en el que operan. Además, las empresas también podrán administrar su entorno y sus aplicaciones con herramientas y directivas utilizadas en toda la organización.

Para que los usuarios puedan leer los mensajes cifrados o verificar los mensajes de correo electrónico firmados, los certificados de usuario deben almacenarse en un directorio público. Este directorio suele encontrarse en un servidor al que se puede acceder desde la unidad de organización en cuestión.

Entre los componentes básicos de una infraestructura de clave pública están los certificados digitales, las listas de revocaciones de certificados y las entidades emisoras de certificados. Los administradores de la empresa deben asegurarse de que se dispone de una infraestructura de clave pública antes de que empiecen a utilizar el cifrado de claves públicas en las redes.

Para configurar una PKI dentro de una organización deben llevarse a cabo los pasos siguientes:

- Instalar un servidor de certificados
- Definir un proveedor de servicios de certificados de otro fabricante
- Configurar [Mozilla Firefox](#) para utilizar la biblioteca PKCS #11 de Infineon Security Platform
- Obtener certificados de una entidad emisora de certificados para la autenticación del cliente

En esta Guía para los primeros pasos se ofrece información general sobre algunos de los elementos mencionados anteriormente y se incluyen los vínculos que ofrecen más información sobre estos temas.



Tras la actualización del software de Security Platform Solution, es posible que las aplicaciones que utilizan Security Platform Solution a través de la interfaz PKCS#11 no funcionen como se espera porque el archivo PKCS#11 DLL (*ifxtpmck.dll*) ahora se encuentra en el directorio de instalación del software de Security Platform Solution. En anteriores versiones del producto se encontraba en el directorio *system32*. Deben

reconfigurarse las aplicaciones para cargar *ifxtpmck.dll* desde la nueva ubicación.



©Infineon

Technologies AG

Infineon Security Platform Solution

Configurar PKCS #11 para Mozilla Firefox

El estándar PKCS #11 define tecnologías e interfaces independientes de la plataforma para la gestión de los elementos relevantes para la seguridad para una PKI en un entorno distribuido. Existen varias soluciones de diferentes fabricantes. El software Infineon Security Platform Solution incluye una biblioteca PKCS #11 (de funciones de software) que implementa toda la funcionalidad necesaria para que Infineon Security Platform funcione. Esta biblioteca utiliza Trusted Platform Module para la mayoría de las operaciones importantes en cuanto a seguridad.

Mozilla Firefox se ha diseñado para admitir más de una biblioteca PKCS #11. El producto estándar incluye una solución basada completamente en mecanismos de software.

La biblioteca PKCS #11 contenida en el software Infineon Security Platform Solution debe configurarse una sola vez en Mozilla Firefox. Durante esta configuración, es posible deshabilitar la biblioteca PKCS #11 estándar si ya no es necesaria. Esta decisión debe tomarse de acuerdo con el administrador del sistema.

Configurar Mozilla Firefox

1. Inicie Mozilla Firefox.
2. Seleccione **Herramientas > Opciones...** . Se abre el panel de Opciones.
3. Haga clic en el ícono **Seguridad** en el panel de Opciones.
4. Tilde **Utilizar una contraseña maestra** para definir la contraseña que protegerá su base de datos de certificados.
5. Ingrese una **Nueva contraseña** dos veces para confirmar. Sólo cuando los valores ingresados son idénticos se habilita el botón Aceptar. El medidor de **calidad de la contraseña** le indica el nivel de seguridad del valor actualmente ingresado. Para tener el mismo nivel de seguridad para esta contraseña tal como se recomienda para las contraseñas del software de la solución Infineon Security Platform, se deben tener en cuenta ciertas pautas acerca de [dichas contraseñas](#). Si desea cambiar una contraseña ya establecida, también deberá ingresar la **contraseña actual**.
6. Haga clic en **Aceptar**.

La configuración de correos electrónicos se describe en la sección de [configuración de correo electrónico seguro](#).

Configure el manejo de certificados

Esta sección explica la configuración sobre cómo se manejan los certificados en Mozilla Firefox.

1. Haga clic en el ícono **Avanzado** en el panel de Opciones para configurar el entorno de manejo de certificados.
2. Haga clic en la lengüeta **Encriptación** . Para la **Selección de certificados** establezca el modo **Preguntar cada vez**. Así se asegura de que no se realizan autenticaciones de cliente sin conocimiento del usuario.
3. Haga clic en el botón **Dispositivos de seguridad** para abrir el Administrador de dispositivos.
4. Haga clic en el botón **Cargar** para abrir el diálogo de configuración del nuevo Módulo PKCS #11.
5. El **Nombre de módulo** es obligatorio; el **nombre de archivo del módulo** is fixed to *IfxTPMCK.dll*. Si el módulo no está ubicado en una carpeta dentro de la variable de RUTA del sistema, se puede utilizar el botón **Examinar** para ubicar el archivo. Confirme las configuraciones con **Aceptar**.
6. Si el nombre del módulo especificado se encuentra posteriormente enumerado en la lista de **Módulos criptográficos**, entonces está correctamente configurado para ser utilizado.

La Solución Infineon Security Platform

Inscripción de certificados

Los certificados actúan como un mecanismo para obtener confianza en la relación entre una clave pública y la entidad que es dueña de la correspondiente clave privada. Un certificado es una declaración que está firmada digitalmente por el emisor, que garantiza que la clave pública dada pertenece a la persona o entidad que tiene en posesión dicho certificado. Los certificados generalmente llevan información sobre la identidad de la persona o entidad que tiene acceso a la clave privada correspondiente a la clave pública que se menciona en el certificado.

Un usuario asociado a uno de los [Cryptographic Service Providers](#) que se entregan con la Solución Security Platform se puede inscribir por medio de

- [Sun Certificate Server](#) o
- [Entidades certificadas públicas con PKCS #11 soporte.](#)



©Infineon

Technologies AG

Infineon Security Platform Solution

Suscribir certificados con una CA basada en Sun Certificate Server

En las secciones siguientes se describe la suscripción de certificados mediante la entidad emisora de certificados de iPlanet. Este producto se encuentra disponible para diferentes plataformas (Windows 2000 o XP, Unix, Linux, etc.).

Para acceder a él debe utilizarse un explorador Web que sea compatible con el estándar PKCS #11.

Suscribir certificados con Mozilla Firefox

1. Asegúrese de que Mozilla Firefox esté instalado.
2. Inicie Mozilla Firefox.
3. Introduzca la dirección Web de su servidor de certificados. Póngase en contacto con el administrador del sistema si no conoce esta dirección. La comunicación utiliza un canal protegido por SSL en el puerto predefinido 1025, de modo que la dirección de su servidor de certificados será la siguiente: *https://nombre_del_servidor:1025*.
4. Una vez que se hayan visualizado algunos mensajes, el certificado ya puede suscribirse.
5. El certificado puede utilizarse para llevar a cabo la autenticación del cliente mediante la entidad emisora de certificados. El usuario puede definir el modo de autenticación.
 - Seleccione la opción para **aceptar este certificado para esta sesión** si tiene que utilizar un certificado nuevo para cada sesión.
 - Seleccione la opción para **no aceptar este certificado y no conectarse** si desea descartar el certificado.
 - Seleccione la opción para **aceptar siempre este certificado (hasta su caducidad)** si desea utilizar el certificado para la autenticación del cliente hasta que caduque.

Nota: puede encontrar información adicional acerca del nivel de seguridad de la comunicación en el servidor de la entidad emisora.

Para comprobar las propiedades de una entidad emisora de certificados, realice los pasos siguientes:

1. Haga clic en el ícono **Avanzado** desde **Herramientas > Opciones...** y haga clic en la lengüeta **Encriptación**.
2. Haga clic en **Visualizar certificados** para abrir el Administrador de certificados y haga clic en la lengüeta **Autoridades**.
3. Seleccione el modo de gestión de entidades emisoras que se adapte a sus necesidades o que haya sido definido por el administrador del sistema.
 - Seleccione la opción para **aceptar esta entidad emisora de**

certificados para la certificación de sitios de red si desea utilizar los certificados emitidos por la entidad emisora para la autenticación basada en Web.

- Seleccione la opción para **aceptar esta entidad emisora de certificados para la certificación de usuarios de correo electrónico** si desea aceptar certificados emitidos por la entidad emisora que se utilizan para firmar y/o cifrar mensajes de correo electrónico.
- Seleccione **Aceptar esta entidad emisora de certificados para la certificación de programadores de software** si desea utilizar certificados emitidos por esta entidad emisora para la gestión de software certificado.



La Solución Infineon Security Platform

Inscripción de certificados con una entidad certificada pública que permita PKCS #11

Las entidades certificadas públicas generalmente ofrecen un método basado en una interfaz Web para la inscripción de certificados.

La interfaz del usuario puede ser la misma, por ejemplo, La [Sun Certificate Server](#). La diferencia es la dirección del servicio. En general, las entidades certificadas públicas ofrecen un [servicio a gran escala](#) en cuanto a seguridad y aspectos del certificado.

El proveedor de servicios también puede ofrecer un software específico para descargar e instalar, el cual automatiza la comunicación y el manejo de solicitud de certificados.



©Infineon

Technologies AG

La Solución Infineon Security Platform

Introducción a su Personal Secure Drive

Su Personal Secure Drive (PSD) provee un área de almacenamiento protegida para los datos sensibles. Se puede establecer uno o más Personal Secure Drives con el [Asistente de inicialización del usuario](#).

Cuando establece un Personal Secure Drive, éste luce como cualquier otra unidad en su computadora: se pueden crear archivos y carpetas en su Personal Secure Drive y se puede acceder a ellos del mismo modo en que accede a archivos y carpetas en otras unidades. No hay límite en el tipo de archivos que se pueden guardar en el Personal Secure Drive.

El Personal Secure Drive difiere de las otras unidades de disco comunes en dos aspectos clave:

1. Los datos están cifrados.
2. Sólo usted puede ver y acceder a él.

La encriptación

Los datos en el Personal Secure Drive se protegen automáticamente por medio de técnicas criptográficas avanzadas que incluyen los algoritmos AES y RSA. Al guardar un archivo o carpeta en su Personal Secure Drive, se encripta automáticamente. Puede crear archivos y carpetas en su Personal Secure Drive, o moverlos de una unidad de disco común a su Personal Secure Drive. Los archivos se encriptan automáticamente al colocarlos en su Personal Secure Drive. De forma similar, si accede a los archivos o carpetas o los copia desde su Personal Secure Drive a una unidad de disco común, se desencriptan automáticamente. No necesita llevar a cabo ningún procedimiento especial para proteger sus archivos o carpetas; toda la encriptación y desencriptación se maneja automáticamente.



Cómo proteger los archivos y carpetas existentes: Mueva los archivos y carpetas existentes a su PSD para protegerlos. Si copia archivos y carpetas a su PSD sin borrarlos de su ubicación original, las copias desencriptadas permanecerán en la ubicación original.

Modo Servidor

En el [modo servidor](#), las configuraciones de PSD son administradas por el Trusted Computing Management Server. Esto significa que las configuraciones de PSD se migran automáticamente al igual que las demás credenciales y certificados (ver [Migración de claves a otros sistemas](#)).



El archivo de imagen de la unidad de PSD no se migra.

Se recomienda configurar el PSD en un medio extraíble (por ejemplo, memoria USB) que le permite llevar su archivo de imagen de la unidad PSD con usted.

Si decide configurar su PSD en un medio fijo (como su disco rígido local), y desea utilizarlo en otra plataforma, debe realizar una copia de seguridad de su archivo de imagen de la unidad PSD en la primera plataforma y restaurarla en la otra plataforma (ver [Copia de seguridad y restauración de los datos de Security Platform](#)). Observe que en este caso estará trabajando en copias físicas diferentes de su PSD.



©Infineon Technologies AG

La Solución Infineon Security Platform

Ventajas de la utilización de la Personal Secure Drive

Tanto si trabaja con información digital para su empresa como para su uso personal, los datos confidenciales deben estar completamente protegidos. La Personal Secure Drive ofrece la máxima protección porque puede almacenar todos los archivos que desee en una unidad virtual cifrada y creará un repositorio de alta seguridad para los datos confidenciales. Algunas de sus ventajas son:

- Cifrado de unidades virtuales mediante una clave AES (estándar de cifrado avanzado) almacenada de forma segura.
- Codificación de la clave de cifrado mediante el algoritmo RSA.
- Seguridad transparente: cifrado/descifrado automático de los datos.
- Procesamiento de archivos incluso mayores sin demora apreciable, porque el cifrado y el descifrado se efectúan al instante.

Protección de archivos más fácil

La Personal Secure Drive se ha diseñado para proporcionar una interfaz de usuario simple e intuitiva, lo cual le permitirá centrarse en la tarea que tiene entre manos, en lugar de centrarse en procesos de seguridad extensos. La Personal Secure Drive ofrece lo siguiente:

- Facilidad de uso: la Personal Secure Drive tiene el mismo comportamiento que cualquier unidad normal de Windows.
- Interfaz basada en el Asistente para facilitar la administración y la configuración.
- Integración con Microsoft EFS (sistema de archivos cifrados).

Garantía máxima con Trusted Platform Module

La Personal Secure Drive se basa en la más reciente iniciativa de Trusted Computing: el módulo Trusted Platform Module (TPM). La Personal Secure Drive usa Trusted Platform Module como parte principal del proceso de cifrado de archivos, lo cual garantiza la protección de los datos frente a personal no autorizado y su "bloqueo" para el PC en el que se han cifrado. Trusted Platform Module proporciona la seguridad de hardware para sus datos, superando todos los esquemas de protección basados en software de que se dispone actualmente.

Beneficios de la Personal Secure Drive

- Permite almacenar los datos de forma segura en el PC local.
- Protección de datos usando Trusted Platform Module (TPM), que ofrece una seguridad basada en hardware.
- Interfaz intuitiva fácil de usar.
- Plena integración en el entorno Windows; la Personal Secure Drive tiene el mismo comportamiento que cualquier otra unidad local.
- Cifrado/descifrado automático de los datos para usuarios autorizados; el usuario final no debe realizar pasos adicionales para proteger los datos.
- Rutinas de cifrado y descifrado sumamente eficientes; sin pérdida de productividad ni de rendimiento para el usuario final.



©Infineon

Technologies AG

La Solución Infineon Security Platform - Carga y descarga del PSD

Carga y descarga de su Personal Secure Drives

Si desea restringir el acceso a sus datos encriptados puede explícitamente cargar (montar) y descargar (desmontar) su Personal Secure Drive.

Antes de acceder a su PSD necesita cargarlo. La carga de PSD requiere de su autorización. Una vez que su PSD se ha cargado, puede acceder a sus datos encriptados hasta que descargue su PSD explícitamente, cierre o apague su computadora.

Cómo cargar su PSD

Cargue su PSD desde el [Icono de Notificación de la Barra de tareas](#), opción **Personal Secure Drive - Cargar** (si ha establecido más de un Personal Secure Drive) o **Personal Secure Drive - <LetraUnidad.Etiquetaunidad> - Cargar** (si ha establecido más de un Personal Secure Drive).

Luego de superada la autenticación, Windows Explorer se inicia mostrando su PSD.

Carga automática de PSD al inicio de sesión

Puede establecer si desea cargar su PSD automáticamente al iniciar sesión en Windows.

Establezca esta opción por medio del [Icono de Notificación de la Barra de tareas](#), opción **Personal Secure Drive - Cargar al iniciar sesión** (si ha establecido más de un Personal Secure Drive) o **Personal Secure Drive - <LetraUnidad.Etiquetaunidad> - Cargar** (si ha establecido más de un Personal Secure Drive). Si se establece esta opción aparece una tilde junto a **Cargar al iniciar sesión**.

Cómo descargar su PSD

Descargue su PSD desde el [Icono de Notificación de la Barra de tareas](#), opción **Personal Secure Drive - Descargar**. (si ha establecido más de un Personal Secure Drive) o **Personal Secure Drive - <LetraUnidad.Etiquetaunidad> - Descargar** (si ha establecido más de un Personal Secure Drives).

Cuadro de diálogo para carga de PSD

Si va a cargar su PSD, aparece el [cuadro de diálogo de autenticación](#) para el uso de las funciones de Security Platform.

Cuadro de diálogo para la descarga de PSD

Si su PSD va a ser descargado, aparece en pantalla un diálogo que muestra el estado de todos los Personal Secure Drives actualmente cargados. Si continua y una PSD a ser descargada tiene archivos abiertos, entonces aparecerá en pantalla un mensaje de advertencia.

Elementos del cuadro de diálogo de descarga de PSD	Explicación
<input type="checkbox"/> <i>Personal Secure Drives</i>	Aquí puede ver el estado de todos los Personal Secure Drives actualmente cargados. Verifique todas las unidades que desea descargar. Asegúrese de que ninguna de las unidades a descargar esté en uso. Se puede actualizar esta lista por medio de la tecla "F5".
<input checked="" type="checkbox"/> <i>Cierre este cuadro de diálogo luego de una descarga exitosa.</i>	Tilde esta casilla de verificación si quiere que el Diálogo para descargar PSD se cierre automáticamente después de haber descargado los Personal Secure Drives seleccionados. Si falla la descarga de PSD, entonces el cuadro de diálogo permanece y muestra un estado de falla.
<input type="checkbox"/> <i>Descargar</i>	Haga clic en Descargar para continuar.
<input type="checkbox"/> <i>Cerrar</i>	Haga clic sobre este botón para cerrar el cuadro de diálogo de descarga de PSD sin descargarlo.



La Solución Infineon Security Platform

Administración de Personal Secure Drive

Este tema cubre los problemas de administración asociados con el Personal Secure Drive.

Política

Las políticas de Personal Secure Drive se incluyen en la [Administración de políticas de Infineon Security Platform](#).

Mapeo de letras de unidad para el Personal Secure Drive

Durante la configuración del Personal Secure Drive, se le pide que elija una letra de unidad de la lista de letras disponibles. La lista excluye las letras de unidad que se encuentran en uso actualmente como así también las letras que se asignaron previamente a dispositivos intercambiables o a unidades removibles. Esto evita posibles conflictos con las letras de unidad.

Además, siete letras sin asignar están marcadas como "no recomendadas" porque se las reserva para ser usadas en el futuro por dispositivos intercambiables en caliente que todavía no han sido cargados. Esto evita posibles conflictos entre letras de unidad con dispositivos intercambiables adicionales.

El número de letras de unidad que se reservan para uso futuro de los dispositivos intercambiables se establece en la clave del registro de Windows `HKEY_LOCAL_MACHINE\Software\Infineon\TPM Software\PSD\DLskip`. Para aumentar o disminuir el número de letras de unidad reservadas, puede editar el valor de esta clave.

Nota: El valor por defecto para esta clave de registro es 7; el valor máximo permitido es 9. Si la clave del registro se establece en un valor mayor a éste, se vuelve a configurar en 9.



©Infineon

Technologies AG

Solución Infineon Security Platform

Recuperación de Personal Secure Drive

Con la recuperación de Personal Secure Drive puede recuperar sus datos del PSD en caso de que se pierdan sus credenciales. La recuperación de datos se habilita a través del uso de agentes de recuperación. El agente de recuperación es un [rol de usuario](#) para la desencriptación de otros datos del usuario. Si el usuario actualiza el sistema desde un Home edition a un sistema operativo superior, por ejemplo Windows XP Home a Windows XP Professional o Windows Vista Basic Home a Windows Vista Home Premium, los agentes de recuperación de Home se invalidan y el usuario necesita volver a configurar la recuperación del PSD según lo especificado en la tabla "Cómo configurar y realizar una recuperación del PSD".



Precondiciones de recuperación de PSD:

- Se lista al menos un agente de recuperación de PSD.
- Su archivo imagen de PSD es accesible.

Observe que un archivo imagen de PSD perdido o algún dato de usuario dentro de un archivo imagen se puede restaurar sólo desde un archivo [Copia de seguridad imagen de PSD](#).

Cómo configurar y realizar una recuperación de PSD

Tareas de recuperación PSD	Ediciones de Windows que no admiten EFS	Ediciones de Windows que admiten EFS
Introducción	<ul style="list-style-type: none">• Se utilizan agentes dedicados a la recuperación de PSD. Los usuarios de PSD necesitan registrar un agente de recuperación PSD.• Todas las tareas se realizan por medio de la herramienta de línea de comandos de recuperación de PSD.	<ul style="list-style-type: none">• Se utilizan agentes de recuperación de EFS.• Un administrador administra los agentes de recuperación por medio de configuración de Microsoft Security.• La recuperación de PSD se realiza por medio de la herramienta de línea de comandos de recuperación de PSD.
Cómo configurar los agentes de recuperación:		
Habilitar la recuperación de PSD	<ol style="list-style-type: none">1. Configurar PSD2. Crear un archivo de	<ol style="list-style-type: none">1. Configurar PSD

	<p>certificado de recuperación y un archivo PKCS #12 de recuperación. Se le solicitará que establezca una contraseña para proteger el archivo PKCS #12. Línea de comando: PSDRecovery /R:nombredearchivo</p> <p>3. Registrar el agente de recuperación de PSD: Línea de comando: PSDRecovery /A:nombredearchivo.CER [/ID:driveID]</p> <p>Nota: También puede realizar el paso 2 primero, y luego el paso 1.</p>	<p>2. Configurar los agentes de recuperación EFS por medio de la configuración de Microsoft Security: Línea de comando: secpol.msc</p> <p>3. Cargue su PSD para que los cambios sean efectivos.</p> <p>Notas: También puede realizar el paso 2 primero, y luego el paso 1. Es este caso el paso 3 ya no es necesario. Windows 2000 EFS crea un agente de recuperación por defecto; Windows 7, Windows Vista y Windows XP Professional no.</p>
<p>Ver la lista de agentes de recuperación registrados</p>	<p>Muestra la lista de los agentes de recuperación registrados por su PSD. Línea de comando:</p>	<p>Ver los agentes de recuperación EFS por medio de la configuración</p>

	PSDRecovery /V [/ID:driveID]	de Microsoft Security: Línea de comando: secpol.msc	
Borrar un agente de recuperación registrado	Borrar un agente de recuperación especificado, registrado por su PSD. Línea de comando: PSDRecovery /D: [nombre][número] [/ID:driveID]	Borrar los agentes de recuperación EFS por medio de la configuración de Microsoft Security: Línea de comando: secpol.msc	
Cómo recuperar su PSD:	<ul style="list-style-type: none"> • Asegúrese de que tiene acceso al certificado digital del agente de recuperación y a la clave privada asociada (por ejemplo necesita importar el archivo PKCS #12 de recuperación). • Asegúrese de que está instalada la aplicación Personal Secure Drive. • Asegúrese de que los datos encriptados de Personal Secure Drive a recuperar son accesibles para el agente de recuperación. 		
Localizar el archivo imagen de PSD	Los datos encriptados para el Personal Secure Drive están localizados dentro de un solo archivo (archivo con extensión * .FSF). Observe que los archivos * .FSF son archivos de sistema ocultos y normalmente son accesibles sólo para los usuarios con derechos de administración. La localización de este archivo se puede	Recuperar los datos de PSD	Rec PSI unic Va a date y cu hern recu De visu

obtener por medio de la herramienta de la línea de comandos de recuperación de PSD:
PSDRecovery /L

cop
loca
Líne
PSI
/M:
[X:]

Sintáxis de la herramienta de línea de comandos de recuperación de PSD

PSDRecovery.exe es una herramienta de la línea de comandos similar al EFS cipher.exe.



Observe que la sintáxis no diferencia entre minúsculas y mayúsculas.

PSDRecovery /A:nombreadearchivo.CER [/ID:driveID]

Admitido sólo en ediciones de Windows que no son compatibles con EFS.

Registre un agente de recuperación agregando a la lista de agentes de recuperación del Personal Secure Drive el certificado del archivo *CER específico.

nombreadearchivo.CER	Un nombre de archivo con extensión .CER [/ID:driveID]
----------------------	--

/ID:driveID	Opcional: Realiza la acción especificada solamente para el Personal Secure Drive con el driveID dado.
-------------	---

PSDRecovery /D:name [/ID:driveID]

PSDRecovery /D:number [/ID:driveID]

Disponible sólo en ediciones de Windows Home.

Borra de la lista de agentes de recuperación de PSD el agente especificado. Se debe especificar el nombre o el número secuencial (que se muestra por PSDRecovery /V).

nombre	El nombre del agente de recuperación como se muestra en PSDRecovery /V
--------	--

número	El número secuencial del agente de recuperación como se muestra en PSDRecovery /V
--------	---

Sin el parámetro /ID , esta acción se realiza para todos los Personal Secure Drives.

PSDRecovery /L

Enumera ID, archivo imagen y ruta del archivo imagen para todos los Personal Secure Drives.

PSDRecovery /M:DriveImageFile.FSF [X:]

Recupera sus datos de PSD a una nueva unidad temporal.

DriveImageFile.FSF	Ruta completa del archivo imagen de PSD como se muestra en PSDRecovery /L
--------------------	---

X	Letra de unidad lógica a asignar para la nueva unidad temporal, la cual contendrá los datos recuperados (opcional). Si no se da ninguna letra de unidad, se utiliza la primera letra disponible.
---	--

PSDRecovery /R:nombredearchivo

Admitido sólo en ediciones de Windows Home.

Genera una clave y un certificado de agente de recuperación de PSD, luego los escribe en un archivo *PFX (que contiene la clave privada y el certificado) y el archivo *CER (que contiene sólo el certificado).

nombredearchivo	Un nombre de archivo (opcionalmente se puede incluir la ruta completa) sin extensiones. Si se especifica la ruta completa, entonces los archivos de salida se escriben en el directorio especificado. De otra manera, los archivos se escriben en el directorio actual.
-----------------	--

PSDRecovery /V [/ID:driveID]

Admitido sólo en ediciones de Windows.

Muestra la lista de agentes de recuperación de PSD registrados. Para cada agente de recuperación se muestran los siguientes parámetros: Un número secuencial, el nombre del agente de recuperación y el valor hash del certificado.

Sin el parámetro /ID , esta acción se realiza para todos los Personal Secure Drives.



Solución Infineon Security Platform

Sistema de archivos de encriptación

La función de sistema de archivos de cifrado (EFS) forma parte de la tecnología de seguridad de los volúmenes de sistemas de archivos NTFS. La integración es total y basta con realizar un paso de configuración una única vez. El EFS garantiza la seguridad de sus documentos frente a intrusos que puedan acceder físicamente a los datos confidenciales que tiene almacenados (por ejemplo, si le roban el equipo portátil). En este paso inicial, se marca como cifrado un volumen o una carpeta. Por consiguiente, se cifrarán todos los archivos y subcarpetas del volumen o la carpeta que ha seleccionado.

Las operaciones con carpetas o volúmenes cifrados son muy parecidas a las operaciones con carpetas o volúmenes no cifrados; el cifrado es totalmente transparente para el usuario al que se ha permitido el acceso.

Nota:

- Se recomienda utilizar el cifrado en el nivel de carpeta o de volumen, no en el nivel de archivo. Para una mayor simplicidad, sólo se describirán estos elementos.
- EFS no se admite en ediciones de Windows Home.



©Infineon

Technologies AG

Solución Infineon Security Platform

Características del sistema de archivos cifrados (EFS)

La información siguiente es un extracto del tema de Ayuda de Microsoft original relativo al EFS. Encontrará información completa en la página de ayuda de Microsoft. Para obtener la información necesaria en la Ayuda de Microsoft, minimice todas las ventanas abiertas para visualizar el entorno de escritorio de Windows. Después pulse F1 y busque la palabra clave apropiada.

- Los usuarios pueden cifrar sus archivos al almacenarlos en el disco. El proceso de cifrado es sencillo: basta con seleccionar una casilla de verificación en el cuadro de diálogo de propiedades del archivo.
- Asimismo, el acceso a los archivos cifrados es rápido y fácil. Los usuarios ven sus datos en forma de texto sin formato cuando acceden a los datos del disco.
- El cifrado de datos se efectúa de forma automática y es completamente transparente para el usuario.
- Los usuarios pueden descifrar un archivo anulando la selección de la casilla de verificación de cifrado en el cuadro de diálogo de propiedades del archivo.
- Los administradores pueden recuperar datos que han sido cifrados por otro usuario. Esto permite acceder a los datos aunque el usuario que los ha cifrado ya no esté disponible o haya olvidado su clave privada.
- El EFS sólo cifra datos cuando éstos están almacenados en el disco. Para cifrar datos mientras se transportan por una red TCP/IP, existen dos características disponibles: seguridad de protocolo de Internet (IPSec) y cifrado de protocolo de túnel punto a punto (PPTP).

Nota: EFS no se admite en ediciones de Windows Home.



©Infineon

Technologies AG

Solución Infineon Security Platform

Trabajar con el Encrypting File System

Es necesario tener en cuenta algunos temas al trabajar con el sistema de archivos cifrados (EFS). Algunos de ellos interesan únicamente a los administradores del sistema, ya que resultan importantes para la configuración del sistema EFS.

Consideraciones sobre la administración

- Sólo pueden cifrarse los archivos y las carpetas de los volúmenes NTFS. Por lo general, no se trata de una restricción real, puesto que es muy recomendable utilizar el sistema de archivos NTFS como sistema de archivos estándar al trabajar con Windows 2000 o XP. Un número considerable de características no relacionadas con la solución de seguridad también se basa en NTFS.
- Los volúmenes FAT siempre rompen el cifrado. Cuando un archivo cifrado se almacena en un volumen FAT, se elimina la protección. Esto se aplica especialmente a los disquetes, los cuales suelen utilizarse para la transferencia de archivos de tamaño reducido. Pero los casos de discos duros con varias particiones también pueden resultar problemáticos si una de las particiones es un volumen FAT que se utiliza para el almacenamiento de archivos (aunque se utilice únicamente para el almacenamiento temporal).
- Los archivos de sistema y los archivos comprimidos no pueden cifrarse. La carpeta de instalación de Windows, así como algunos archivos de la carpeta raíz de la partición de inicio, no pueden protegerse mediante el mecanismo del sistema de archivos cifrados (EFS). Esto no significa en absoluto que se rompa la seguridad, ya que el mismo sistema operativo protege los archivos principales del sistema con mecanismos especiales que no pueden desactivarse. Para obtener información adicional sobre este tema, consulte las [preguntas más frecuentes](#).
- Asimismo, los archivos temporales resultan de interés para los posibles intrusos. Para evitar brechas en la estructura de seguridad de los datos, también deben cifrarse las carpetas y los archivos temporales. La mayoría de las aplicaciones utilizan las carpetas estándar para el almacenamiento de archivos temporales. Al cifrar estas carpetas, se amplía el nivel de seguridad de un sistema de forma considerable. No es recomendable utilizar una carpeta temporal común para todos los usuarios, ya que esto supondría llevar a cabo operaciones administrativas adicionales.

Consideraciones sobre el uso

Los usuarios que trabajan con archivos y carpetas cifrados deben tener en mente la información y las recomendaciones siguientes.

- El cifrado es fácil de configurar. Puede encontrar información más detallada en la ayuda Microsoft EFS Help.
- Un archivo cifrado sólo puede abrirlo el usuario que lo ha cifrado. Para permitir el acceso a otros usuarios debe utilizarse un proceso manual archivo por archivo.
- Los usuarios deben utilizar el procedimiento de copiar y pegar para mantener el cifrado de los archivos que se mueven a una carpeta cifrada. Si utilizan el procedimiento consistente en arrastrar y colocar para mover los archivos, éstos no se cifrarán de forma automática en la nueva carpeta.
- Para utilizar el sistema EFS en equipos remotos, esta funcionalidad debe configurarse manualmente en dichos equipos.
- Los usuarios deben cifrar la carpeta **Mis documentos** en el caso de que guarden la mayoría de sus documentos en esta ubicación. De este modo, se garantiza que los documentos personales de estos usuarios se cifren de forma predeterminada.

Los temas que aparecen en la lista constituyen un resumen del modo en que se trabaja con el sistema EFS. Puede encontrar información más detallada en la ayuda Microsoft EFS Help. Para obtener la información necesaria en la Ayuda de Microsoft, minimice todas las ventanas abiertas para visualizar el entorno de escritorio de Windows. Después pulse F1 y busque la palabra clave apropiada.

Algunos aspectos técnicos de EFS se tratan en la [solución de problemas](#).

Nota: EFS no se admite en ediciones de Windows Home.



©Infineon Technologies AG

La solución Infineon Security Platform

Correo electrónico seguro

El correo electrónico seguro es una de las aplicaciones más utilizadas que utilizan claves públicas, ya que permite a los usuarios compartir información de manera confidencial y confiar en que se preservará la autenticidad de la información durante la transferencia. Esto se consigue mediante el cifrado de correo electrónico específico del usuario y/o la firma para impedir que personas no autorizadas lean o modifiquen los mensajes de correo electrónico. El uso de esta característica garantiza que sólo el autor del mensaje de correo electrónico y los destinatarios especificados puedan descifrar y leer el mensaje o validar la identidad del remitente.

Este documento proporciona una introducción para la utilización de [certificados digitales](#) y ofrece instrucciones detalladas para la configuración de [Microsoft Windows Mail/Outlook](#) y [Mozilla Thunderbird](#).



©Infineon

Technologies AG

La solución Infineon Security Platform

Correo electrónico seguro con Windows Mail/Outlook Express/Outlook

En esta sección se describe la configuración de Windows Mail/Outlook Express/Outlook para un correo electrónico seguro y el modo en que se puede utilizar el [certificado digital](#) para enviar mensajes de correo electrónico firmados digitalmente y mensajes de correo electrónico cifrados:

- [Configurar el correo electrónico seguro](#)
- [Envío de mensajes firmados digitalmente](#)
- [Envío de mensajes encriptados](#)

Technologies AG



La solución Infineon Security Platform

Configurar el correo electrónico seguro

Asegúrese de tener instalado Windows Mail/Outlook Express/Outlook y de que ya lo tiene configurado para el envío y recepción de correo electrónico por medio de su servidor de correo. Además, se requiere la presencia de al menos un certificado digital antes de poder proceder con las instrucciones a continuación.

Nota: Si todavía no dispone de un certificado que pueda utilizarse para el correo electrónico seguro, obténgalo antes de continuar con los pasos de configuración enunciados a continuación.

⊕ **Windows Mail/Outlook Express**

⊕ **Outlook 2007**

⊕ **Outlook 2003**

⊕ **Outlook XP**

⊕ **Outlook 2000**



©Infineon Technologies AG

La solución Infineon Security Platform

Envío de mensajes firmados digitalmente

⊕ **Windows Mail/Outlook Express**

⊕ **Outlook 2007**

⊕ **Outlook 2003**

⊕ **Outlook XP**

⊕ **Outlook 2000**



©Infineon Technologies AG

La solución Infineon Security Platform

Envío de mensajes encriptados

Para enviar un mensaje cifrado a una persona, necesitará una copia de su clave de cifrado pública o su certificado de cifrado (el certificado contiene una copia de la clave pública). Antes de realizar los pasos descritos a continuación, asegúrese de que ha obtenido el certificado de clave pública del destinatario y de que el destinatario figura en su lista de contactos:

☒ **Windows Mail/Outlook Express**

☒ **Outlook 2007**

☒ **Outlook 2003**

☒ **Outlook XP**

☒ **Outlook 2000**

No es necesario que introduzca la clave privada para enviar mensajes de correo electrónico cifrado, ya que el cifrado se efectúa mediante la clave pública del destinatario. Sin embargo, sí que necesitará la clave privada para leer un mensaje de correo electrónico cifrado, ya que para descifrarlo es preciso que la clave privada coincida con la clave pública utilizada para cifrar el mensaje.



La solución Infineon Security Platform

Correo electrónico seguro con Mozilla Thunderbird

En esta sección se describe la configuración de Mozilla Thunderbird Mail para un correo electrónico seguro y el modo en que se puede utilizar el [certificado digital](#) para enviar mensajes de correo electrónico firmados digitalmente y mensajes de correo electrónico cifrados:

- [Configurar el correo electrónico seguro](#)
- [Envío de mensajes firmados digitalmente](#)
- [Envío de mensajes encriptados](#)



©Infineon

Technologies AG

La solución Infineon Security Platform

Configurar el correo electrónico seguro

Asegúrese de que tenga instalado Mozilla Thunderbird y de que esté configurado para enviar y recibir mensajes de correo electrónico a través de su servidor de correo electrónico. Asimismo, debe disponer de al menos un certificado digital para realizar las instrucciones siguientes.

Nota: Si todavía no dispone de un certificado que pueda utilizarse para un correo electrónico seguro, obtenga uno antes de proseguir con los pasos de configuración que se describen a continuación.

Mozilla Thunderbird

1. Inicie Mozilla Thunderbird.
2. Haga clic en **Herramientas > Configuraciones de cuenta...** para abrir el panel de Configuraciones de cuenta.
3. Haga clic en **Seguridad** en el panel izquierdo bajo el nombre de cuenta.
4. Haga clic en el botón **Seleccionar...** de la sección **Firma digital** para definir el certificado que debe utilizarse para la firma del correo electrónico. Aparece una lista que contiene todos los certificados disponibles. Seleccione un certificado y establezca la firma mediante la opción **Firmar mensajes digitalmente (de forma predeterminada)**.
5. En la sección **Cifrado** puede configurar el comportamiento de cifrado predeterminado.
 - A. Seleccione **Nunca (no utilizar cifrado)** si desea definir el comportamiento de cifrado sólo cuando lo solicite.
 - B. Seleccione **Requerido (no se puede enviar el mensaje a menos que los destinatarios dispongan de certificados)** para que se cifre todo su correo electrónico de forma automática.

La configuración de PKCS #11 está descrita en la sección [Configuración de PKCS #11 para Mozilla Firefox](#).



©Infineon

Technologies AG

La solución Infineon Security Platform

Envío de mensajes firmados digitalmente Mozilla Thunderbird

1. Inicie Mozilla Thunderbird.
2. Haga clic en **Escribir** en la barra de íconos o **Archivo > Nuevo > Mensaje** para obtener una plantilla de mensaje en blanco.
3. Inserte la dirección del destinatario o selecciónela en una lista mediante el botón **Para**.
4. Si desea agregar datos adjuntos, haga clic en el icono **Adjuntar** de la barra de iconos para que se abra un diálogo de selección de archivos.
5. Agregue el texto al campo **Asunto** y al **cuerpo** del mensaje.
6. Haga clic en el pequeño **botón de flecha que se encuentra en el icono Seguridad** o seleccione **Opciones > Seguridad** para que aparezca el menú de configuración de seguridad. Seleccione **Firmar digitalmente este mensaje** para firmar el mensaje de correo electrónico. Está representada por un símbolo representativo en el lado derecho de la barra de estado.



©Infineon

Technologies AG

La solución Infineon Security Platform

Enviar mensajes cifrados mediante Mozilla Thunderbird

1. Inicie Mozilla Thunderbird.
2. Haga clic en Escribir en la barra de íconos o **Archivo > Nuevo > Mensaje** para obtener una plantilla de mensaje en blanco.
3. Inserte la dirección del destinatario o selecciónela en una lista mediante el botón **Para**.
4. Si desea agregar datos adjuntos, haga clic en el icono **Adjuntar** de la barra de iconos para que se abra un diálogo de selección de archivos.
5. Agregue el texto al campo **Asunto** y al **cuerpo** del mensaje.
6. Haga clic en el pequeño **botón de flecha que se encuentra en el icono Seguridad** o seleccione **Opciones > Seguridad** para que aparezca el menú de configuración de seguridad. Seleccione **Firmar digitalmente este mensaje** para firmar el mensaje de correo electrónico. Está representada por un símbolo representativo en el lado derecho de la barra de estado.



©Infineon

Technologies AG

Infineon Security Platform Solution

Macros firmadas en Microsoft Word

Microsoft Word admite niveles de seguridad que permiten a los usuarios ejecutar macros en función de si éstas están firmadas digitalmente o no por un programador de macros que figura en la lista de fuentes de confianza de un usuario. Un sello digital de identificación en una macro confirma que ésta procede del programador que la ha firmado y que no ha sufrido ninguna modificación, lo que garantiza que la macro es auténtica y que no contiene ningún virus.

El mecanismo de firma de macros se admite en Microsoft Word 2000 y en Microsoft Word XP.



Technologies AG

La Solución Infineon Security Platform

Configurar Microsoft Word para firmar macros

Para utilizar macros firmadas, se debe configurar primero a Microsoft Word. Solo luego de esta configuración, esta función de seguridad está disponible.

Microsoft Word ofrece **tres niveles de seguridad** para permitirle reducir la posibilidad de que macro-virus infecten sus documentos, plantillas o add-ins. Si su administrador de sistemas no ha impuesto un nivel de seguridad para su organización, lo puede cambiar usted mismo en cualquier momento. Si el nivel de seguridad para Microsoft Word está en Medio o Alto, puede mantener una lista de fuentes de macros confiable. Al abrir un documento o cargar un add-in que contiene macros desarrolladas por cualquiera de dichas fuentes, las macros se habilitan automáticamente.



©Infineon

Technologies AG

Infineon Security Platform Solution

Firmar digitalmente un proyecto de macro en Microsoft Word

Niveles de seguridad

1. Haga clic en **Herramientas** > **Macro** > **Seguridad...** para abrir el cuadro de diálogo Seguridad..
2. Elija el nivel de seguridad que necesite: Alto, Medio o Bajo.

Grabar una macro nueva

1. Abra un documento nuevo haciendo clic en **Nuevo documento en blanco**.
2. Clic en **Herramientas > Macros > Registrar macro nuevo...** (Nota en **Microsoft Word 2007**: Haga clic en **Visualizar > Macros > Registrar macro nuevo...**).
3. Aparece el diálogo **Grabar macro**.
4. Introduzca el nombre de la macro y haga clic en el botón **Aceptar** para cerrar el diálogo.
5. Escriba el texto de la macro.
6. Haga clic en **Detener grabación**.

Firma de un (nuevo) Macro en Microsoft Word 2007

1. Abra el documento o plantilla que contiene el proyecto de macros que desea firmar, si es que el archivo no se encuentra abierto.
2. Haga clic en **Visualizar > Visualizar macros;** , aparece el diálogo **Macros**.
3. Seleccione un **nombre de Macro** de la lista. Se puede ejecutar, editar, crear o borrar un macro.
4. Haga clic en el botón **Editar** para abrir una ventana de **Visual Basic**. Ahora edite el macro seleccionado.
5. Vaya al **Explorador de proyectos** para seleccionar el proyecto que desea firmar.
6. Haga clic en **Herramienta > Firma digit...** en la ventana de Visual Basic para abrir el diálogo de **Firma digital**.
7. Haga clic en **Elegir...** para abrir el diálogo **Seleccionar certificado**.
8. Seleccione un certificado adecuado desde la lista.
9. Haga clic en **Visualizar certificado** o para ver la información del certificado en el diálogo **Certificado**.
Nota: Haga clic en la lengüeta **Detalles** tab para visualizar la información del **certificado** en el diálogo. Haga clic en el botón **Aceptar** para cerrar este diálogo.
10. Haga clic en el botón **Aceptar** para cerrar el diálogo **Seleccionar certificado**.
11. Cierre el diálogo **Firma digital** haciendo clic en el botón **Aceptar**.
12. Para guardar su macro haga clic en **Guardar** y guarde el documento o plantilla como un **Documento habilitado con macros de Word**.
Nota: Debido a que **Microsoft Word** usa clave privada para firmar su macro, se debe insertar el secreto de la clave privada.
13. Haga clic en **Archivo > Cerrar** to para regresar a Microsoft Word.

Firmar una macro (nueva)

1. Abra el documento o la plantilla que contiene el proyecto de macro que desea firmar, en caso de que el archivo no esté abierto.
2. Haga clic en **Herramientas > Macro > Macros**, y aparecerá el diálogo **Macros**.
3. Seleccione un **nombre de macro** de la lista. Puede ejecutar, modificar, crear o eliminar una macro.
4. Haga clic en el botón **Modificar** para abrir una ventana de **Visual Basic**. Ahora modifique la macro que ha seleccionado.

Nota: también puede abrir la ventana **Visual Basic** haciendo clic en **Herramientas > Macro > Editor de Visual Basic**.

5. Vaya al **explorador de proyectos** para seleccionar el proyecto que desee firmar.
6. Haga clic en **Herramientas > Firma digital...** en la ventana de Visual Basic para abrir el diálogo **Firma digital**.
7. Haga clic en **Elegir** para abrir el diálogo **Seleccionar certificado**.
8. Seleccione un certificado adecuado de la lista.
9. Haga clic en **Ver certificado** para ver la información del certificado en el diálogo **Certificado**.

Nota: haga clic en **Detalle...** para ver la información del certificado en el diálogo **Certificado**. Haga clic en el botón **Aceptar** para cerrar el diálogo.

10. Haga clic en el botón **Aceptar** para cerrar el diálogo.
11. Cierre el cuadro de diálogo **Seleccionar certificado** haciendo clic en el botón **Aceptar**.
12. Cierre el diálogo **Firma digital** haciendo clic en el botón **Aceptar**.
13. Para guardar la macro, haga clic en **Guardar normal**.

Nota: puede guardar la macro en la carpeta de proyecto **Normal (Todos los documentos Normal.dot)** o en la carpeta de proyecto **Documento**.

Puesto que **Microsoft Word** utiliza su clave privada para firmar la macro, debe insertar su clave privada secreta.

14. Haga clic en **Archivo > Cerrar** para regresar a Microsoft Word.



©Infineon Technologies AG

La Solución Infineon Security Platform

Conexiones seguras de red

Con la Solución Security Platform puede asegurar sus conexiones de red. Si utiliza los servicios de integración de Security Platform (por ejemplo, el Cryptographic Service Providers para Microsoft Crypto-API y PKCS #11 Crypto-API), luego sus claves privadas de certificado serán protegidas por medio del Trusted Platform Module.

Se soportan los siguientes tipos de redes:

- [Explorador para la Web/conexión con el servidor \(Autenticación de cliente\)](#)
- [Red privada virtual \(VPN por sus siglas en inglés\)](#)
- [Red de área local inalámbrica \(WLAN por sus siglas en inglés\) o LAN alámbrica](#)

Puede utilizar certificados de usuario para autenticarse usted mismo, y certificados de computadora para autenticar su computadora.

Las siguientes tablas muestran las redes soportadas y los tipos de certificados:

Tipo de red	Servicio de integración de Security Platform	Protocolo	Tipo de certificado
Explorador para la Web/conexión con el servidor (Autenticación de cliente)	Infineon TPM Cryptographic Provider o Infineon TPM RSA and AES Cryptographic Provider (Usuario CSPs)	SSL/TLS	Certificado de usuario
Explorador para la Web/conexión con el servidor (Autenticación de cliente)	Proveedor de Infineon TPM PKCS #11	SSL/TLS	Certificado de usuario
VPN	Infineon TPM Cryptographic Provider	IPsec	Certificado de usuario

	o Infineon TPM RSA and AES Cryptographic Provider (Usuario CSPs)		
VPN	Infineon TPM Platform Cryptographic Provider (Platform CSP)	IPsec	Certificado de computadora
WLAN o LAN alámbrica	Infineon TPM Cryptographic Provider o Infineon TPM RSA and AES Cryptographic Provider (Usuario CSPs)	WLAN: IEEE 802.11 EAP-TLS LAN alámbrica: IEEE 802.1X EAP-TLS	Certificado de usuario
WLAN o LAN alámbrica	Infineon TPM Platform Cryptographic Provider (Platform CSP)	WLAN: IEEE 802.11 EAP-TLS LAN alámbrica: IEEE 802.1X EAP-TLS	Certificado de computadora

Para otros tipos de redes y áreas de aplicación, póngase en contacto con su soporte de producto.



Infineon Security Platform Solution

Autenticación del cliente

Hasta hace poco, las redes de sistemas informáticos utilizaban una base de datos de cuentas centralizada para administrar los usuarios, sus privilegios y sus controles de acceso. Esta técnica es sencilla y eficaz para redes pequeñas. Sin embargo, en el panorama actual, donde las redes grandes con miles de usuarios están a la orden del día, esta forma de control centralizado resulta difícil de administrar. Los problemas de este sistema van desde la comprobación de una cuenta en una base de datos ubicada en Internet hasta la administración de una lista interminable de usuarios. Además, la aparición de Internet ha causado que las redes de sistemas informáticos sean más propensas a sufrir ataques de entidades externas.

Uso de certificados

Los certificados con clave pública ofrecen una solución que facilita en gran modo la administración de grandes números de usuarios en redes extensas, al mismo tiempo que reduce el riesgo de ataques de Id. o contraseña. Estos certificados pueden distribuirse ampliamente, pueden tener varios emisores y pueden comprobarse sin necesidad de consultar una base de datos centralizada.

Los certificados pueden utilizarse para obtener una autenticación de usuarios y unas comunicaciones seguras entre clientes y servidores en el Web. Los certificados permiten a los clientes establecer la identidad de un servidor, ya que el servidor presenta un certificado de autenticación de servidor que revela su origen. Si se conecta a un sitio Web que tiene un certificado de servidor emitido por una entidad emisora de certificados de confianza, puede estar seguro de que quien administra el servidor es realmente la persona u organización que se identifica mediante el certificado. De forma parecida, los certificados permiten a los servidores determinar la identidad de los usuarios. Si un usuario se conecta a un sitio Web, el servidor puede estar seguro de la identidad de dicho usuario si recibe su certificado de cliente. Un certificado utilizado para identificar un servidor recibe el nombre de certificado de servidor, y el proceso de comprobar realmente la identidad del servidor se denomina **autenticación del servidor**. De forma parecida, un certificado utilizado para comprobar la identidad de un cliente recibe el nombre de certificado de cliente, y el proceso de autenticar un cliente se denomina **autenticación del cliente**.

Por ejemplo, si un servidor Web quiere restringir el acceso a la información o los servicios para determinados usuarios o clientes, solicita un certificado de cliente durante el establecimiento de la conexión segura (por ejemplo: SSL).

Mientras que la autenticación del servidor garantiza una transmisión segura de datos, la autenticación del cliente mejora la seguridad de dichas transacciones en línea.

Asignar certificados a cuentas de usuario

La tecnología de clave pública ha proporcionado soluciones para muchas de las preocupaciones en materia de seguridad en redes de gran tamaño. Los certificados pueden utilizarse para verificar la identidad de una entidad, y para comprobar su autenticidad sin necesidad de utilizar extensas bases de datos de usuarios y listas de cuentas de usuario junto con sus privilegios de acceso.

Sin embargo, los sistemas operativos y las herramientas de administración existentes sólo están diseñados para trabajar con cuentas de usuario, no con certificados. La solución más sencilla para conservar las ventajas de los certificados y de las cuentas de usuario consiste en crear una asociación –o asignación– entre un certificado y una cuenta de usuario. De este modo, el sistema operativo puede seguir utilizando cuentas, mientras que los sistemas más grandes y los usuarios utilizan certificados.

En este modelo, un certificado que se ha emitido para un usuario se asigna a la cuenta de dicho usuario en una red. Cuando un usuario presenta su certificado, el sistema busca la asignación y determina qué cuenta debe registrarse.

En esta Guía para los primeros pasos se esbozan distintos enfoques de este tema. Se explica la manera en que pueden prepararse IIS y Active Directory para la autenticación del cliente, así como el uso de la autenticación del cliente con Internet Explorer.

- [Asignar certificados a cuentas de usuario en IIS y Active Directory](#)
- Autenticación del cliente con Internet Explorer

Para un entorno PKCS #11 con Mozilla Firefox, también quedan cubiertas la asignación de certificados y la autenticación del cliente.

- [Asignar certificados a cuentas de usuario en Mozilla Firefox](#)
- [Autenticación del cliente con Mozilla Firefox](#)



La Solución Infineon Security Platform

Autenticación de clientes con Internet Explorer

Si el servidor Web requiere un certificado de cliente por parte del mismo, Internet Explorer firma un mensaje con la clave privada correspondiente al certificado de cliente provisto para asegurar que el usuario es el Propietario auténtico de dicho certificado de cliente.

En Microsoft TechNet hay más información disponible sobre la autenticación de clientes con Internet Explorer.



©Infineon

Technologies AG

La Solución Infineon Security Platform

Mapeo de certificados a cuentas de usuarios en IIS y Active Directory

Se puede mapear un certificado a un usuario de Windows 2000 / XP ya sea a través del servicio de Windows 2000 / XP Active Directory o mediante las reglas definidas en Internet Information Services (IIS).

Puede optar por mapear certificados a cuentas de usuarios tanto en IIS como en Active Directory dependiendo de si está realizando la autenticación de clientes para usuarios dentro de su dominio o de entidades externas fuera del mismo. El mapeo de certificados con Active Directory es ideal para autenticar usuarios dentro de su dominio solamente. Debe utilizar un mapeo IIS si desea autenticar usuarios que no pertenecen a su dominio.

Nota: La autenticación de clientes con IIS involucra el uso de Secure Sockets Layer (SSL) de su servidor Web, lo que implica que deberá obtener un certificado de servidor de una entidad certificada. Esto se debe a que la autenticación del servidor por medio de un certificado de servidor es obligatoria para una conexión SSL y la autenticación del cliente es sólo una medida de seguridad adicional.

En Microsoft TechNet encontrará más información sobre el "mapeo de certificados a cuentas de usuarios en IIS y Active Directory" y sobre "Internet Information Service".



©Infineon

Technologies AG

Infineon Security Platform Solution

Autenticación del cliente con Mozilla Firefox

Si el servidor Web solicita al cliente un certificado de cliente, Mozilla Firefox firma un mensaje con la clave privada correspondiente al certificado de cliente configurado a fin de garantizar que el usuario sea realmente el propietario del certificado de cliente.

Según la configuración de la caché de contraseñas, puede ser que deba introducir la contraseña de la base de datos de certificados cada vez que se solicite el certificado de cliente para la autenticación. De lo contrario, sólo se le solicitará la primera vez que se realice la autenticación.

Si ya tiene asignado un certificado para utilizarlo con una página Web especial, éste se toma automáticamente. Si no es así, se le solicitará que especifique el certificado correcto. La descripción del procedimiento para [asignar certificados a cuentas de usuarios y páginas Web](#) le indica los pasos necesarios para configurar su entorno de seguridad correctamente.



©Infineon

Technologies AG

Infineon Security Platform Solution

Asignar certificados a cuentas de usuario en Mozilla Firefox

La asignación de un certificado a una cuenta de usuario se realiza automáticamente debido a que el certificado se almacena en la base de datos de certificados local del usuario. El acceso a esta base de datos está protegido mediante una contraseña específica del usuario. Mientras no se realice ninguna modificación en el equipo, los certificados del almacén de certificados local estarán disponibles.

En una red de empresa de grandes dimensiones, puede surgir la necesidad de que los certificados no sólo estén disponibles en un equipo local, sino en todas las máquinas de la red. Dado que las estructuras administrativas no ofrecen carpetas compartidas para almacenar los perfiles de usuario, es necesario exportar los certificados de usuario del equipo del usuario a un directorio de la empresa. Este servicio de directorio proporcionará un servicio de autenticación centralizado o permitirá volver a importar un certificado de usuario en otro equipo.

Enfoque alternativo: los perfiles de usuario almacenados en una carpeta compartida (perfiles móviles) reducen todo lo posible el trabajo administrativo. En conjunción con la base de datos de certificados de usuario y TODOS los demás datos específicos del usuario almacenados en esa carpeta, queda garantizado el acceso coherente desde toda la red de la empresa.

Nota: la autenticación del cliente implica el uso del nivel de sockets seguros (SSL) de su servidor Web, lo que significa que deberá obtener un certificado de servidor de una entidad emisora de certificados. Esto se debe a que la autenticación del servidor mediante un certificado de servidor es obligatoria para una conexión SSL y la autenticación del cliente es sólo una medida de seguridad adicional.

La Solución Infineon Security Platform

Red privada virtual (VPN)

Una VPN es una red privada que utiliza una red pública (generalmente, Internet) para conectar sitios o usuarios remotos entre sí. En lugar de utilizar una conexión física dedicada, como una línea dedicada, las VPN utilizan conexiones "virtuales" que se direccionan a través de Internet desde la red privada de la empresa hasta el sitio o empleado remoto.

Acceso remoto, también denominado conexión telefónica privada virtual (VPDN), es decir, una conexión entre el usuario y la red de área local (LAN) empleada por las empresas. Un ejemplo es una empresa con empleados que necesitan conectarse a la red privada desde diversas ubicaciones remotas. Normalmente, una empresa que desee diseñar una VPN de gran tamaño para acceso remoto contratará los servicios externos de un proveedor de servicios para empresas (ESP). El ESP configura el servicio de acceso a la red (NAS) y proporciona a los usuarios remotos el software de cliente necesario para sus equipos de sobremesa.

La Solución Infineon Security Platform

Protocolo de autenticación extensible (EAP)

El Protocolo de autenticación extensible se utiliza para crear configuraciones más seguras de redes privadas virtuales.

EAP proporciona una capa adicional de seguridad a las tecnologías VPN. EAP es un componente tecnológico esencial para garantizar la seguridad de las conexiones en las redes privadas virtuales (VPN), ya que la seguridad que ofrece contra ataques basados en la fuerza bruta o en diccionarios o contra sistemas de descubrimiento de contraseñas es superior a la que ofrecen otros métodos de autenticación.

EAP posibilita esta función mediante tecnologías basadas en entidades emisoras de certificados (CA) y Security Platform. Para utilizar EAP con una VPN, el servidor y el cliente deben estar configurados para aceptar la autenticación EAP como método de autenticación válido, y deben disponer de un certificado de usuario (X.509).



©Infineon

Technologies AG

Solución Infineon Security Platform

Configuración de una VPN para el uso de EAP

La solución Infineon Security Platform, la cual provee la autenticación del cliente, utiliza el método de autenticación de certificados. Antes de proceder con la configuración del cliente se debe disponer de un [certificado](#) aprobado por una entidad certificada. Tanto el cliente como el servidor deben tener una misma entidad certificada o una entidad certificada en jerarquía de confianza. El cliente también debe tener un Trusted Platform Module.



Cuando se solicita un certificado se debe elegir uno de los [Cryptographic Service Providers](#) provistos con la solución Security Platform. El propósito del certificado debe ser la **autenticación de cliente**. En grandes empresas el administrador posiblemente ya ha determinado certificados para tal propósito.

Para obtener más información sobre VPN consulte las Páginas de ayuda de Microsoft VPN o Microsoft TechNet. Para obtener la información necesaria en la Ayuda de Microsoft, minimice todas las ventanas abiertas para visualizar el entorno de escritorio de Windows. Después pulse F1 y busque la palabra clave apropiada.

La Red privada virtual utiliza Internet o Intranet para funcionar. Antes de realizar la conexión VPN el usuario debe disponer de instalaciones de Internet o Intranet para conectarse al servidor VPN.

Para utilizar EAP el cliente debería realizar inicialmente una conexión. Puede utilizar las **Conexiones de red** de su sistema operativo para configurar las conexiones VPN. En caso de que necesite ayuda detallada acerca de los pasos necesarios para su sistema operativo, consulte Microsoft Windows Help o Microsoft TechNet.

Después de realizar la conexión, ésta debe configurarse para utilizar EAP. Para hacerlo, siga estos pasos:

- Haga clic con el botón derecho en la conexión VPN nueva para ver las propiedades.
- Configure los ajustes de autenticación en la pestaña de seguridad para utilizar el Protocolo de autenticación extensible (EAP) con la opción de utilizar SmartCard u otro certificado.
- Configure las propiedades de EAP para utilizar un certificado en el

ordenador.



Si posee más de un certificado para autenticación de clientes y encriptación, asegúrese de utilizar el certificado correcto para la conexión VPN. Cuando inicie una conexión VPN seleccione un certificado asociado con uno de los [Cryptographic Service Providers](#) entregados con la Solución Security Platform.

El usuario debe iniciar una sesión en la computadora para utilizar EAP con un certificado de usuario.



©Infineon

Technologies AG

La Solución Infineon Security Platform

Red de área local inalámbrica (WLAN por sus siglas en inglés)

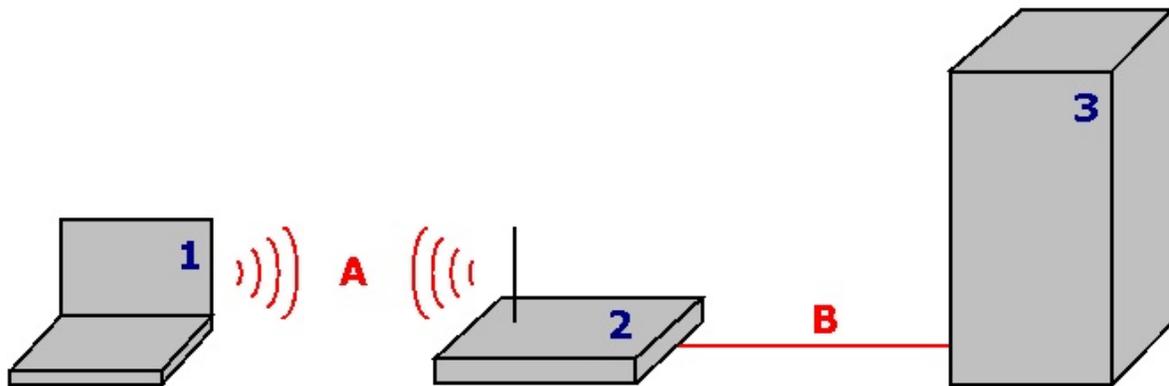
Con la Solución Security Platform puede proteger las claves privadas de los certificados que se utilizan para las WLANs (IEEE 802.1 EAP-TLS) y las LANs alámbricas (IEEE 802.1X EAP-TLS). Se realiza al utilizar uno de los Cryptographic Service Providers (CSP) que se incluyen en la Solución Security Platform.

Este tema se enfoca en las WLANs.

Introducción a la WLAN

Una red de área local inalámbrica (WLAN por sus siglas en inglés) utiliza ondas de radio de alta frecuencia en lugar de cables para comunicarse entre los nodos. Las WLAN no requieren línea de vista entre el emisor y el receptor. Los puntos de acceso inalámbricos (estaciones base) se encuentran conectados por cables a una red Ethernet y transmiten una frecuencia de radio sobre una zona de cobertura. Las LAN inalámbricas funcionan como los sistemas de telefonía celular. En los sistemas que se diseñan para el uso de oficina, los usuarios se pueden cambiar discretamente de punto de acceso sin perder la conexión.

El estándar **IEEE 802.11** (wireless fidelity, "Wi-Fi") especifica la tecnología para las LAN inalámbricas. El estándar incluye los métodos de encriptación Wi-Fi Protected Access (**WPA**) y Wired Equivalent Privacy (**WEP**).



1	Cliente WLAN	Su PC de Security Platform. El Trusted Platform Module protege su clave privada de certificado. Los clientes WLAN poseen una conexión inalámbrica (A) hacia un punto de acceso.
2	Punto de acceso	También llamado "estación base". El punto de acceso de la WLAN conecta los clientes WLAN a un red por cable (B).
3	Servidor RADIUS	Por ejemplo, el servicio de autenticación de Internet (IAS por sus siglas en inglés) que se incluye en Microsoft Windows 2003 Server.

El servidor RADIUS administra su autenticación.

Más información básica

En Internet puede encontrar disponible información básica sobre WLANs:

- Microsoft Developer Network (MSDN) y Microsoft Windows Help (busque "wireless networking")
- Wi-Fi Alliance
- Wireless LAN Association (WLANA)

Cómo asegurar su WLAN con la Solución Security Platform



Precondiciones:

- Aparte del hardware y del software que se requieren las WLAN, su cliente WLAN debe ser una PC de Security Platform con un Trusted Platform Module.
- Necesita inscribir un certificado protegido por el Security Platform.

[WLAN paso a paso](#)



©Infineon Technologies AG

La Solución Infineon Security Platform

WLAN paso a paso

Este tema se enfoca en las WLANs. En lo concerniente a la configuración de las LAN por cable (IEEE 802.1X), el único paso específico de Security Platform (la selección del Cryptographic Service Provider) es el mismo que para la WLAN.

Configuración y utilización de la WLAN paso a paso

Paso	Para ser realizado por el/los usuario(s)
1. Obtenga un certificado de autenticación de cliente	Todos los usuarios de Security Platform a utilizar la WLAN
2. Configure el software de la WLAN	Un administrador
3. Conecte su cliente WLAN	Todos los usuarios de Security Platform a utilizar la WLAN

Obtenga de un certificado de autenticación de cliente

Para asegurar su conexión WLAN necesita un [certificado](#) aprobado por una entidad certificada. Tanto el cliente WLAN como el servidor RADIUS deben utilizar una entidad certificada de confianza. Asegúrese de utilizar una plantilla de solicitud de certificado para *Autenticación del cliente*.



Selección del Cryptographic Service Provider:

Durante la solicitud del certificado necesita seleccionar el Cryptographic Service Provider a usar por su certificado.

- Si se quiere autenticar usted mismo, seleccione un usuario CSP (*Infineon TPM Cryptographic Provider* o *Infineon TPM RSA and AES Cryptographic Provider*).
- Si desea autenticar su computadora, seleccione la plataforma CSP (*Infineon TPM Platform Cryptographic Provider*).
Par utilizar la plataforma CSP, debe ser un administrador o miembro del grupo de administradores.

Configure el software de la WLAN

Refiérase a la documentación de su proveedor de WLAN en lo relativo a la configuración de la WLAN completa. El software de su proveedor puede incluir un software cliente para configurar las conexiones WLAN.

También puede utilizar las **Conexiones de red** de su sistema operativo para configurar las conexiones WLAN:

- Configure una conexión de red inalámbrica en su cliente WLAN como se describe en Microsoft Windows Help (busque "wireless networking").
- Asegúrese de utilizar los siguientes valores de configuración de **Autenticación**:
 - Seleccione **Habilitar autenticación IEEE 802.1x para esta red**.
 - En **Tipo EAP**, seleccione **Smart Card u otro certificado**.
 - En Propiedades, seleccione **Utilizar un certificado en esta computadora**.
 - Si desea seleccionar el certificado cada vez que comienza una conexión inalámbrica, entonces destilte la opción **Utilizar selección de certificado simple**.



Para configurar los valores de la configuración de **Autenticación** debe ser un administrador o un miembro del grupo de administradores.

Conecte su cliente WLAN

Refiérase a la documentación de su proveedor de WLAN en lo relativo a las conexiones WLAN.

También puede utilizar las **Conexiones de red** de su sistema operativo para conectar su cliente WLAN:

- Conecte su cliente WLAN como se describe en Microsoft Windows Help (busque "wireless networking").
- Asegúrese de utilizar el certificado solicitado en el paso "Obtenga un certificado de autenticación de cliente".



©Infineon Technologies AG

La Solución Infineon Security Platform

Preguntas más frecuentes y solución de problemas

[Preguntas más frecuentes \(FAQ\)](#)

[Solución de problemas](#)

Technologies AG



Solución Infineon Security Platform

Preguntas más frecuentes (FAQ)

[¿Cómo se puede quitar un usuario de Infineon Security Platform?](#)

[¿Es un problema de seguridad almacenar datos de recuperación de emergencia en una máquina remota?](#)

[¿Se puede desinstalar el software de la solución Infineon Security Platform, y de ser así, cómo se hace?](#)

[¿Qué información permanece en el sistema luego de una desinstalación exitosa?](#)

[Después de inscribir un certificado por medio de Internet Explorer, el certificado no se puede utilizar. Aparece un mensaje de error.](#)

[La función de compresión de carpetas del sistema operativo se utiliza para almacenar datos del usuario. ¿Cómo se puede activar EFS para esta carpeta comprimida? ¿Pueden combinarse las funciones?](#)

[El certificado asignado a una carpeta EFS debe cambiarse. ¿Se puede realizar sin arriesgar los datos de esta carpeta? ¿Es posible asignar un certificado arbitrario a la carpeta?](#)

[¿Cómo se puede preparar un Infineon Security Platform para una copia de seguridad exitosa? ¿Qué archivos son esenciales para una restauración exitosa de un Infineon Security Platform que utiliza mecanismos del sistema?](#)

[¿Cómo configurar y administrar el Archivo de Copia de Seguridad, especialmente con relación a los valores de la política?](#)

[¿Cómo se crea un archivo de almacenamiento de clave pública a partir de un archivo de tarjeta de seguridad?](#)



Los comentarios sobre EFS sólo son importantes para las ediciones de Windows que admiten EFS.

¿Cómo se puede quitar un usuario de Infineon Security Platform?

Existen dos tipos diferentes de operaciones de remoción:

- **La eliminación total de una cuenta de usuario del sistema operativo es una operación directa permitida por Windows. Al quitar una cuenta de usuario, debe tildar la casilla de verificación para la eliminación del perfil de usuario. Esta operación elimina completamente del sistema la**

información de la cuenta del usuario.

- **Para eliminar solamente la información del usuario de Infineon Security Platform sin alterar la información de la cuenta del sistema, debe borrar la carpeta específica del usuario**
`\\%AppData%\Infineon\TPM Software 2.0.`

Si desea eliminar todos los datos relacionados a un Usuario de Security Platform, consulte los datos específicos del usuario enumerados en esta sección [¿Qué información permanece en el sistema luego de una desinstalación exitosa?](#).

Nota:  **Si existen datos en el sistema que fueron encriptados con una clave específica de usuario de Infineon Security Platform, una vez eliminado el usuario dichos datos no se podrán descryptar.**



¿Es un problema de seguridad almacenar datos de recuperación de emergencia en una máquina remota?

No hay ningún problema de seguridad. Los datos están protegidos por la tarjeta de seguridad para la recuperación de emergencia, la cual se protege a su vez por medio de una contraseña.



En el [modo servidor](#) no hay problemas de seguridad ya que la recuperación de emergencia es llevada a cabo por el Trusted Computing Management Server.



¿Se puede desinstalar el software de la solución Infineon Security Platform, y de ser así, cómo se hace?

Se puede desinstalar utilizando el proceso estándar de eliminación de software que ofrece el sistema operativo. Antes de hacerlo, debe guardar todos los datos del usuario protegidos por Security Platform. Si no lo hace, no se podrá acceder a estos datos una vez que el Software de la Solución Infineon Security Platform se eliminó del sistema. El último paso es desactivar el Trusted Platform Module en la BIOS de la computadora.

Se puede instalar una nueva versión sobre una anterior, sin desinstalarla. En este caso no se requiere una copia de seguridad de los datos completos del usuario.



¿Qué información permanece en el sistema luego de una desinstalación exitosa?

Si se desinstala el Software de la Solución Security Platform, queda algo de información en el sistema. Al guardar las configuraciones y credenciales del usuario y la plataforma, el sistema volverá al mismo estado anterior una vez reinstalado. De esta manera no se perderán los datos encriptados previamente luego de una reinstalación del Software de Infineon Security Platform.

Sin embargo, si estos datos ya no fueran necesarios y se debiera limpiar el sistema completamente, deberán borrarse los siguientes datos.

Paquete de archivos de la copia de seguridad: Los administradores especifican la ubicación de los paquete de archivos de la copia de seguridad escritos automáticamente. Observe que los Archivos de copia de seguridad creados automáticamente se representan en el sistema como un archivo XML y una carpeta con el mismo nombre, por ejemplo: archivo [SPSystemBackup.xml](#) y carpeta [SPSystemBackup](#). Además, puede haber los paquete de archivos de la copia de seguridad escritos manualmente.

Tarjeta de seguridad para la recuperación de emergencia: La ubicación la especifica el propietario de Security Platform durante la inicialización del mismo.

paquete de archivos de la restauración de emergencia:

i) Windows 7 y Vista: `\\%ALLUSERSPROFILE%\Infineon\TPM Software 2.0\RestoreData\<<Machine SID>\Users\<<User SIDs>\SHTempRestore.xml`

ii) Windows XP Professional, Windows 2000 y otros sistemas operativos habilitados: `\\%ALLUSERPROFILE%\<Application Data>\Infineon\TPM Software 2.0\RestoreData\<<Machine SID>\Users\<<User SIDs>\SHTempRestore.xml`

Archivos de claves del sistema y datos del sistema:

i) Windows 7 y Vista: `\\%ALLUSERSPROFILE%\Infineon\TPM Software 2.0\PlatformKeyData
IFXConfigSys.xml
IFXFeatureSys.xml
TCSps.xml
TPMCPSys.xml`

ii) Windows XP Professional, Windows 2000 y otros sistemas operativos

habilitados: \%ALLUSERPROFILE%\<Application Data>\Infineon\TPM Software 2.0\ PlatformKeyData
IFXConfigSys.xml
IFXFeatureSys.xml
TCSps.xml
TPMCPSys.xml

Archivos locales de la copia de seguridad sombra:

i) Windows 7 y Vista:

\%ALLUSERSPROFILE%\Infineon\TPM Software 2.0\BackupData\<Machine SID>\System\SHBackupSys.xml
\%ALLUSERSPROFILE%\Infineon\TPM Software 2.0\BackupData\<Machine SID>\Users\<User SIDs\SHBackup.xml

ii) Windows XP Professional, Windows 2000 y otros sistemas operativos habilitados:

\%ALLUSERPROFILE%\<Application Data>\Infineon\TPM Software 2.0\BackupData\<Machine SID>\System\SHBackupSys.xml
\%ALLUSERPROFILE%\<Application Data>\Infineon\TPM Software 2.0\BackupData\<Machine SID>\Users\<User SIDs\SHBackup.xml

Archivos de claves de usuario: \%AppData%\Infineon\TPM Software 2.0\UserKeyData\TSPps.xml

Contenedor del TPM Cryptographic Service Provider:

\%AppData%\Infineon\TPM Software 2.0\UserKeyData\TSPps.xml

Archivo del proveedor de TPM PKCS #11: \%AppData%\Infineon\TPM Software 2.0\UserKeyData\TSMck.xml

Archivos de configuración de usuario: \%AppData%\Infineon\TPM Software 2.0\UserKeyData\
IFXConfig.xml
IFXFeature.xml

Claves del registro:

HKEY_LOCAL_MACHINE\SOFTWARE\Infineon\TPM Software
HKEY_CURRENT_USER\Software\Infineon\TPM software

Las siguientes claves de registro de **Personal Secure Drive** deben borrarse manualmente cuando se desinstala la función de seguridad del Personal Secure Drive:

[HKEY_LOCAL_MACHINE\SOFTWARE\Infineon\TPM Software\PSD]
[HKEY_CURRENT_USER\SOFTWARE\Infineon\TPM Software\PSD]

Personal Secure Drive Directorios: Los siguientes directorios también se deben borrar manualmente:

x:\Security Platform\Personal Secure Drive\System Data

donde x: es la unidad de disco donde se encuentran los Personal Secure Drives. Esta unidad de disco puede seleccionarse durante la creación del Personal Secure Drive y por lo tanto puede ser cualquier disco duro local, o se puede definir por la política de usuario local del Personal Secure Drive.

Misceláneos:

Tarea de copia de seguridad programada de certificados registrados basados en Trusted Platform Module (por ejemplo: C:\WINDOWS\Tasks\Security Platform Backup Schedule)



Después de inscribir un certificado por medio de Internet Explorer, el certificado no se puede utilizar. Aparece un mensaje de error.

Internet Explorer bloqueó el certificado, a pesar de encontrarse almacenado en el depósito de certificados del usuario. Cierre Internet Explorer y vuelva a abrirlo para desbloquear el certificado.



La función de compresión de carpetas del sistema operativo se utiliza para almacenar datos del usuario. ¿Cómo se puede activar EFS para esta carpeta comprimida? ¿Pueden combinarse las funciones?

No es posible una combinación, ya que el sistema operativo no permite que una carpeta comprimida sea también una carpeta protegida de EFS. Primero, se debe cancelar la compresión. Luego puede activarse la funcionalidad de EFS para la carpeta.



El certificado asignado a una carpeta EFS debe cambiarse. ¿Se puede realizar sin arriesgar los datos de esta carpeta? ¿Es posible asignar un certificado arbitrario a la carpeta?

Por lo general, no hay problemas en asignar un certificado adicional a una carpeta EFS. La condición límite primordial es que todos los certificados deben estar bajo el control del mismo [Cryptographic Service Provider](#). Mientras exista uno o más certificados asignados previamente, los datos encriptados todavía podrán leerse. Una vez que se borra el certificado que protege un archivo en una carpeta EFS, se pierden los archivos respectivos.



¿Cómo se puede preparar un Infineon Security Platform para una copia de seguridad exitosa? ¿Qué archivos son esenciales para una restauración exitosa de un Infineon Security Platform que utiliza mecanismos del sistema?

Los archivos del núcleo del Infineon Security Platform no incluyen las aplicaciones del software de Infineon Security Platform. Se puede reinstalar después de restaurada una copia de seguridad del sistema.

Mediante el [asistente para copia de seguridad de Infineon Security Platform](#) se resguardan los datos específicos del software de la solución Infineon Security Platform.

El asistente para la copia de seguridad de Infineon Security Platform no realiza copias de seguridad de datos protegidos, como son sus archivos encriptados o correo electrónico, que deben resguardarse por medio de otras herramientas de copia de seguridad. Debe incluir el paquete de archivos de copia de seguridad del asistente para la copia de seguridad de Infineon Security Platform en su rutina de copia de seguridad de datos en masa.

Si no utiliza el asistente para la copia de seguridad de Infineon Security Platform para los datos específicos del Software de la Solución Security Platform, asegúrese de realizar una copia de seguridad de todos los datos enumerados en la sección [¿Qué información queda en el sistema luego de una desinstalación exitosa?](#).



- Las copias de seguridad automáticas de sistema configuradas por el administrador de Security Platform, también incluyen datos de recuperación de emergencia.
- En el [modo servidor](#), las copias de seguridad y las restauraciones son llevadas a cabo por Trusted Computing Management Server.



¿Cómo configurar y administrar el Archivo de Copia de Seguridad, especialmente con relación a los valores de la política?

Puede configurar todas las Security Platforms de su empresa para usar un Archivo de Copia de Seguridad común ajustando la *Ubicación del Archivo de Copia de Seguridad* de la [política](#).

En el caso de que se tenga que crear un nuevo Archivo de Copia de Seguridad, es muy importante no importar las políticas antes de que se haya inicializándola primera de Infineon Security Platform.

Luego debe ejecutarse el administrador de políticas y configurar correctamente la política estableciendo la ubicación del paquete de archivos de la copia de seguridad que se creó previamente. Finalmente el archivo configurado será usado automáticamente cuando se hayan inicializado el resto de las Security Platforms de la empresa.



Esta sección no es aplicable en [modo servidor](#), ya que las Copias de Seguridad y la Recuperación están administrados por el Trusted Computing Management Server.



¿Cómo se crea un archivo de almacenamiento de clave pública a partir de un archivo de tarjeta de seguridad?

En la configuración de política de grupo, puede especificar que se utilice desde un archivo de almacenamiento la clave pública de una tarjeta de seguridad para la recuperación de emergencia existente o la tarjeta de seguridad de restablecimiento de la contraseña (consulte *Uso de la clave pública de la Tarjeta de Recuperación de emergencia del archivo* y *Uso de la clave pública de la Tarjeta de restablecimiento de contraseña del archivo* en [Políticas del Sistema](#)).

Para crear dicho archivo de almacenamiento a partir del archivo de tarjeta de seguridad existente, realice los siguientes pasos:

- Inicialice por completo la plataforma (incluida la recuperación de emergencia y el restablecimiento de la contraseña) con configuración de políticas predeterminadas en el primer sistema (p. ej. en un sistema de prueba). El Asistente para la inicialización rápida crea un archivo de tarjeta de seguridad genérico tanto para la recuperación de emergencia como para el

restablecimiento de la contraseña.

El Asistente para la inicialización rápida crea un archivo de tarjeta de seguridad para la recuperación de emergencia y otro para el restablecimiento de la contraseña.

- Ejecute la secuencia de comandos que se adjunta a continuación en el mismo sistema para crear el archivo de almacenamiento de clave pública necesario a partir del archivo de tarjeta de seguridad correspondiente.
- Copie el archivo de almacenamiento de clave pública en una ubicación adecuada y habilite las directivas anteriormente mencionadas.

Secuencia de comandos GeneratePubKeyArchive.vbs:

```
'GeneratePubKeyArchive.vbs <Ruta completa a tarjeta.xml> <Ruta completa a  
PubKeyArchive.xml>
```

```
'La <Ruta completa a tarjeta.xml> puede ser una de las siguientes tarjetas:
```

```
' - SPPwdResetToken.xml
```

```
' - SPEmRecToken.xml
```

```
' - SPGenericToken.xml
```

```
'La <Ruta completa a PubKeyArchive.xml> es la salida, que contiene la clave  
pública extraída de la tarjeta de entrada:
```

```
' - SPPwdResetTokenPubKeyArchive.xml
```

```
' - SPEmRecTokenPubKeyArchive.xml
```

```
' - SPGenericTokenPubKeyArchive.xml
```

```
'Para que lo utilice la política "Uso de la clave pública de la Tarjeta de  
Recuperación de emergencia del archivo":
```

```
' - SPEmRecTokenPubKeyArchive.xml
```

```
' - SPGenericTokenPubKeyArchive.xml
```

```
'Para que lo utilice la política "Uso de la clave pública de la Tarjeta de  
restablecimiento de contraseña del archivo":
```

```
' - SPPwdResetTokenPubKeyArchive.xml
```

```
' - SPGenericTokenPubKeyArchive.xml
```

```
'Asegúrese de especificar la ruta completa, p. ej.:
```

```
' GeneratePubKeyArchive.vbs "c:\tmp\SPGenericToken.xml"
```

```
"c:\tmp\SPGenericTokenPubKeyArchive.xml"
```

```
Si WScript.Arguments.Count <> 2 Entonces
```

```
    WScript.Echo "Usage: " & Wscript.ScriptName & " ""<Ruta completa a  
tarjeta.xml>"" ""<Ruta completa a PubKeyArchive.xml>"""
```

```
    WScript.Quit
```

```
End If
```

```
Set MPBase = WScript.CreateObject("IfxSpMgtPrv.MgmtProvider")
```

```
Set MPToken = MPBase.GetInterface(10)
' CreationFlags: keep existing file = 0, overwrite existing file = 1
CreationFlags = 0
ReservedFlag = 0
MPToken.CreatePublicKeyFile WScript.Arguments(0), WScript.Arguments(1),
CreationFlags, ReservedFlag
'Error Handling if failing to be added here
WScript.Echo "Done"
```



Esta sección no es aplicable en [modo servidor](#), ya que la recuperación de emergencia y el restablecimiento de la contraseña están administrados por el Trusted Computing Management Server.



Solución Infineon Security Platform

Solución de problemas

La siguiente sección describe los procedimientos para a llevar a cabo las operaciones más habituales de solución de problemas en un Infineon Security Platform:

[Debe configurarse una plataforma, pero el Trusted Platform Module ya tiene un propietario.](#)

[Se configuró el Infineon Security Platform, pero cambió su propietario.](#)

[¿Qué debe tenerse en cuenta para la recuperación de emergencia al utilizar el asistente para la inicialización de Infineon Security Platform?](#)

[Los documentos que se encuentran en una carpeta protegida EFS deben restaurarse desde una copia de seguridad del sistema. El usuario de Infineon Security Platform no existe en el sistema de destino. ¿Cómo se puede resolver esta situación?](#)

[Una aplicación utilizada con frecuencia genera archivos temporales fuera de las carpetas temporales estándar. Generalmente, ninguna carpeta temporal está protegida por EFS. ¿Cómo se pueden resguardar los archivos temporales de esta aplicación, en especial ya que estos archivos permanecen en el disco duro cuando la misma se cierra?](#)

[Cuando el usuario de Infineon Security Platform accede por primera vez a una carpeta EFS, se le solicita la contraseña para la clave de usuario básico. Si se cancela este diálogo y se configura un agente de recuperación, el usuario aún puede acceder a los datos en la carpeta EFS siempre y cuando la clave privada del agente de recuperación esté disponible para el usuario. ¿Esto es un error del sistema?](#)



Los comentarios sobre EFS no son importantes para las ediciones Windows Home porque no admiten EFS.

Debe configurarse una plataforma, pero el Trusted Platform Module ya tiene un propietario.

En este caso se utilizará el Propietario de Security Platform existente para inicializar Security Platform. Para esto se requiere conocimiento de la Contraseña de propietario existente o acceso al correspondiente Archivo de copia de seguridad de contraseña de propietario.

Esta es una situación típica en un entorno multisistema, donde existe más de un sistema operativo en una computadora. El Propietario de Infineon Security Platform ("Storage Root Key", SRK por sus siglas en inglés) no puede salir del Trusted Platform Module, y no se puede introducir desde el exterior. Por lo tanto, no es posible realizar una operación de "importación".

Dependiendo de la existencia de las claves de usuario básico, se requiere una metodología diferente durante la [inicialización de Security Platform](#).

Si no se creó una clave de usuario básico para el Security Platform, se puede crear un nuevo paquete de archivos de la copia de seguridad (que contiene datos de recuperación de emergencia). Una vez hecho esto, el Infineon Security Platform está listo para las demás operaciones.

Si se configura una clave de usuario básico y un paquete de archivos de la copia de seguridad (que contiene los datos de recuperación de emergencia), es muy importante no sobrescribir el paquete de archivos durante la inicialización de Security Platform.



En [modo servidor](#), primero tiene que limpiar el propietario si ya existe un propietario antes de conectar el sistema al Trust Domain. La Security Platform será entonces incorporada automáticamente en el Trust Domain (Vea [la inscripción de la plataforma](#)).



Se configuró el Infineon Security Platform, pero cambió su propietario.

Si se configuró el Security Platform con la recuperación de emergencia, sus credenciales de Security Platform se pueden reactivar por medio de la [Asistencia para la recuperación de emergencia](#) de la solución de Security Platform.



En [modo servidor](#), el Trusted Platform Module no deberá tener un Propietario antes de conectar el sistema al Trust Domain, es decir, no se ha inicializado aún (ni por Infineon TPM Professional Package en modo independiente ni por Trusted Domain Server en modo servidor, o por cualquier otro software como Windows Vista Trusted Platform Module (TPM) Management).



¿Qué debe tenerse en cuenta para la recuperación de emergencia al utilizar el asistente para la inicialización de Infineon Security Platform?

Se puede realizar una recuperación de emergencia de un sistema si su Trusted Platform Module se ha reemplazado o restablecido, y si se encuentra disponible una imagen de la copia de seguridad la cual permita restaurar sus datos. Los datos específicos del usuario relacionado a Security Platform y los datos de la recuperación de emergencia se resguardan en copias de seguridad automáticas del sistema.

El administrador de Infineon Security Platform debe tener acceso al paquete de archivos de la copia de seguridad y a la tarjeta de seguridad de la recuperación de emergencia que se creó al configurar el sistema, y debe conocer la contraseña que protege esta tarjeta.

El administrador del Infineon Security Platform debe restaurar el sistema, ejecutando el [asistente para copia de seguridad de Infineon Security Platform](#).

Si la recuperación se hace en una computadora cuyo nombre se ha modificado, se debe conocer el antiguo nombre de la misma o el ID de la plataforma de la computadora (SID). Es posible que el paquete de archivos de copia de seguridad contenga datos de recuperación de varias computadoras. En este caso necesita seleccionar la computadora a restaurar del paquete de archivos de la copia de seguridad.



En el [modo servidor](#), la recuperación de emergencia es llevada a cabo por Trusted Computing Management Server.



Los documentos que se encuentran en una carpeta protegida EFS deben restaurarse desde una copia de seguridad del sistema. El usuario de Infineon Security Platform no existe en el sistema de destino. ¿Cómo se puede resolver esta situación?

Si la clave de usuario básico ya no está disponible y no se configuró un certificado de recuperación (para un agente de recuperación), el documento se pierde definitivamente.

Caso contrario, el primer paso es restaurar el archivo desde la copia de seguridad. Esto se lleva a cabo sin alterar las propiedades relevantes de seguridad del archivo. Como próximo paso se debe utilizar el certificado de recuperación para habilitar el agente de recuperación para descifrar el archivo.



Una aplicación utilizada con frecuencia genera archivos temporales fuera de las carpetas temporales estándar. Generalmente, ninguna carpeta temporal está protegida por EFS. ¿Cómo se pueden resguardar los archivos temporales de esta aplicación, en especial ya que estos archivos permanecen en el disco duro cuando la misma se cierra?

Este es un problema común para muchas aplicaciones. Dependiendo de la aplicación, puede que los archivos temporales se creen fuera de las carpetas EFS que se configuraron. Cuando esta no es la carpeta %AppData% común en el perfil del usuario (comúnmente llamada "Application data"), se trata de una función específica de la aplicación y no se puede llevar a cabo ninguna orden para manejar la situación. Una vez que se conoce la ubicación (y la aplicación no permite la configuración de la carpeta), aplicar la seguridad EFS en la carpeta especificada puede ser una solución. Cuando esto no es factible, debe asegurarse de borrar esos archivos al cerrar la aplicación.

En Microsoft Developer Network (MSDN) encontrará más información con respecto a la solución de problemas para el Encrypting File System.



Cuando el usuario de Infineon Security Platform accede por primera vez a una carpeta EFS, se le solicita la contraseña para la clave de usuario básico. Si se cancela este diálogo y se configura un agente de recuperación, el usuario aún puede acceder a los datos en la carpeta EFS siempre y cuando la clave privada del agente de recuperación esté disponible para el usuario. ¿Esto es un error del sistema?

Este comportamiento es correcto debido al diseño del agente de recuperación. Al configurar un certificado de recuperación para una carpeta EFS, el agente de recuperación lo utiliza cuando se accede por primera vez a la carpeta. Dependiendo de si la computadora se encuentra o no en un dominio, existen diferentes soluciones:

La computadora se encuentra en un dominio: Aquí el administrador debe encargarse de la asignación del certificado. Si no existe ninguna asignación a un usuario específico de Infineon Security Platform, el comportamiento descrito no ocurre.

La computadora corre bajo Windows 2000 y no es miembro de un dominio: Una de las posibilidades es asegurarse de que la clave privada del agente de recuperación no esté disponible para los usuarios comunes de Security

Platform.

El equipo se ejecuta con otro sistema operativo admitido y no es miembro de un dominio: En este caso el certificado de recuperación normalmente no existe, por lo que el comportamiento no debe ocurrir.



©Infineon Technologies AG

La Solución Infineon Security Platform - Visor de certificados y selección de certificados

Visor de certificados y selección de certificados de Infineon Security Platform

El visor de certificados y la selección de certificados de Infineon Security Platform se utilizan para la administración de certificados.

Diferencias con el Microsoft Management Console Certificates Snap-In

A diferencia del [Microsoft Management Console Certificates Snap-In](#), puede vincular certificados al Security Platform por medio del Visor de certificados y selección de certificados de Security Platform:

- Se pueden proteger las claves privadas mediante el Trusted Platform Module
- Se pueden seleccionar los certificados a utilizar para la encriptación de archivos y carpetas por medio de Encrypting File System (EFS) y Personal Secure Drive (PSD).

Diferencias entre el visor de certificados y la selección de certificados

El visor de certificados y la selección de certificados comparten algunas funcionalidades de administración de certificados comunes, e.j. visualización de una lista de certificados, visualización de los detalles de las claves privadas y de los certificados e importación de los certificados PKCS #12 a la Security Platform.

Las diferencias entre el visor de certificados y la selección de certificados son:

Visor de certificados: El visor de certificados es una herramienta especial para la administración de certificados de la solución Security Platform. Por ejemplo, se pueden proteger las claves privadas mediante el Trusted Platform Module.

Selección de certificados: El objetivo de la función de selección de certificados es seleccionar un certificado para la encriptación de archivos y carpetas con EFS o PSD. También puede crear un certificado autofirmado o solicitar un certificado de una entidad certificante (CA, por sus siglas en inglés)

Cómo inscribir y seleccionar certificados

Inscriba y seleccione **Certificados EFS** por medio de **Selección de certificados**:

- Por medio de **Solicitar...** se puede solicitar un certificado de una entidad certificante externa (CA, por sus siglas en inglés)
- Por medio de **Crear** se puede solicitar un certificado de una entidad certificante dentro de su propio dominio, o crear un certificado autofirmado.
- Por medio de **Seleccionar** se puede seleccionar el certificado a utilizar para EFS o PSD.

Observe que ambas opciones, **Solicitar...** y **Crear** dependen de la política sobre el [*tipo de certificado e inscripción EFS*](#).

Observe que certificados EFS no son utilizados solamente para EFS, sino también para PSD.

Inscriba **certificados para cualquier uso** por medio de la página [*Solicitar un certificado*](#) del asistente para la inicialización de usuarios.

Esto depende de la política [*URL para el comienzo desde el asistente para la inscripción de certificados*](#).

[Más detalles sobre el certificado de inscripción](#)

Elementos de diálogo

Elementos comunes de diálogo	Explicación
<input type="checkbox"/> <i>Mostrar certificados con el objetivo deseado</i>	<p>Seleccione aquí el objetivo desado para filtrar la lista de certificados.</p> <p>Por ejemplo, se pueden mostrar solamente losb certificados de e-mails seguros, o mostrar todos los certificados.</p> <p> En la opción Selección de certificados, la selección esta configurada como <i>Encrypting File System (EFS)</i> y se encuentra deshabilitada. Observe que este parámetro se utiliza tanto para EFS como para PSD.</p>
<input type="checkbox"/> Lista de certificados	<p>Esta lista muestra los certificados en su PC que cumplen con los criterios que ha establecido (por ejemplo, <i>el propósito deseado</i>).</p> <p> Este símbolo se utiliza para certificados que tienen claves privadas accesibles.</p> <p> Este símbolo se utiliza para certificados que ya no tienen claves privadas accesibles.</p> <p> Este símbolo se utiliza si no se sabe si la clave privada de un certificado es accesible o no, por ejemplo, si la clave privada se almacena en una smart card. En este caso introduzca la smart card y seleccione el certificado.</p> <p> Este símbolo se utiliza para los certificados sin su correspondiente clave privada.</p> <p>En la selección de certificado, se muestra en negritas el certificado EFS o PSD que se utiliza actualmente.</p>
<input type="checkbox"/> <i>Ver...</i>	Haga clic aquí para mostrar detalles del certificado seleccionado.
<input type="checkbox"/> <i>Importar...</i>	Haga clic aquí para importar un certificado PKCS

	<p>#12. Se inicia el asistente para la importación de Security Platform PKCS #12. Trusted Platform Module protegerá la clave privada del certificado.</p> <p> Este botón sólo se encuentra activado si la política Permitir la importación de la clave para el usuario lo permite.</p>
<input type="checkbox"/> <i>Clave privada</i>	Si se ha seleccionado un certificado que contiene una clave privada, aquí se muestran las propiedades de dicha clave.
Elementos de diálogo adicionales en el visor de certificados	Explicación
<input checked="" type="checkbox"/> <i>Mostrar certificados de otros proveedores</i>	Tilde esta casilla de verificación para mostrar no sólo los certificados de <i>Infineon TPM Cryptographic Provider</i> , sino también de otros proveedores.
<input checked="" type="checkbox"/> <i>También mostrar los certificados privados &PKCS #11</i>	Al tildar esta casilla de verificación, deberá autenticarse al Security Platform cada vez que el visor de certificados acceda a un certificado privado PKCS #11.
<input type="checkbox"/> <i>Proteger</i>	<p>Haga clic aquí para proteger la clave privada del certificado mediante el Trusted Platform Module.</p> <p> Observe que no puede deshacer la protección de su clave privada. Si desea poder realizar una restauración a la versión no protegida, primero debe exportar el certificado por medio de la ventana de certificados de Microsoft.</p>
<input type="checkbox"/> <i>Borrar</i>	<p>Haga clic aquí para eliminar el certificado seleccionado y su clave privada de su PC.</p> <p>Este botón sólo se encuentra habilitado si EFS o PSD no utilizan el certificado seleccionado, pero su clave privada se encuentra protegida por el Trusted Platform Module.</p>

	 Indique mediante la casilla de verificación si el certificado aún está en uso. De ser así, ya no podrá utilizarlo.
<input type="checkbox"/> <i>Cerrar</i>	Haga clic aquí para cerrar el visor de certificados.
Elementos de diálogo adicionales en la selección de certificados	Explicación
<input type="checkbox"/> <i>Solicitar...</i>	<p>Haga clic aquí para solicitar un certificado de una entidad certificante (CA). Aparecerá un cuadro de diálogo de solicitud de certificado. Siga las indicaciones en pantalla para finalizar el proceso de solicitud del certificado. Luego, cierre la ventana de solicitud del certificado haciendo clic en el botón Cerrar de la barra de título de la ventana.</p> <p> Este botón se encuentra deshabilitado si no hay una dirección Web de solicitud de certificado configurada dentro de los parámetros de la política Inscripción y tipo de certificado EFS.</p>
<input type="checkbox"/> <i>Crear</i>	<p>Haga clic aquí para obtener un certificado de dominio o para crear un certificado autofirmado. El software de la solución Security Platform tratará de obtener un certificado de una entidad certificante de Microsoft (CA, por sus siglas en inglés) dentro de su dominio. Si no hay disponible un dominio de una entidad certificante, se creará un certificado autofirmado.</p> <p> Notas:</p> <ul style="list-style-type: none"> • Dependiendo de los valores de dominio de la entidad certificante, no se podrá obtener el certificado solicitado directamente. Razones posibles: Entidad certificante operada

	<p>manualmente, entrega del certificado por correo. En este caso, consulte a su operador de la entidad certificante respecto de la disponibilidad del certificado.</p> <ul style="list-style-type: none"> • Dependiendo de la política que determina la inscripción y tipo de certificado EFS, puede no estar permitida la creación de certificados autofirmados. Si no hay un dominio de entidad certificante disponible y la política prohíbe los certificados autofirmados, no podrá obtener un certificado por medio de la opción <i>Crear</i>. • La validez de certificados auto-assinados se puede configurar dentro de los parámetros de la política Período de validez dos certificados EFS auto-assinados.
<input type="checkbox"/> <i>Seleccionar</i>	<p>Haga clic aquí para utilizar el certificado seleccionado en la lista de certificados de la ventana para EFS y PSD . La selección de certificados se cierra, volviendo a la página del certificado de encriptación en el asistente para la inicialización de usuarios.</p>
<input type="checkbox"/> <i>Cancelar</i>	<p>Haga click aquí para cerrar la opción Selección de certificados y volver la página del certificado de encriptación del asistente para la inicialización de usuarios, sin cambiar el certificado EFS o PSD.</p>

Inicio de la aplicación

Visor de certificados: Inicie el visor de certificados de Security Platform a través de la herramienta de configuración ([Herramienta de configuración - Configuraciones del usuario - Administrar...](#)).

Selección de certificados: Para iniciar la selección de certificados de Security Platform, haga clic en **Seleccionar...** durante la configuración de la encriptación de archivos y carpetas con EFS o PSD ([Asistente para la inicialización de usuario - Certificado de encriptación](#))



©Infineon Technologies AG

Infineon Solución Security Platform - Asistente para el restablecimiento de la contraseña

Pasar por alto el dispositivo de autenticación

Esta página del asistente no le permite actualizar su dispositivo de autenticación con la nueva frase de contraseña de usuario básico. Esto es de ayuda si su dispositivo de autenticación no funciona o no se encuentra disponible.



Disponibilidad de la página: Esta página sólo se encuentra disponible si configuró la autenticación avanzada.

Página del asistente Elemento	Explicación
<input checked="" type="checkbox"/> <i>Pasar por alto el dispositivo de autenticación</i>	No actualizar su dispositivo con la nueva frase de contraseña de usuario básico. En este caso debe actualizar su dispositivo de autenticación tan pronto como se encuentre nuevamente disponible. Se puede llevar a cabo al reconfigurar la autenticación avanzada en la herramienta de configuración: Herramienta de configuración - Configuraciones del usuario - Configurar...

