

Módulo Safeguard Device Encryption

Prevenga el acceso no autorizado de portátiles y equipos de manera transparente y fácil, con el cifrado de discos. Si un PC cifrado con SafeGuard cae en las manos equivocadas, los datos serán ilegibles, incluso si se extrae el disco duro.

SafeGuard Device Encryption es un módulo de SafeGuard Enterprise, una solución centralizada para administrar la protección de la información en entornos informáticos mixtos. (Consulte la hoja de datos de SafeGuard Enterprise Management Center para obtener información sobre la administración central.)

Cifrado sólido y transparente

- Amplia funcionalidad de cifrado transparente
- Cifrado total del disco duro (NTFS, FAT, FAT32)
- Algoritmos de cifrado estandarizados y sólidos
- Hibernación segura y cifrada
- Los datos cifrados no se pueden leer aunque se extraigan los discos duros de los equipos, excepto si lo hacen los administradores de seguridad
- Algoritmos de cifrado/descifrado de alta velocidad

Autenticación y autorización de inicio seguras

- Autenticación de usuarios previa al arranque, mediante contraseña, token cifrado o tarjeta inteligente, o inicio de sesión biométrico único; acceso al conjunto de claves y acciones de bloqueo del escritorio mediante tokens y tarjetas inteligentes¹
- Inicio de sesión único en el sistema operativo
- Reglas de contraseñas definidas y aplicadas de forma centralizada
- Entorno previo al arranque para múltiples usuarios con pistas de auditoría
- Adición y eliminación dinámica de usuarios registrados del entorno previo al arranque mediante actualizaciones de las políticas
- Proceso de inicio de sesión reforzado para evitar los ataques de interpretación de contraseñas
- Pantalla gráfica de inicio de sesión previa al arranque personalizable y fácil de usar
- Las cuentas de servicios permiten a los administradores acceder de forma segura a los equipos, a la vez que los usuarios finales mantienen su propiedad

Recuperación segura de contraseñas, datos y análisis

Ventajas Claves

- » Seguridad de datos gracias a los algoritmos de cifrado probados, que maximizan la seguridad y el rendimiento
- » Cifrado de archivos de intercambio e hibernación para obtener una seguridad completa
- » Cifrado en segundo plano transparente para el usuario, que garantiza el trabajo sin interrupciones
- » Mayor productividad para el usuario final, gracias a la recuperación segura de la contraseña por teléfono o la opción de auto-ayuda local
- » Comodidad y velocidad para los usuarios finales, gracias a un único inicio de sesión para acceder al sistema operativo desde la etapa previa al arranque
- » Pantalla gráfica de inicio de sesión personalizable y fácil de usar
- » Autenticación biométrica mediante huellas digitales en el momento del arranque; compatible también con tokens y tarjetas inteligentes
- » Seguridad de datos amplia y completa cuando se instala junto con los otros módulos de SafeGuard Enterprise

¹ Consulte el artículo monográfico sobre SafeGuard Enterprise para obtener una lista detallada de las tarjetas inteligentes, tokens y biométricos compatibles, como los lectores de huellas digitales Lenovo.

- Desafíos/respuestas por teléfono con el servicio de asistencia para la recuperación de contraseñas olvidadas
- Función de auto-ayuda local para la recuperación de contraseñas olvidadas durante el momento previo al arranque sin llamadas al servicio de asistencia ni la necesidad de conexión a Internet
- Acceso rápido y seguro a los discos cifrados de otros sistemas para la recuperación o el acceso urgente a los datos, gracias a las reasignaciones automatizadas de claves habilitadas por la administración del conjunto de claves de SafeGuard
- Opción de inicio externo con Windows PE (por ejemplo, para recuperar configuraciones dañadas de sistemas operativos en discos cifrados)
- Compatible con EnCase (Guidance Software), AccessData y Kroll Ontrack (el acceso requiere la cooperación del usuario o administrador)
- Compatibilidad con Microsoft Business Desktop Deployment y Computrace
- Integración con Lenovo Rescue and Recovery para la recuperación segura de sistemas operativos y datos cifrados

Administración centralizada

- Políticas de cifrado aplicadas de forma centralizada
- Información del usuario/ordenador importada mediante la integración con los servicios de directorio (por ejemplo, Microsoft Active Directory)
- Registros detallados para la supervisión del cumplimiento
- Los dispositivos que no se hayan comunicado con el centro de administración durante períodos determinados de tiempo, mientras estén conectados, pueden bloquearse o cerrarse según la política de seguridad establecida
- Comunicación con el SafeGuard Management Center mediante los protocolos XML/SOAP avanzados
- Actividades administrativas automatizadas (por ejemplo, administración de parches) habilitadas por el Wake-On-LAN seguro
- Administración centralizada de claves para el intercambio y recuperación de datos

(Se precisa el módulo SafeGuard Enterprise Management Center para la administración central. Consulte la hoja técnica del producto.)

Instalación fácil y administrada de forma centralizada

- Los paquetes de instalación se pueden distribuir e instalar de forma centralizada y sin supervisión, mediante los paquetes MSI estándar.
- La distribución en red no requiere la participación del usuario.
- Ofrece opciones de cifrado inicial rápido, que permiten cifrar de forma aislada las áreas utilizadas en una partición, lo que acelera el proceso inicial de cifrado/descifrado.

² Para MacOS, consulte la hoja de datos de SafeGuard Disk Encryption para Mac.

Requisitos del sistema

Sistemas operativos²

- » Microsoft Windows 7 (de 32 y 64 bits)
- » Microsoft Windows Vista (32 y 64 bits; SP 1 y SP 2)
- » Microsoft Windows XP (32 bits; SP 2 y SP 3)

Certificaciones

- » Criptografía validada por FIPS 140-2
- » Common Criteria EAL-3+
- » Compatible con Aladdin eToken

Estándares y protocolos

- » Cifrado simétrico: AES de 128/256 bits
- » Cifrado asimétrico: RSA
- » Funciones Hash: SHA-256, SHA-512
- » Hashing de contraseña: PKCS #5 y PKCS #12
- » Tarjeta inteligente/token: PKCS #15, PKCS #11, Microsoft Cryptographic Service Provider (CSP), PC/SC y Kerberos
- » PKI: certificados PKCS #7, PKCS #12 y X.509

Idiomas

- » Español, inglés, francés, alemán, italiano y japonés
- » Compatibilidad de unicode para otros idiomas

Para más información, visite <http://esp.sophos.com>