TREND MICRO™

3.1

TREND MICRO™ Endpoint Encryption

Manual del administrador

Cifrado completo de punto final para datos inactivos



Endpoint Security

Trend Micro Incorporated se reserva el derecho de efectuar cambios en este documento y en el producto que en él se describe sin previo aviso. Antes de instalar y empezar a utilizar el producto, consulte los archivos Léame, las notas de la versión y/o la última versión de la documentación correspondiente que encontrará disponibles en el sitio Web de Trend Micro, en:

http://docs.trendmicro.com/es-es/enterprise/endpoint-encryption.aspx

Trend Micro, el logotipo en forma de pelota de Trend Micro, Endpoint Encryption, PolicyServer, Full Disk Encryption, FileArmor y KeyArmor son marcas registradas o marcas comerciales de Trend Micro Incorporated. El resto de nombres de productos o empresas pueden ser marcas comerciales o marcas comerciales registradas de sus respectivos propietarios.

Copyright © 2012. Trend Micro Incorporated. Reservados todos los derechos.

Nº de documento: APSM35733/121016

Fecha de publicación: Dec 2012

Protegido por las patentes de Estados Unidos: patentes pendientes.

Esta documentación presenta las funciones principales del producto y/o proporciona las instrucciones de instalación para un entorno de producción. Lea la documentación anets de instalar o utilizar el producto.

También podrá encontrar información detallada sobre cómo utilizar funciones específicas del producto en la Ayuda en línea y/o en la Base de conocimientos de Trend Micro en el sitio Web de Trend Micro.

Trend Micro trata constantemente de mejorar la documentación. Si tiene alguna duda, comentario o sugerencia con relación a los documentos de Trend Micro, póngase en contacto con nosotros a través del correo electrónico docs@trendmicro.com.

Valore la documentación en el siguiente sitio Web:

http://www.trendmicro.com/download/documentation/rating.asp

Tabla de contenidos

Prefacio

Prefacio ix

Documentación del producto x

Convenciones del documento x

Audiencia de destino xi

Terminología xii

Acerca de Trend Micro xiv

Capítulo 1: Descripción de Trend Micro Endpoint Encryption

Acerca de Endpoint Encryption 1-2

- Componentes de Endpoint Encryption 1-2
- Requisitos del sistema 1-5

Características y ventajas principales 1-8

Descripción del cifrado 1-9

- Cifrado de archivos 1-10
- Full Disk Encryption 1-10
- Administración de claves 1-11
- Acerca de FIPS 1-11

Administración e integración 1-12

Funciones y autenticación de cuentas 1-12

- Funciones de cuenta 1-12
- Control de acceso por aplicación 1-13
- Opciones de autenticación por aplicación 1-14
- Opciones de Seguridad 1-14
- Métodos de autenticación 1-15

Funciones nuevas en Endpoint Encryption 3.1.3 1-20

- Compatibilidad multilingüe 1-20
- Sincronización de Active Directory 1-21

Mejoras de PolicyServer 3.1.3 1-21
Mejoras de Full Disk Encryption 3.1.3 1-21

Capítulo 2: Introducción a PolicyServer

Autenticación por primera vez 2-2

Introducción a PolicyServer 2-2
Interfaz de la MMC de PolicyServer 2-3

Trabajo con grupos y usuarios 2-4
Definición de usuarios y grupos 2-5
Adición de un grupo superior 2-5
Agregar un nuevo usuario a un grupo 2-7
Agregar un nuevo usuario empresarial 2-9
Agregar un usuario existente a un grupo 2-11

Descripción del control de políticas 2-13
Indicadores visuales de políticas 2-14
Botones y campos de la política 2-14
Modificación de políticas 2-15

Activar aplicaciones 2-17

Capítulo 3: Descripción de políticas

Trabajar con políticas 3-2

Administración de políticas 3-2
Selección de una política para su modificación 3-3
Edición de políticas con intervalos 3-3
Edición de políticas con respuestas de Verdadero/Falso o Sí/No 3-5
Edición de políticas con selección múltiple / selección única 3-7
Edición de políticas con argumentos de cadenas de texto 3-10
Edición de políticas de varias opciones 3-11

Políticas de PolicyServer 3-13
Políticas de consola de administración 3-13
Políticas de administrador 3-14
Políticas de autenticador 3-16
Políticas de alertas del registro 3-17
Políticas de PDA 3-18

Políticas de descarga de Service Pack 3-19
Políticas del mensaje de bienvenida 3-20

Políticas de Full Disk Encryption 3-20
Políticas comunes 3-21
Políticas de PC 3-23
Políticas de PPC 3-27

Políticas de FileArmor 3-30
Políticas de equipos 3-30
Políticas de cifrado 3-30
Políticas de inicio de sesión 3-33
Políticas de contraseña 3-35

Políticas de MobileSentinel 3-36
Políticas comunes 3-36
Políticas de PPC 3-38

Políticas de KeyArmor 3-40
Políticas antivirus 3-41
Políticas de seguridad de KeyArmor 3-41
Políticas de inicio de sesión 3-42
Políticas de mensajes de notificación 3-44
Políticas de conexión de PolicyServer 3-45

Políticas de DriveArmor 3-46
Políticas de autenticación 3-46
Políticas de comunicaciones 3-49
Políticas de dispositivo 3-51

Políticas comunes 3-52
Política de agente 3-52
Políticas de autenticación 3-52

Capítulo 4: Trabajar con grupos, usuarios y dispositivos

Trabajar con grupos 4-2
Adición de un grupo superior 4-2
Agregar un subgrupo 4-4
Modificar un grupo 4-5
Eliminación de un grupo 4-5

Trabajar con grupos sin conexión 4-5
Creación de un grupo sin conexión 4-6
Actualizar un grupo sin conexión 4-9

Trabajar con usuarios 4-10
Agregar usuarios a PolicyServer 4-10
Encontrar un usuario 4-14
Modificación de un usuario 4-15
Ver la pertenencia a grupo de un usuario 4-15
Agregar un nuevo usuario a un grupo 4-16
Agregar un usuario existente a un grupo 4-18
Cambiar el grupo predeterminado de un usuario 4-20
Permitir al usuario instalar en un grupo 4-21
Eliminación de usuarios individuales de un grupo 4-22
Eliminación de todos los usuarios de un grupo 4-22
Restauración de un usuario eliminado 4-23
Trabajar con contraseñas 4-24

Trabajar con dispositivos 4-31
Agregar un dispositivo a un grupo 4-31
Eliminación de un dispositivo de un grupo 4-33
Eliminación de un dispositivo de una empresa 4-34
Ver el contenido del directorio 4-35
Ver atributos del dispositivo 4-35
Ver listado de directorio 4-36
Eliminación de un dispositivo 4-37
Bloqueo de un dispositivo 4-37
Reiniciar un dispositivo 4-38
Restauración de un dispositivo eliminado 4-38

Capítulo 5: Trabajar con Full Disk Encryption

Herramientas de Endpoint Encryption 5-2

Autenticación en el arranque previo de Full Disk Encryption 5-2
Opciones de menú 5-3
Conectividad de red 5-4
Teclado en pantalla 5-4
Cambiar el diseño del teclado 5-4
Cambiar métodos de autenticación 5-5

Cambiar las contraseñas 5-5
Ayuda remota 5-9
Tarjeta inteligente 5-11
Autoayuda 5-13

Conectividad de Full Disk Encryption 5-15
Actualización de clientes de Full Disk Encryption 5-16

Consola de recuperación de Full Disk Encryption 5-16
Acceso a la consola de recuperación 5-18
Acceso a la consola de recuperación desde Windows 5-18
Uso de Descifrar disco 5-19
Montar particiones 5-20
Restaurar arranque 5-21
Administrar usuarios de Full Disk Encryption 5-21
Administrar políticas 5-24
Ver registros 5-24
Configuración de red 5-24

Métodos de recuperación de Full Disk Encryption 5-26

CD de reparación 5-28
Recuperación de datos con el CD de reparación 5-29

Capítulo 6: Trabajar con FileArmor

Autenticación de FileArmor 6-2
Primera autenticación con FileArmor 6-2
Autenticación de dominio de FileArmor 6-3
Autenticación con tarjeta inteligente de FileArmor 6-4
Autenticación por código de color de FileArmor 6-5
Autenticación con PIN de FileArmor 6-5
Cambio de contraseña en FileArmor 6-6
Restablecimiento forzoso de contraseña 6-6

Menú del icono de la bandeja del sistema de FileArmor 6-8
Sincronización con PolicyServer 6-9
Sincronización con archivos sin conexión de PolicyServer 6-10
Cambiar PolicyServer 6-10

Cifrado de FileArmor 6-11
Cifrado de clave local de FileArmor 6-11

Cifrado de clave compartida de FileArmor 6-12
Cifrado de contraseñas fijas de FileArmor 6-13
Cifrado de certificado digital de FileArmor 6-14

Archivar y grabar de FileArmor 6-15
Grabar un archivo con una contraseña fija 6-15
Grabar un archivo con un certificado 6-16

Eliminación segura de FileArmor 6-16

Capítulo 7: Trabajar con KeyArmor

Autenticación en KeyArmor 7-2
Autenticación en KeyArmor por primera vez 7-2
Cambiar métodos de autenticación 7-3
Contraseña fija 7-3

Características de KeyArmor 7-4
Componentes de dispositivos 7-4
Protección de archivos con KeyArmor 7-5
Ninguna información sin controlar 7-5
Actualizaciones y actividad de antivirus de KeyArmor 7-5
Notificación de comprobación de disco de KeyArmor 7-6

Uso de KeyArmor 7-6
Advertencias acerca de dispositivos sin cifrar 7-6
Barra de tareas de KeyArmor 7-7
Menú de KeyArmor 7-8
Protección de archivos con KeyArmor 7-12
Registro de actividad de KeyArmor 7-13
Extraer KeyArmor de forma segura 7-13
Exploración completa de KeyArmor 7-14
Reasignación de un dispositivo KeyArmor a otro usuario 7-16
Añadir de nuevo un KeyArmor eliminado a la empresa 7-18

Capítulo 8: Trabajar con registros e informes

Sucesos del registro 8-2
Administración de sucesos del registro 8-2
Alertas 8-3
Configuración de las alertas de PolicyServer 8-3

Activación de PolicyServer para transmitir SMS y Envío de correo electrónico 8-4

Informes 8-6
Opciones de informes 8-6
Iconos de informes 8-7
Tipos de informes 8-7
Mostrar informes 8-10
Programación de informes 8-11
Mostrar errores de los informes 8-11

Capítulo 9: Obtener asistencia

Comunidad de Trend 9-2

Portal de asistencia 9-2

Ponerse en contacto con el equipo de asistencia técnica 9-3
Resolver problemas de manera más rápida 9-3

TrendLabs 9-4

Apéndice A: ID de mensajes de PolicyServer

Índice

Índice IN-1

Prefacio

Prefacio

Bienvenido al Manual del administrador de Trend Micro™ Endpoint Encryption. En este manual se explican los aspectos principales de Endpoint Encryption: arquitectura de seguridad, cifrado, autenticación y administración de puntos finales. Los temas incluyen cómo usar las aplicaciones de servidores y de clientes de punto final para ayudar a cumplir los objetivos de seguridad, cómo aprovisionar usuarios, grupos y dispositivos para implementar políticas, y cómo usar los informes y registros para analizar la seguridad de la empresa. Además, en este manual también se incluye información sobre la solución de problemas de configuración, el uso de herramientas y la resolución de problemas.

En este prefacio se describen los temas siguientes:

- *Documentación del producto en la página x*
- *Convenciones del documento en la página x*
- *Audiencia de destino en la página xi*
- *Terminología en la página xii*
- *Acerca de Trend Micro en la página xiv*

Documentación del producto

La documentación de Trend Micro Endpoint Encryption incluye lo siguiente:

TABLA 1. La documentación del producto

DOCUMENTO	DESCRIPCIÓN
Manual de instalación	La Guía de instalación describe los requisitos del sistema y contiene instrucciones detalladas acerca de cómo implementar, instalar, migrar y actualizar los clientes de punto final de PolicyServer.
Manual del administrador	La Guía del administrador explica conceptos sobre el producto, características e instrucciones detalladas acerca de cómo configurar y administrar los clientes de punto final de PolicyServer.
Archivo Léame	El archivo Léame contiene la información más reciente del producto no disponible en la documentación impresa o en línea. Entre sus temas se incluyen: una descripción de las nuevas funciones, problemas conocidos y el historial de versiones del producto.
Base de conocimientos	Una base de datos en línea que contiene información para solucionar problemas. Incluye la información más reciente acerca de los problemas conocidos de los productos. Para acceder a la Base de conocimientos, visite el siguiente sitio Web: http://esupport.trendmicro.com

Nota

Toda la documentación está disponible en:

http://docs.trendmicro.com/es-es/home.aspx

Convenciones del documento

La documentación utiliza las siguientes convenciones:

TABLA 2. Convenciones del documento

CONVENCIÓN	DESCRIPCIÓN
MAYÚSCULAS	Acrónimos, abreviaciones y nombres de determinados comandos y teclas del teclado
Negrita	Menús y opciones de menú, botones de comandos, pestañas y opciones
Cursiva	Referencias a otros documentos
`Monoespacio`	Líneas de comandos de ejemplo, código de programa, direcciones URL, nombres de archivos y mensajes del programa
Ruta > **navegación**	La ruta de navegación para llegar a una pantalla determinada Por ejemplo, **Archivo** > **Guardar** significa, haga clic en **Archivo** y, a continuación, haga clic en **Guardar** en la interfaz
Nota	Notas sobre la configuración
Consejo	Recomendaciones o sugerencias
Importante	Información relativa a configuración requerida o predeterminada y limitaciones del producto
¡ADVERTENCIA!	Opciones de configuración y acciones críticas

Audiencia de destino

Esta guía es para los administradores de TI que implementen Trend Micro Endpoint Encryption en medianas y grandes empresas, y para el personal de asistencia técnica que

administra usuarios, grupos, políticas y dispositivos. La documentación presupone unos conocimientos básicos de los dispositivos, las redes y la seguridad, que incluyen:

- Instalación y configuración de hardware del dispositivo
- Partición, formato y mantenimiento del disco duro
- Arquitectura cliente-servidor

Terminología

La tabla siguiente proporciona la terminología utilizada en toda la documentación:

TABLA 3. Terminología de Endpoint Encryption

TÉRMINO	DESCRIPCIÓN
Autenticación	El proceso de identificación de un usuario.
ColorCode™	Una contraseña de secuencia de colores.
Ayuda de la línea de comandos	Cree valores cifrados para proteger las credenciales al crear una secuencia de comandos de instalación.
Ayuda del instalador de la línea de comandos	Cree valores cifrados para proteger las credenciales al generar secuencias de comandos para instalaciones automatizadas.
Dispositivo	Equipo de sobremesa, portátil o medios extraíbles (unidad externa, unidad USB).
Autenticación de dominios	Inicio de sesión único (SSO) con Active Directory.
DriveTrust™	Tecnología de cifrado basada en hardware de Seagate™.
Cliente de punto final	Cualquier dispositivo con una aplicación de Endpoint Encryption instalada.
FileArmor	Cliente de Endpoint Encryption para el cifrado de archivos y carpetas en unidades locales y medios extraíbles.

Término	Descripción
FIPS	Federal Information Processing Standard. Normativas de computación del gobierno federal estadounidense.
Contraseña fija	Una contraseña de usuario estándar formada por letras, números o caracteres especiales.
Full Disk Encryption	Cliente de Endpoint Encryption para el cifrado de hardware y software con autenticación de arranque previo.
KeyArmor	Cliente de Endpoint Encryption para una unidad USB cifrada y protegida con contraseña.
OCSP	El OCSP (protocolo de estado de certificados en línea) es un protocolo de Internet que se usa para certificados digitales X.509.
OPAL	Clase de subsistema de seguridad del Trusted Computing Group para dispositivos cliente.
Contraseña	Un tipo de datos de autenticación, como fija PIN y código de color.
PolicyServer	El servidor de administración central que implementa políticas de autenticación y cifrado en los clientes de punto final (Full Disk Encryption, FileArmor, KeyArmor).
SED	Cifrado de dispositivo seguro. Un disco duro u otro dispositivo, que está cifrado.
Tarjeta inteligente	Una tarjeta física que se utiliza junto con un PIN o una contraseña fija.
PIN	Un número de identificación personal, que suele utilizarse para las transacciones de ATM.
Consola de recuperación	Sirve para recuperar un dispositivo en caso de error del sistema operativo principal, solucionar problemas de red y administrar usuarios, políticas y registros.
Ayuda remota	Autenticación interactiva para usuarios que olvidan sus credenciales o para dispositivos que no han sincronizado sus políticas en un plazo de tiempo predeterminado.

TÉRMINO	DESCRIPCIÓN
CD de reparación	Use este CD de arranque para descifrar la unidad antes de la eliminación de Full Disk Encryption en caso de que el disco resulte dañado.
RSA SecurID	Mecanismo para realizar la autenticación de dos factores para un usuario en un recurso de red.
Autoayuda	Combinaciones de preguntas y respuestas que permiten a los usuarios restablecer una contraseña olvidada sin ponerse en contacto con el servicio de asistencia.

Acerca de Trend Micro

Como líder mundial en seguridad en Internet, Trend Micro desarrolla soluciones de contenido de Internet y gestión de amenazas para crear un mundo seguro para el intercambio de información digital a nivel empresarial y de consumidores. Con más de 20 años de experiencia, Trend Micro proporciona soluciones del más alto nivel para clientes, servidores e Internet que detienen las amenazas más rápidamente y protege los datos en entornos físicos, virtualizados y de Internet.

Mientras siguen apareciendo nuevas amenazas y vulnerabilidades, Trend Micro mantiene su compromiso de ayudar a los clientes a proteger sus datos, a garantizar la conformidad, a reducir los costes y a proteger la integridad empresarial. Para obtener más información, visite:

http://www.trendmicro.com

Trend Micro y el logotipo en forma de pelota de Trend Micro son marcas comerciales de Trend Micro Incorporated y están registradas en algunas jurisdicciones. El resto de marcas son marcas comerciales o marcas registradas de sus respectivas compañías.

Capítulo 1

Descripción de Trend Micro Endpoint Encryption

Trend Micro™ Endpoint Encryption proporciona una sólida protección de los datos y un control de dispositivos para una amplia gama de dispositivos, incluidos equipos portátiles, equipos de sobremesa, tabletas, CD, DVD, unidades de USB y otros medios extraíbles.

En este capítulo se describen los siguientes temas:

- *Acerca de Endpoint Encryption en la página 1-2*
- *Características y ventajas principales en la página 1-8*
- *Descripción del cifrado en la página 1-9*
- *Requisitos del sistema en la página 1-5*
- *Funciones y autenticación de cuentas en la página 1-12*
- *Funciones nuevas en Endpoint Encryption 3.1.3 en la página 1-20*

Acerca de Endpoint Encryption

Trend Micro Endpoint Encryption es una solución de cifrado basada en hardware y en software totalmente integrada para proteger equipos portátiles y de sobremesa, archivos y carpetas, medios extraíbles y unidades USB cifradas con protección antimalware y antivirus incrustada. Con Endpoint Encryption, los administradores pueden utilizar una única consola de administración para administrar con flexibilidad una combinación de cifrado basado en software y hardware con total transparencia para los usuarios finales.

Trend Micro Endpoint Encryption garantiza la protección de datos de principio a fin mediante un cifrado de nivel FIPS 140-2 de los datos que residen en el servidor de administración, de todos los datos transmitidos al servidor y desde este, de todos los datos almacenados en el dispositivo de punto final y de todos los registros de cliente almacenados localmente.

Gracias a la criptografía acreditada FIPS 140-2, Endpoint Encryption ofrece la siguientes ventajas:

- Amplia protección de los datos gracias al cifrado completo totalmente integrado de discos, archivos, carpetas, unidades USB y medios extraíbles.
- Administración centralizada de políticas y claves mediante un único servidor y consola de administración.
- Administración de dispositivos mediante la recopilación de información específica del dispositivo, bloqueo y reinicio remotos y la capacidad de borrar todos los datos de punto final.
- Opciones avanzadas de creación de informes y auditoría en tiempo real para garantizar el cumplimiento de las normas de seguridad.

Componentes de Endpoint Encryption

Endpoint Encryption consta de un servidor de administración central (servicio Web de PolicyServer) que administra las bases de datos de políticas y registros (MobileArmor DB), la autenticación LDAP con Active Directory y todas las actividades cliente-servidor. Los clientes de Endpoint Encryption no pueden interactuar directamente con PolicyServer y se deben conectar a través del servicio Web del cliente. Para obtener una

ilustración de esta arquitectura, consulte *Figura 1-1: Arquitectura cliente-servidor de Endpoint Encryption en la página 1-3*.

Nota

La configuración del puerto para todo el tráfico HTTP se puede definir en el momento de la instalación o a través de la configuración del cliente de Endpoint Encryption.

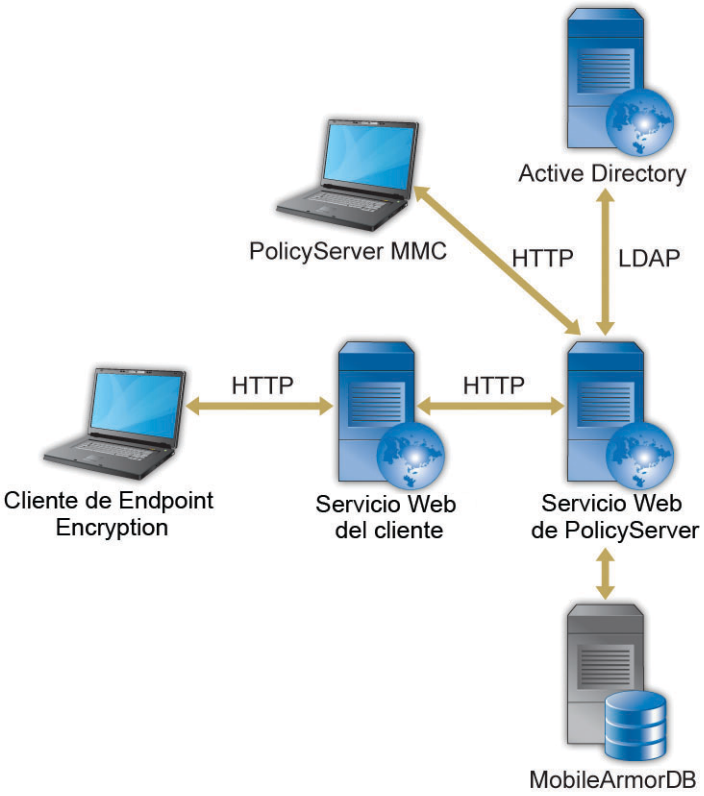


FIGURA 1-1. Arquitectura cliente-servidor de Endpoint Encryption

La siguiente tabla describe estos componentes.

TABLA 1-1. Componentes de Endpoint Encryption

COMPONENTE	DESCRIPCIÓN
Servicio Web de PolicyServer	El servicio Web de IIS que ofrece gestión centralizada para la administración, autenticación y creación de informes de políticas.
PolicyServer MMC	Microsoft™ Management Console (MMC) de PolicyServer es la interfaz que se utiliza para controlar PolicyServer.
Cliente de Endpoint Encryption	Un cliente de Endpoint Encryption es cualquier dispositivo con Full Disk Encryption, FileArmor o KeyArmor instalado. • Full Disk Encryption proporciona cifrado de disco completo basado en hardware y software, así como la autenticación de arranque previo. • FileArmor proporciona cifrado para el contenido de archivos y carpetas en unidades locales y medios extraíbles. • KeyArmor es una unidad USB cifrada y potente con protección antivirus integrada.
MobileArmorDB	La base de datos de Microsoft™ SQL Server almacena toda la información de usuarios, políticas y registros.
Active Directory	El servicio Web de PolicyServer sincroniza la información de cuenta del usuario comunicándose con Active Directory mediante LDAP. La información de la cuenta se almacena en la memoria caché de forma local en MobileArmorDB. **Nota** Active Directory es opcional.
Servicio Web del cliente	El servicio Web de IIS que los clientes de Endpoint Encryption utilizan para comunicarse con el servicio Web de PolicyServer.

Requisitos del sistema

Las siguientes tablas proporcionan información general sobre los requisitos del sistema de Endpoint Encryption.

TABLA 1-2. Requisitos de hardware de PolicyServer

HOSTS INDEPENDIENTES		HOST ÚNICO
Host de PolicyServer (3.000 usuarios)	Host de SQL Server (3.000 usuarios)	PolicyServer y SQL Server (1.500 usuarios)
• Procesadores duales Intel™ Xeon™ Quad Core Core2 de 2 GHz • 4GB RAM • Espacio en disco duro de 40 GB	• Procesadores duales Intel™ Xeon™ Quad Core Core2 de 2 GHz • 8GB RAM • Espacio en disco duro de 100GB	• Procesadores Intel™ Xeon™ Quad Core Core2 de 2 GHz • 8GB RAM • Espacio en disco duro de 120GB

TABLA 1-3. Requisitos mínimos de software de PolicyServer

FUNCIÓN	REQUISITO
Sistema operativo	• Windows Server 2003 SP2 de 32/64 bits • Windows Server 2008 o 2008 R2 de 64 bits

Aplicaciones y configuración	• Servidor de aplicaciones
	  • IIS
	  • Permitir las páginas Active Server
	  • Permitir ASP.NET
	• .Net Framework 2.0 SP2
	
	Nota
	PolicyServer 3.1.3 requiere dos ubicaciones de IIS. La interfaz de administración de PolicyServer y la interfaz de aplicación cliente deben estar instaladas en diferentes ubicaciones de IIS.

Función	Requisito
Base de datos	• Microsoft SQL 2005/2008/2008 R2 • Microsoft SQL Express 2005(SP3)/2008 • Autenticación de modo mixto (contraseña de SA) instalada • Servicios de creación de informes instalados

Tabla 1-4. Requisitos del sistema de Full Disk Encryption

Evento	Requisito
Procesador	Intel™ Core™ 2 o procesador compatible.
Memoria	• Mínimo: 1GB
Espacio en disco	• Mínimo: 30GB • Necesario: 20% de espacio libre en disco • Necesario: Espacio libre contiguo de 256MB
Conectividad de red	Es necesaria la comunicación con PolicyServer 3.1.3 para las instalaciones administradas
Sistemas operativos	• Windows 8™ (32 o 64 bits) • Windows 7™ (32 o 64 bits) • Windows Vista™ con SP1 (32 o 64 bits) • Windows XP™ con SP3 (32 bits)

EVENTO	REQUISITO
Otro software	Requisitos adicionales para Windows 8: • Microsoft .NET Framework 3.5 está activado • Para dispositivos con UEFI, consulte la Guía de instalación de Endpoint Encryption para obtener instrucciones sobre cómo cambiar la prioridad de arranque. Requisitos adicionales para Windows XP: • Microsoft .NET Framework 2.0 SP1 o versión posterior • Microsoft Windows Installer 3.1
Disco duro	• Unidades DriveTrust de Seagate • Unidades Seagate OPAL y OPAL 2 **Nota** • Los discos RAID y SCSI no son compatibles. • Full Disk Encryption para Windows 8 no es compatible con las unidades RAID, SCSI, eDrive y OPAL 2.
Otro hardware	El controlador de disco duro ATA, AHCI o IRRT.

TABLA 1-5. Requisitos del sistema de FileArmor

EVENTO	REQUISITO
Procesador	Intel™ Core™ 2 o procesador compatible.
Memoria	• Mínimo: 512MB • Recomendado: 1GB
Espacio en disco	• Mínimo: 2GB • Necesario: 20% de espacio libre en disco
Conectividad de red	Comunicación con los PolicyServer necesarios para las instalaciones administradas

EVENTO	REQUISITO
Sistemas operativos	• Windows 8™ (32 o 64 bits) • Windows 7™ (32 o 64 bits) • Windows Vista™ con SP1 (32 o 64 bits) • Windows XP™ con SP3 (32 bits)
Otro software	Requisitos adicionales para Windows 8: • Microsoft .NET Framework 3.5 está activado • Para dispositivos con UEFI, consulte la Guía de instalación de Endpoint Encryption para obtener instrucciones sobre cómo cambiar la prioridad de arranque. Requisitos adicionales para Windows XP: • Microsoft .NET Framework 2.0 SP1 o versión posterior • Microsoft Windows Installer 3.1

TABLA 1-6. Requisitos del sistema de KeyArmor

EVENTO	REQUISITO
Hardware	Puerto USB 2.0
Conectividad de red	Comunicación con los PolicyServer necesarios para las instalaciones administradas
Sistemas operativos	• Windows 7™ (32 o 64 bits) • Windows Vista™ con SP1 (32 o 64 bits) • Windows XP™ con SP3 (32 bits)
Otro software	Software adicional necesario al instalar en Windows XP™: • Microsoft .NET Framework 2.0 SP1 o versión posterior

Características y ventajas principales

Endpoint Encryption ofrece las siguientes características y ventajas principales:

TABLA 1-7. Características principales de Endpoint Encryption

CARACTERÍSTICA	VENTAJAS
Cifrado	• Protección para el disco completo, incluido el registro de arranque maestro (MBR), el sistema operativo y todos los archivos de sistema. • Cifrado basado en hardware y software para entornos mixtos.
Autenticación	• Métodos de autenticación flexible, incluida la autenticación de uno y varios factores. • Actualizaciones de políticas antes de la autenticación y el arranque del sistema. • Acciones configurables cuando se alcanza el número de intentos de contraseña fallidos.
Administración de dispositivos	• Políticas para proteger los datos de equipos, portátiles, tabletas, unidades USB, CD y DVD. • Posibilidad de bloquear, borrar o eliminar un dispositivo de forma remota.
Administración central	• Control total sobre el cifrado, la supervisión y la protección de los datos. • Aplicación automatizada de políticas con corrección de los sucesos de seguridad.
Mantenimiento de registros, informes y auditorías	• Análisis de las estadísticas de uso con informes programados y notificaciones de alerta.

Descripción del cifrado

Cifrado es el proceso de hacer que los datos sean ilegibles si no se tiene acceso a la clave de cifrado. El cifrado se puede realizar mediante software o hardware (o una combinación de ambos) para garantizar que los datos estén protegidos localmente en un dispositivo, en un medio extraíble, en archivos y carpetas específicos, y los datos que circulan por las redes o por Internet. El cifrado de punto final es la principal manera de

asegurar los datos y garantizar el cumplimiento de las normas relativas a la protección de datos.

Cifrado de archivos

FileArmor protege los archivos y carpetas individuales en discos duros y dispositivos de medios extraíbles (unidades USB). Los administradores pueden configurar políticas que especifiquen las carpetas y unidades que se cifrarán en el dispositivo y políticas sobre los datos cifrados en los medios extraíbles. El cifrado de archivos y carpetas se realiza después de llevarse a cabo la autenticación.

FileArmor también puede proteger archivos diferentes con claves diferentes, lo que permite a los administradores configurar políticas de acceso a un dispositivo y políticas independientes para acceder a determinados archivos. Esto resulta útil en entornos en los que varios usuarios acceden a un punto final.

Full Disk Encryption

El cifrado de disco completo es la solución de cifrado que se implementa con más frecuencia en los puntos finales en la actualidad porque protege todos los datos de la unidad, incluidos los archivos de sistema operativo, de programa, temporales y de usuario final. Muchas aplicaciones de cifrado de disco completo también mejoran la seguridad del sistema operativo haciendo que el usuario se autentique antes de iniciar o desbloquear la unidad y proporcionar acceso al sistema operativo.

Como solución de cifrado, Trend Micro Full Disk Encryption ofrece cifrado basado tanto en software como en hardware. Aunque el cifrado basado en hardware es más sencillo de implementar en hardware nuevo, más fácil de mantener y ofrece un mayor grado de rendimiento, el cifrado basado en software no requiere ningún hardware y es más económico de implementar en los puntos finales existentes. Trend Micro PolicyServer puede administrar Full Disk Encryption centralmente y ofrece a las organizaciones la flexibilidad de usar dispositivos con cifrado basado en software o hardware según necesiten.

Una característica de red exclusiva de Endpoint Encryption actualiza las políticas en tiempo real antes de permitir la autenticación. Endpoint Encryption también permite a

los administradores bloquear o borrar una unidad antes de que se pueda acceder al sistema operativo (y los datos confidenciales).

Administración de claves

Los productos de cifrado no administrado requieren que los administradores o usuarios realicen un seguimiento de la clave de cifrado en un dispositivo USB. Endpoint Encryption protege y custodia las claves de cifrado de forma transparente, al tiempo que permite a un administrador utilizar una clave para iniciar sesión en el dispositivo protegido para recuperar los datos protegidos.

Las unidades flash USB de KeyArmor protegen los datos con cifrado de hardware siempre activado y protección antivirus y antimalware integrada para satisfacer los requisitos de cumplimiento y las estrictas normas gubernamentales. Con KeyArmor, los administradores tienen visibilidad y control total de quién, cuándo, dónde y cómo se utilizan las unidades flash USB en su organización.

Acerca de FIPS

Federal Information Processing Standard (FIPS) Publication 140-2 es un estándar para la seguridad de los dispositivos del gobierno de Estados Unidos que especifica los requisitos de seguridad de los módulos de cifrado. FIPS 140-2 incluye cuatro niveles de seguridad:

TABLA 1-8. Niveles de seguridad de FIPS 140-2

NIVEL	DESCRIPCIÓN
Nivel 1	Requiere que todos los componentes de cifrado hayan sido diseñados para producción y no presenten agujeros de seguridad.
Nivel 2	Incluye los requisitos del nivel 1 además de evidencias de manipulación física y autenticación basada en la función.
Nivel 3	Incluye los requisitos del nivel 2 además de resistencia a la manipulación física y autenticación basada en la identidad.
Nivel 4	Incluye los requisitos del nivel 3 además de requisitos de seguridad física adicionales.

Endpoint Encryption garantiza una protección de los datos de principio a fin mediante un cifrado de nivel FIPS 140-2 de los datos que residen en PolicyServer, de todos los datos transmitidos entre PolicyServer y los clientes de punto final, de todos los datos almacenados en el dispositivo de punto final y de todos los registros de cliente almacenados localmente.

Administración e integración

Cuando los usuarios finales requieren protección de datos reforzada en varios tipos de dispositivos, que podrían necesitar tipos de cifrado diferentes, una solución Endpoint Encryption integrada y administrada centralmente reduce los costes de administración y mantenimiento. Endpoint Encryption es una solución administrada centralmente que permite las siguientes funciones de protección de datos:

- Actualización de manera centralizada y transparente de los clientes de Endpoint Encryption cuando se publican nuevas versiones
- Administración y aprovechamiento de las políticas de seguridad de personas y grupos desde un único servidor de políticas
- Control de seguridad de contraseñas y regularidad de cambios de contraseña
- Actualización de las directivas de seguridad en tiempo real previa a la autenticación para revocar las credenciales de usuario antes de iniciar el sistema operativo

Funciones y autenticación de cuentas

Trend Micro Endpoint Encryption ofrece a los administradores una serie de funciones de cuenta y métodos de autenticación dependiendo de sus necesidades específicas, incluida la autenticación de varios factores.

Funciones de cuenta

Endpoint Encryption incluye diferentes tipos de cuenta diseñados para las diferentes funciones de la empresa. Estas funciones determinan cómo las cuentas acceden y realizan diferentes tareas.

TABLA 1-9. Funciones de cuenta de Endpoint Encryption

FUNCIONES	DESCRIPCIÓN
Administrador de empresa	Controla toda la empresa y tiene derechos administrativos en todos los grupos, usuarios, dispositivos y políticas independientemente de dónde se encuentren dentro de la empresa.
Administrador de grupo	Derechos administrativos en cualquier grupo y sus subgrupos a los que esté asignado. **Nota** Los derechos no se aplican a grupos primarios, grupos del mismo nivel en la jerarquía o sus subgrupos.
Autenticador de empresa	Diseñado para que el personal de asistencia técnica proporcione asistencia remota. Esto puede ocurrir cuando un usuario tiene que llamar al servicio técnico porque olvidó su contraseña o tiene un problema técnico. Los autenticadores de empresa tienen privilegios configurables en toda la empresa.
Autenticador de grupo	Similar al autenticador de empresa, pero limitado únicamente al nivel de grupo.
Usuario	Para los usuarios finales que utilizan los clientes de punto final pero que no están asignados a responsabilidades de administrador o autenticador.

Control de acceso por aplicación

La autenticación y el control del acceso son importantes en cualquier empresa. Full Disk Encryption limita el acceso al sistema en el arranque y el acceso a archivos y carpetas una vez que el usuario ha iniciado sesión en el sistema operativo. FileArmor, KeyArmor y PolicyServer proporcionan el mismo nivel de seguridad y control de acceso mediante autenticación de dos factores.

Cada aplicación de Endpoint Encryption ofrece características y niveles de control únicos.

TABLA 1-10. Control de autenticación por aplicación

APLICACIÓN	CONTROL
PolicyServer	Acceso de la aplicación a la consola de administración.
Full Disk Encryption	Control de autenticación antes de iniciar Windows.
FileArmor	Control de acceso a archivos y carpetas una vez se está en el sistema operativo.
KeyArmor	Control de dispositivos para el acceso a contenido cifrado en dispositivos extraíbles.

Opciones de autenticación por aplicación

TABLA 1-11. Opciones de autenticación disponibles para clientes de punto final

PRODUCTO	OPCIONES DE AUTENTICACIÓN					
	CONTRASEÑA FIJA	CONTRASEÑA DE DOMINIO	TARJETA INTELIGENTE	PIN	RSA	COLORCODE
PolicyServer	Sí	Sí	Sí	No	No	No
Full Disk Encryption	Sí	Sí	Sí	Sí	No	Sí
FileArmor	Sí	Sí	Sí	Sí	No	Sí
KeyArmor	Sí	No	Sí	Sí	Sí	Sí

Opciones de Seguridad

Si un usuario no puede autenticarse, se le pide que vuelva a introducir sus credenciales. En función de la configuración de las políticas, demasiados intentos consecutivos de autentificación harán que el cliente exceda el tiempo de espera, se bloquee o se borren todos los datos del punto final.

TABLA 1-12. Opciones de seguridad de autenticación

OPCIÓN DE SEGURIDAD	DESCRIPCIÓN
Demora de tiempo	El dispositivo está bloqueado y no se pueden realizar intentos de autenticación hasta que transcurra el tiempo de bloqueo. • Asegúrese de que las credenciales son correctas • Utilice la autoayuda (si está disponible) para evitar esperar el tiempo de demora.
Requiere autenticación remota	El dispositivo está bloqueado. • Asegúrese de que las credenciales son correctas. • Póngase en contacto con el administrador para usar Ayuda remota y desbloquear el dispositivo. Para conocer más detalles, consulte *Ayuda remota en la página 1-19*.
Borrar el dispositivo	Se eliminan todos los datos del dispositivo.

Métodos de autenticación

Endpoint Encryption ofrece varios métodos de autenticación. PolicyServer determina los métodos específicos disponibles para el cliente de punto final.

TABLA 1-13. Métodos de autenticación compatibles

TIPO DE AUTENTICACIÓN	DESCRIPCIÓN
Autenticación de dominios	Inicio de sesión único (SSO) con Active Directory.
Contraseña fija	Una cadena de caracteres, número y símbolos.
PIN	Un número de identificación personal.
ColorCode™	Utilice una secuencia de colores como una contraseña.
Tarjeta inteligente	Una tarjeta física que se utiliza junto con un PIN o una contraseña fija.

Tipo de autenticación	Descripción
Autoayuda	Combinaciones de preguntas y respuestas que permiten a los usuarios restablecer una contraseña olvidada sin ponerse en contacto con el servicio de asistencia.
Ayuda remota	Autenticación interactiva para usuarios que olvidan sus credenciales o para dispositivos que no han sincronizado sus políticas en un plazo de tiempo predeterminado.

Autenticación de dominios

La autenticación de dominios con Active Directory permite el inicio de sesión único (Single Sign-On, SSO). Los usuarios solo tienen que proporcionar las credenciales una vez para autenticarse en Full Disk Encryption, iniciar sesión en Windows y acceder a FileArmor.

Requisitos previos

Para una integración sin problemas, asegúrese de que se cumplen los requisitos siguientes:

- Todos los dispositivos están en el mismo dominio que PolicyServer.
- El nombre de usuario configurado en Active Directory coincide exactamente con el de PolicyServer, incluidas las mayúsculas y minúsculas.
- El nombre de usuario se encuentra dentro de un grupo de PolicyServer y la política Autenticación de dominio está establecida en **Sí**.
- Las políticas **Común** > **Inicio de sesión de red** (nombre de host, nombre de dominio) están correctamente configuradas en la configuración del servidor de LDAP o Active Directory.



Nota

Para obtener más información acerca de cómo configurar LDAP y Active Directory, consulte *Sincronización de Active Directory en la página 1-21*.

Contraseñas fijas

Las contraseñas fijas son el método de autenticación más común. El usuario crea una contraseña fija y puede ser casi cualquier combinación. Los administradores pueden poner restricciones a las contraseñas fijas para asegurarse de que no se interceptarán con facilidad.

PIN

Los números de identificación personal (PIN) son otro método común de identificación. Al igual que la contraseña fija, el usuario crea un PIN y puede ser casi cualquier combinación. Al igual que las contraseñas fijas, los administradores pueden poner restricciones a la combinación PIN.

ColorCode

ColorCode™ es un método de autenticación diseñado para ser recordado fácilmente. En lugar de utilizar números o letras para una contraseña, la autenticación por código de

color consta de una secuencia de colores creada por el usuario (por ejemplo: rojo, rojo, azul, amarillo, azul y verde).



FIGURA 1-2. Inicio de sesión de ColorCode

Tarjeta inteligente

La autenticación de tarjetas inteligentes requiere tanto un PIN como una tarjeta física para confirmar la identidad de un usuario. Inserte la tarjeta inteligente antes de proporcionar un PIN.

Importante

Para activar la autenticación de tarjetas inteligentes para todos los clientes de Endpoint Encryption, habilite la siguiente política: **Full Disk Encryption** > **Equipo** > **Iniciar sesión** > **Autenticación de símbolo**.

Autoayuda

Utilice la autoayuda para autenticar cuando los usuarios han olvidado sus credenciales. La autoayuda requiere que los usuarios respondan a las preguntas personales predefinidas. La autoayuda también se puede utilizar en lugar de la contraseña fija o de otros métodos de autenticación.

Importante

PolicyServer debe configurarse para poder utilizar la autenticación de autoayuda. Para obtener más información, consulte *Descripción de políticas en la página 3-1*.

¡ADVERTENCIA!

Se puede mostrar un máximo de seis preguntas para clientes de punto final. No cree más de seis preguntas en PolicyServer o de lo contrario los usuarios no podrán iniciar sesión.

Ayuda remota

Utilice Ayuda remota cuando un usuario se bloquea en un cliente de punto final debido a que se han realizado demasiados intentos de inicio de sesión fallidos o porque el período comprendido desde la última sincronización de PolicyServer ha sido demasiado largo.

En cada política de la aplicación, establezca la acción en **Autenticación remota**.

TABLA 1-14. Políticas que afectan a la autenticación remota

POLÍTICA	DESCRIPCIÓN
Iniciar sesión > **Período de bloqueo de cuenta**	Número de días que un dispositivo no se puede comunicar con PolicyServer antes de llamar a una acción de bloqueo de cuenta.
Iniciar sesión > **Acción de bloqueo de cuenta**	Acción que tiene lugar cuando transcurre el período de bloqueo de cuenta. Las acciones de bloqueo de cuenta son: borrar, autenticación remota.

Política	Descripción
Iniciar sesión > **Intentos de inicio de sesión fallidos permitidos**	Número de intentos de inicio de sesión fallidos que se permiten antes de ejecutar la acción definida en Acción de dispositivo bloqueado
Iniciar sesión > **Acción de dispositivo bloqueado**	Acción que tiene lugar cuando se excede el valor de la política Intentos de inicio de sesión fallidos permitidos. Las acciones incluyen: tiempo de demora, borrar, autenticación remota.

Funciones nuevas en Endpoint Encryption 3.1.3

Trend Micro Endpoint Encryption 3.1.3 incluye las siguientes mejoras:

Compatibilidad multilingüe

Endpoint Encryption ahora ofrece compatibilidad para los siguientes idiomas:

Tabla 1-15. Idiomas admitidos

Producto	Idiomas		
	Español	Francés	Alemán
Full Disk Encryption	Sí	Sí	Sí
FileArmor	Sí	Sí	Sí
PolicyServer	Sí	Sí	Sí
KeyArmor	No	No	No

Sincronización de Active Directory

Endpoint Encryption ahora admite la sincronización de cuentas entre Active Directory y PolicyServer. Active Directory se puede utilizar para inicio de sesión único en todas las aplicaciones cliente de punto final.

Consulte la Guía de instalación de Endpoint Encryption para obtener información detallada sobre cómo configurar PolicyServer para la sincronización con AD. La Guía de instalación está disponible en:

http://docs.trendmicro.com/es-es/enterprise/endpoint-encryption.aspx

Mejoras de PolicyServer 3.1.3

- El instalador de PolicyServer incluye ahora una licencia de prueba que caduca a los 30 días. El nombre de empresa y la cuenta de administrador de empresa se configuran durante la instalación.
- El número de puerto para los servicios Web ahora se puede establecer durante la instalación.
- Para mejorar la seguridad, PolicyServer dispone ahora de un servicio Web del cliente que todos los clientes pueden utilizar para conectarse a PolicyServer.
- Mejora de las búsquedas y asignación nombres de políticas.
- Mejora de los registros de auditoría.
- Un nuevo nodo de la Papelera de reciclaje permite a los administradores recuperar los usuarios y dispositivos eliminados.
- Las políticas globales permiten que los cambios en las políticas se transfieran fácilmente a los subgrupos desde el nivel principal.

Mejoras de Full Disk Encryption 3.1.3

Nuevas funciones

- Ahora es compatible con OPAL 2

- Windows 8 ahora es compatible con dispositivos que no son UEFI
- Las políticas ahora se sincronizan automáticamente con PolicyServer cuando un dispositivo carga el inicio de sesión de arranque previo
- Ahora se admite el uso compartido de contraseñas entre dispositivos del mismo grupo de PolicyServer (para dispositivos que compartan contraseñas)
- Las instalaciones no administradas admiten ahora cifrado por hardware y software en su totalidad
- El arranque previo basado en consola ahora funciona con las configuraciones de pantalla no compatibles

Instalación más sencilla

- Ahora hay un instalador para el cifrado basado en software y hardware (Seagate OPAL y DriveTrust). Este mismo instalador es compatible también con instalaciones de SO de 32 y 64 bits
- Comprobación previa a la instalación mejorada e informes de error y registro
- Full Disk Encryption ahora puede instalarse sin cifrado y sin necesidad de arranque previo (mediante el ajuste de política). De esta forma se logra un mejor control de las fases de implementación para distribuir el software, permitir la autenticación durante el arranque previo y activar el cifrado

Mejora de la gestión y la administración

- Acceso a la consola de recuperación desde Windows y en el arranque previo
- Actualice fácilmente la información de PolicyServer y reasigne un dispositivo al PolicyServer original o a un nuevo PolicyServer
- CD de reparación más robusto
- Desinstalaciones mediante secuencia de comandos

Capítulo 2

Introducción a PolicyServer

Antes de configurar PolicyServer para administrar de forma centralizada los clientes de punto final, es necesario tener ya instalados los servicios y las bases de datos de PolicyServer, y MMC de PolicyServer. Consulte la Guía de instalación de Endpoint Encryption para obtener información detallada sobre cómo configurar los servicios, las bases de datos y MMC de PolicyServer. La Guía de instalación está disponible en:

http://docs.trendmicro.com/es-es/enterprise/endpoint-encryption.aspx

En este capítulo se describen los siguientes temas:

- *Autenticación por primera vez en la página 2-2*
- *Introducción a PolicyServer en la página 2-2*
- *Trabajo con grupos y usuarios en la página 2-4*
- *Descripción del control de políticas en la página 2-13*
- *Activar aplicaciones en la página 2-17*

Autenticación por primera vez

El nombre de empresa y la cuenta de administrador de empresa se configuraron durante la instalación. PolicyServer funciona normalmente con todas las aplicaciones cliente, con un número ilimitado de dispositivos y con 100 usuarios durante un período de prueba de 30 días. Transcurridos los 30 días, hay que ponerse en contacto con el servicio de asistencia técnica para recibir un archivo de licencia. No obstante, los usuarios/dispositivos podrán seguir iniciando sesión una vez finalizado el período de prueba.

En esta tarea se explica cómo importar el archivo de licencia y cómo iniciar sesión en PolicyServer. Generalmente, se trata de un archivo de texto.

Procedimiento

1. Abra la MMC de PolicyServer.
2. Vaya a **Archivo** > **Importar licencia**.
3. Escriba el código de desbloqueo del archivo de licencia.
4. Busque el archivo de licencia y, a continuación, haga clic en **Actualizar**.
5. Indique la empresa, el nombre de usuario, la contraseña y la dirección IP o nombre de host de PolicyServer especificados en el archivo de licencia.
6. Haga clic en **Iniciar sesión**.

Introducción a PolicyServer

PolicyServer usa Microsoft Management Console (MMC). PolicyServer tiene una estructura jerárquica que distribuye la responsabilidad administrativa al tiempo que mantiene un control centralizado para:

- Definir parámetros de políticas de seguridad
- Administrar usuarios, dispositivos y grupos (incluidos los grupos sin conexión)
- Activar o desactivar aplicaciones de punto final

Use las funciones de auditoría y creación de informes de la MMC de PolicyServer para supervisar la infraestructura de la seguridad y cumplir los requisitos de conformidad.

Interfaz de la MMC de PolicyServer

La interfaz de la MMC de PolicyServer contiene los siguientes paneles:

TABLA 2-1. Interfaz de la MMC de PolicyServer

VENTANA	DESCRIPCIÓN
Panel izquierdo (1)	Utilice el panel izquierdo para ver usuarios, grupos, políticas, dispositivos y aplicaciones. Expanda el nivel superior para administrar los elementos anidados en la estructura de árbol. Al abrir los elementos se actualizará el contenido en la ventana de resultados.
Panel derecho (2)	Utilice el panel derecho para modificar políticas, información del usuario e información del grupo. El elemento del árbol actualmente seleccionado se muestra en la ventana de resultados. El formato exacto de la información mostrada en la ventana de resultados depende del elemento seleccionado en el árbol.



FIGURA 2-1. Interfaz de la MMC de PolicyServer

Dentro de la estructura de árbol del panel izquierdo, existen diferentes nodos. La siguiente tabla describe cada nodo:

TABLA 2-2. Jerarquía de la estructura de árbol de la MMC de PolicyServer

NODO	OBJETIVO
Usuarios empresariales	Ver todos los administradores, autenticadores y usuarios en toda la empresa. Para ver los afiliados a un grupo, abra el grupo y haga clic en **Usuarios**.
Dispositivos empresariales	Ver todas las instancias de clientes de punto final y desde qué dispositivo se están conectando. Para ver los afiliados a un grupo, abra el grupo y haga clic en **Dispositivos**.
Políticas empresariales	Controla si las aplicaciones finales pueden conectarse a PolicyServer. Además, administra todas las políticas de la empresa. Las políticas de grupo sobrescriben las políticas empresariales.
Registros de sucesos de la empresa	Ver todas las entradas del registro para la empresa.
Informes empresariales	Administrar diversos informes y alertas. No existen informes disponibles en el nivel de grupo.
Mantenimiento empresarial	Administrar complementos de la aplicación MMC de PolicyServer.
Papelera de reciclaje	Ver usuarios y dispositivos eliminados.
Grupos	Administrar usuarios, dispositivos, políticas y eventos del registro de una colección de usuarios.

Trabajo con grupos y usuarios

Esta sección ofrece una introducción al trabajo con grupos y usuarios de Endpoint Encryption. Primero, defina los usuarios y grupos y, después, asigne los usuarios a los grupos. También se pueden agregar usuarios nuevos directamente a un grupo. Se necesita al menos un grupo superior.

Recomendaciones para la estructura de usuarios y grupos:

- Siga la estructura de Active Directory a la hora de configurar la estructura de un grupo.
- Cree un nuevo grupo cada vez que exista una política diferente entre los grupos de usuarios. Si un grupo requiere autenticación de dominio y otro requiere contraseña fija, son necesarios dos grupos de políticas independientes.
- Cree varios grupos para minimizar el acceso a los dispositivos de un grupo. Todos los miembros de un grupo tienen permiso de acceso a los dispositivos de ese grupo.

Definición de usuarios y grupos

Defina todas las afiliaciones de funciones y grupos antes de agregar usuarios o grupos a PolicyServer.

1. Identifique los administradores y autenticadores de empresa.
2. Cree los administradores y autenticadores de empresa.
3. Identifique los grupos.
4. Cree los grupos.
5. Identifique los administradores y autenticadores de grupo.
6. Cree los administradores y autenticadores de grupo.
7. Identifique los usuarios que se asignarán a cada grupo.
8. Importe o cree nuevos usuarios para cada grupo.

Adición de un grupo superior

Los grupos simplifican la administración de aplicaciones, usuarios, políticas, subgrupos y dispositivos activados. Un grupo superior es el grupo que está en el nivel más alto.



Nota

Las cuentas de administrador o autenticador no se pueden agregar a grupos. Para crear un administrador de grupo, agregue un usuario y cambie sus permisos en el grupo.

Procedimiento

1. En el panel izquierdo, haga clic con el botón derecho en el nombre de la empresa y, a continuación, haga clic en **Agregar grupo superior**.



FIGURA 2-2. Adición de un grupo superior

Aparecerá la pantalla **Añadir nuevo grupo**.

2. Proporcione el nombre y la descripción del grupo.

3. Seleccione **Admitir dispositivos heredados** solamente si usa dispositivos heredados que no admitan codificación Unicode. Algunos dispositivos heredados no podrán comunicarse con PolicyServer mediante Unicode. Asigne los dispositivos Unicode y los dispositivos heredados a grupos distintos.

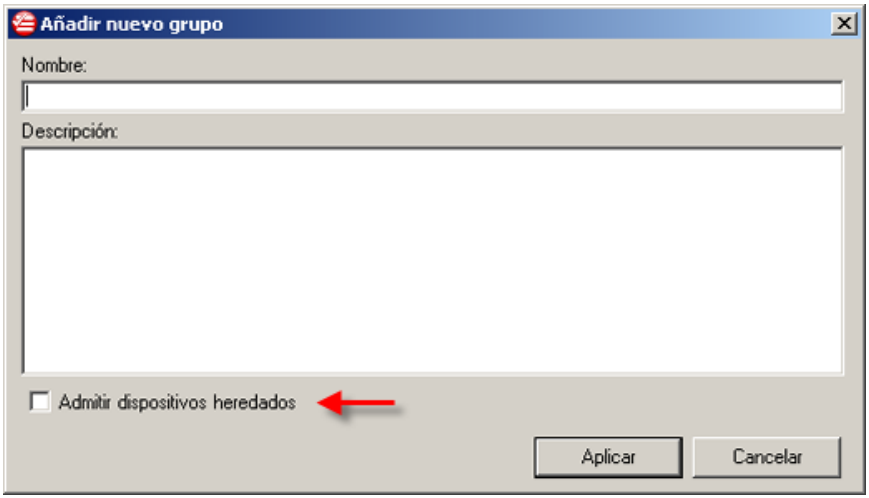


FIGURA 2-3. Añadir nuevo grupo

4. Haga clic en **Aplicar**.
5. En el mensaje de confirmación, haga clic en **Aceptar**.

   El nuevo grupo se agrega a la estructura de árbol del panel izquierdo.

Agregar un nuevo usuario a un grupo

Nota

- El hecho de agregar un usuario a la empresa no asigna el usuario a ningún grupo.
- Agregar un usuario a un grupo lo agrega al grupo y a la empresa.

Procedimiento

1. Seleccione el grupo y abra **Usuarios**.

2. En el panel derecho, haga clic con el botón derecho en el espacio en blanco y seleccione **Agregar nuevo usuario**.

   Aparecerá la pantalla **Agregar nuevo usuario**.

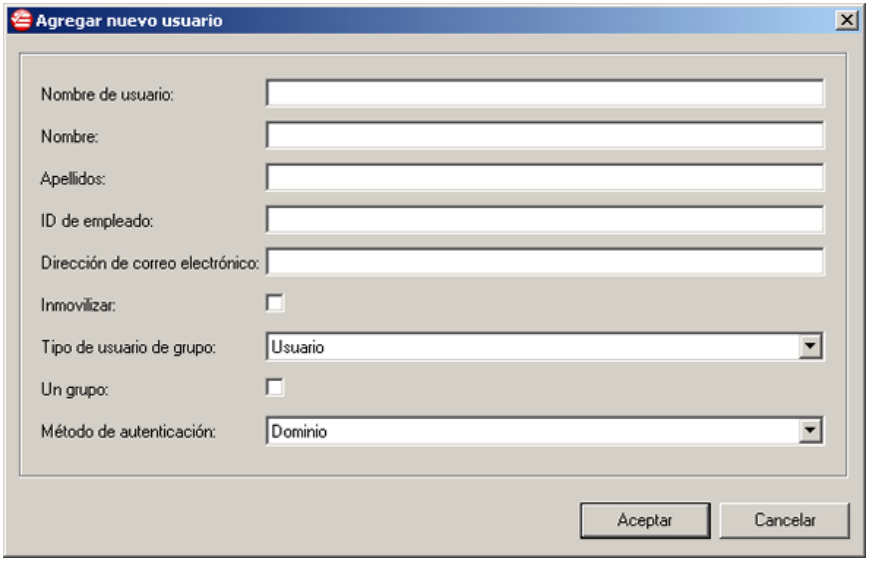


FIGURA 2-4. Pantalla Agregar nuevo usuario

3. Especifique la información de usuario. La información obligatoria es el nombre de usuario, el nombre y el apellido.

4. Solo seleccione **Inmovilizar** si la cuenta debiera estar temporalmente desactivada. Mientras esté inmovilizada, el usuario no podrá iniciar sesión en dispositivos.

5. Use el campo **Tipo de usuario de grupo** para definir los privilegios de la nueva cuenta. Los administradores y autenticadores empresariales no se pueden agregar a grupos.

6. Seleccione **Un grupo** para desactivar al usuario de la pertenencia a varios grupos.

7. Seleccione el **Método de autenticación**.

Nota

El método de autenticación predeterminado para los usuarios en **Ninguno**.

8. Haga clic en **Aceptar**.

   El nuevo usuario se agrega al grupo seleccionado **y** a la empresa. El usuario ya puede iniciar una sesión en un dispositivo.

Agregar un nuevo usuario empresarial

Nota

- El hecho de agregar un usuario a la empresa no asigna el usuario a ningún grupo.
- Agregar un usuario a un grupo lo agrega al grupo y a la empresa.

Procedimiento

1. Seleccione la empresa y abra **Usuarios**.
2. En el panel derecho, haga clic con el botón derecho en el espacio en blanco y seleccione **Agregar usuario**.

   Aparecerá la pantalla **Agregar nuevo usuario**.

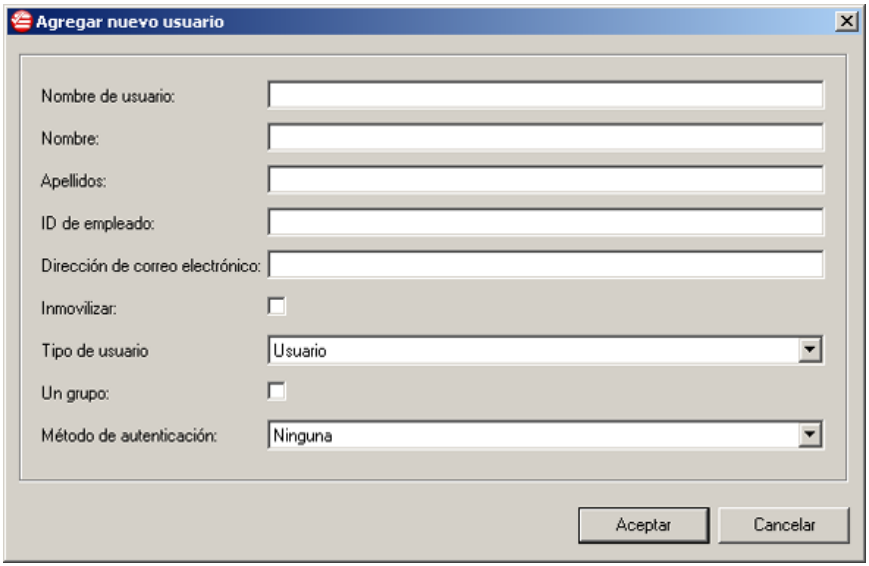


FIGURA 2-5. Pantalla Agregar nuevo usuario

3. Especifique la información de usuario. La información obligatoria es el nombre de usuario, el nombre y el apellido.

4. Solo seleccione **Inmovilizar** si la cuenta debiera estar temporalmente desactivada. Mientras esté inmovilizada, el usuario no podrá iniciar sesión en dispositivos.

5. Use el campo **Tipo de usuario** para definir los privilegios de la nueva cuenta. Los administradores y autenticadores empresariales no se pueden agregar a grupos.

6. Seleccione **Un grupo** para desactivar al usuario de la pertenencia a varios grupos.

7. Seleccione el **Método de autenticación**.

Nota

El método de autenticación predeterminado para los usuarios en **Ninguno**.

---

8. Haga clic en **Aceptar**.

Se ha agregado el nuevo usuario a esta empresa de PolicyServer. El usuario no podrá iniciar sesión en un dispositivo hasta que se agregue a un grupo.

Agregar un usuario existente a un grupo

Un usuario se puede agregar a varios grupos.

Procedimiento

1. En el panel izquierdo, seleccione un grupo y, a continuación, haga clic en **Usuarios**.
2. En el panel derecho, haga clic con el botón derecho en el espacio en blanco y seleccione **Agregar usuario existente**.

   Aparecerá la pantalla **Agregar usuarios a grupo**.

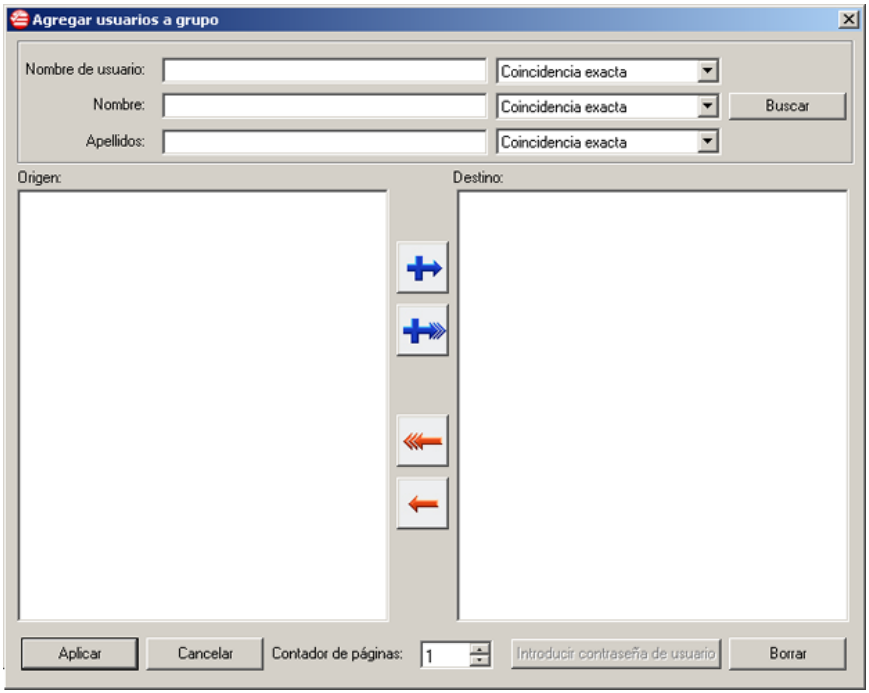


FIGURA 2-6. Pantalla Agregar usuarios a grupo

3. Especifique los detalles del usuario y haga clic en **Buscar**.

   Si hay alguna coincidencia, el campo **Fuente** se rellena con las cuentas.

4. Seleccione las cuentas de usuario de la lista y haga clic en la **flecha azul** para agregarlas. Consulte *Tabla 2-3: Iconos para agregar/eliminar usuarios en la página 2-12* para obtener controles adicionales.

TABLA 2-3. Iconos para agregar/eliminar usuarios

ICONOS CENTRALES	DESCRIPCIÓN
	Agregue un único usuario seleccionado al campo **Destino**.

Iconos centrales	Descripción
	Agregue todos los usuarios encontrados basados en el criterio de búsqueda al campo **Destino**.
	Elimine un único usuario seleccionado del campo **Destino**.
	Elimine todos los usuarios del campo **Destino**.

5. Para cambiar la contraseña de un usuario:

   a. En el campo **Destino**, resalte el usuario.

   b. Haga clic en **Introducir contraseña de usuario** ubicada en la parte inferior de la ventana.

   c. En la ventana que aparece, especifique el método de autenticación del usuario.

   d. Haga clic en **Aplicar**.

6. Haga clic en **Aplicar**.

   El usuario se ha agregado al grupo. Si el usuario solo pertenece a este grupo, podrá iniciar sesión en el cliente de punto final.

Descripción del control de políticas

Después de configurar todos los usuarios y grupos de la empresa, configure las políticas de la empresa o grupo. Cada grupo de la estructura de árbol del panel izquierdo (sea un grupo superior o un subgrupo) contiene una o varias carpetas de políticas de aplicación final.

Para obtener información detallada acerca de la interfaz de PolicyServer, consulte *Interfaz de la MMC de PolicyServer en la página 2-3*.

Nota

Las políticas se pueden activar o desactivar en el nivel de empresa o en el nivel de grupo. Consulte *Trabajar con políticas en la página 3-2*.

Indicadores visuales de políticas

Los círculos de colores al lado de cada política indican el estado de la política.

TABLA 2-4. Indicadores de políticas

INDICADOR	DESCRIPCIÓN
	El valor de la política se hereda del grupo primario o de la empresa.
	Se modifica una política para el grupo.
	La política puede tener múltiples matrices de valores.
	La política tiene una o más subpolíticas.

Botones y campos de la política

Utilice los campos y botones que se muestran a continuación para controlar los elementos de la política. Todos los valores modificados se extienden a los subgrupos de un grupo. En función de lo que controle la política, determinados campos no estarán presentes.

TABLA 2-5. Botones y campos de la política

CAMPO/BOTÓN	DESCRIPCIÓN	¿MODIFICABLE?
Aceptar	Guarda los cambios de la política seleccionada.	N/D

Campo/Botón	Descripción	¿Modificable?
Descripción	Describe la política seleccionada.	No
Intervalo de política	Muestra el intervalo de valores admitidos para la política seleccionada.	Sí
Valor de política	En función de la política, muestra el valor actual de la política seleccionada y si contiene una cadena, un número o una serie de entradas.	Sí
Valor múltiple de política	Especifica si esta política puede utilizarse varias veces para distintas configuraciones (por ejemplo, varias cadenas "si se encuentra").	No
Nombre de la política	Muestra el nombre de la política seleccionada.	No
Tipo de política	Especifica la categoría de la política seleccionada.	No
Controlado por la empresa	Hace que los cambios de esta política se reflejen en la misma política en el nivel de empresa.	Sí
Guardar en subgrupos	Envía la configuración de la política a la misma política en todos los subgrupos.	Sí

Modificación de políticas

PolicyServer tiene un conjunto común de ventanas para modificar políticas. Existen diferentes tipos de entrada disponibles en función de lo que controle la política y qué parámetros se requieran. Los pasos necesarios para editar políticas difieren de una política a otra. Esta tarea ofrece una descripción general acerca de cómo editar una política.

Para obtener más detalles acerca de cómo modificar políticas, incluidas explicaciones sobre la configuración de diferentes tipos de políticas, consulte *Administración de políticas en la página 3-2*.

Procedimiento

1. Expanda la **Empresa**.
2. Elija qué nivel de políticas modificar:
   a. Para las políticas de nivel de empresa, expanda **Políticas de empresa**.
   b. Para las políticas de nivel de grupo, expanda **Nombre del grupo** y, seguidamente, expanda **Políticas**.
3. Abra la aplicación específica o seleccione **Común**.

   La lista de políticas se muestra en las ventanas de resultados.

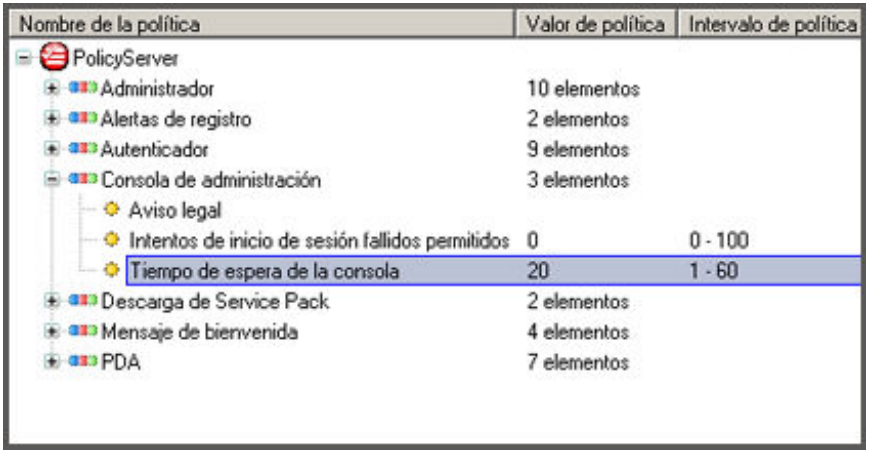


FIGURA 2-7. Modificar una política

4. Vaya a una política y haga doble clic para abrir la ventana de edición. Utilizaremos **Tiempo de espera de la consola** para este ejemplo.

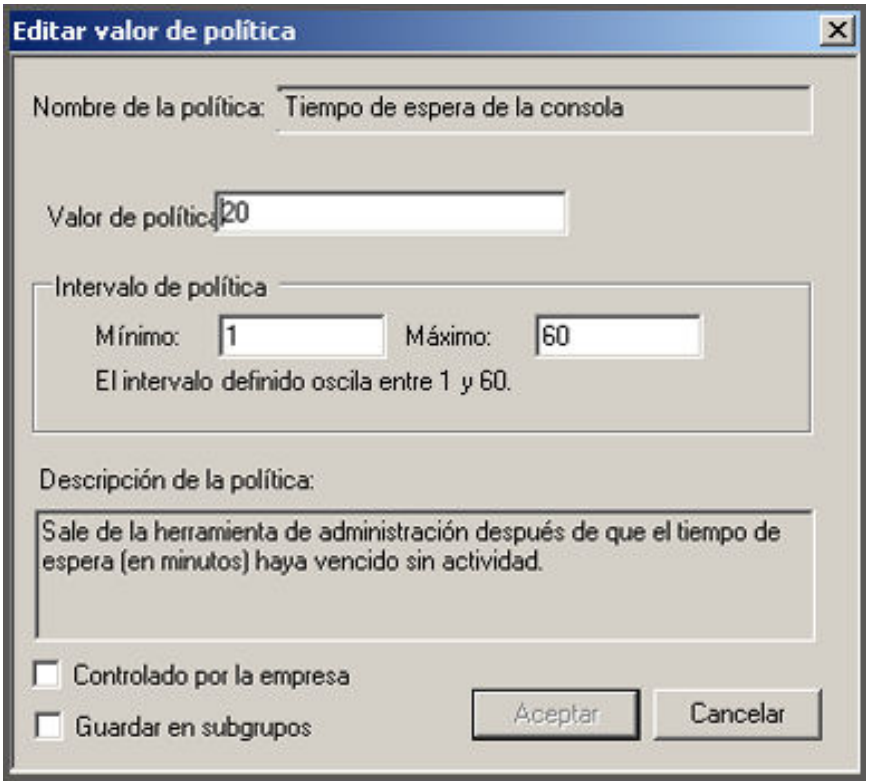


FIGURA 2-8. Ventana del editor de la política Tiempo de espera de la consola

5. Realice los cambios adecuados para la política y, a continuación, haga clic en **Aceptar**.

Activar aplicaciones

Importante

Para garantizar la correcta comunicación y sincronización de políticas, debe activarse la aplicación Endpoint Encryption en PolicyServer antes de la instalación.

Procedimiento

1. Inicie sesión en la MMC de PolicyServer.
2. Haga clic en **Políticas de empresa**.

   Todas las aplicaciones aparecen en el panel derecho

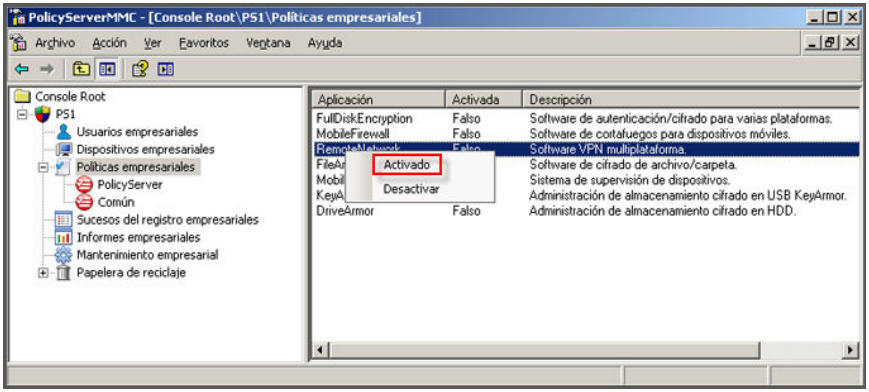


FIGURA 2-9. Habilitar aplicaciones

3. Haga clic con el botón derecho en la aplicación y seleccione **Activar**.

> **Nota**
>
> Para usar Full Disk Encryption, deben activarse tanto Full Disk Encryption como MobileSentinel.

PolicyServer activa y administra la aplicación.

Capítulo 3

Descripción de políticas

En este capítulo se explica cómo usar las políticas y proporciona información detallada sobre los valores de configuración de las políticas individuales. Para obtener información sobre cómo administrar usuarios, grupos y dispositivos, consulte *Trabajar con grupos, usuarios y dispositivos en la página 4-1*.

Este capítulo aborda los siguientes temas:

- *Trabajar con políticas en la página 3-2*
- *Administración de políticas en la página 3-2*
- *Políticas de PolicyServer en la página 3-13*
- *Políticas de Full Disk Encryption en la página 3-20*
- *Políticas de FileArmor en la página 3-30*
- *Políticas de MobileSentinel en la página 3-36*
- *Políticas de KeyArmor en la página 3-40*
- *Políticas de DriveArmor en la página 3-46*
- *Políticas comunes en la página 3-52*

Trabajar con políticas

En esta sección se explica cómo usar varias ventanas para cambiar una política, pero no explica el proceso de modificar las políticas. Todas las políticas tienen valores predeterminados. MMC de PolicyServer tiene un conjunto común de ventanas para modificar políticas. Una política tendrá disponible una ventana de edición para modificar los números, intervalos y valores asociados con la política, mientras que otra política tendrá una ventana para modificar cadenas de texto.

Cuando administre políticas, recuerde lo siguiente:

- Las políticas son configurables por aplicación dentro de cada grupo.
- La herencia de políticas solo sucede cuando se crea un subgrupo. Para obtener información detallada acerca de los permisos de grupo, consulte *Trabajar con grupos en la página 4-2*.

Administración de políticas

Cada grupo de la estructura de árbol del panel izquierdo (sea un grupo superior o un subgrupo) contiene una o varias carpetas de políticas de aplicación final.

La ventana de resultados situada en el panel derecho muestra controles para:

- Mostrar una lista de políticas y sus valores.
- Modificar una política mediante la ventana de edición.
- Ejecutar informes y otros sucesos de registro.
- Ejecutar el mantenimiento empresarial.

Para obtener una explicación detallada de la interfaz, consulte *Interfaz de la MMC de PolicyServer en la página 2-3*.

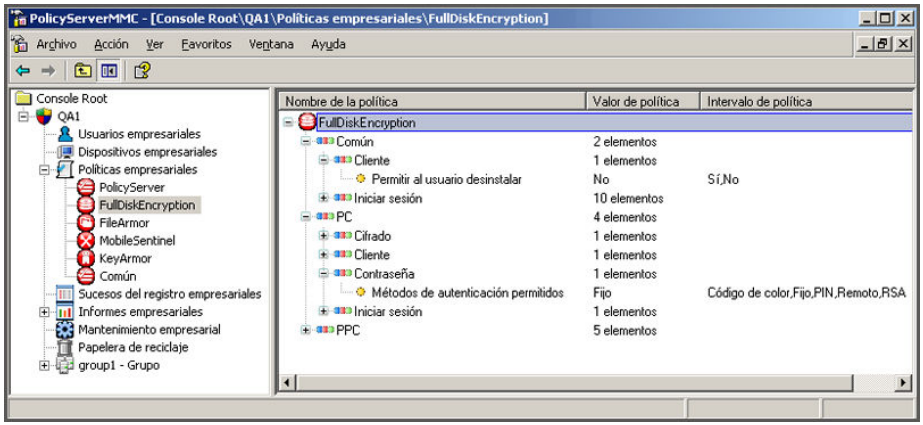


FIGURA 3-1. Ventana de MMC de PolicyServer

Selección de una política para su modificación

Procedimiento

1. Vaya a **Nombre de grupo** > **Políticas** > **Nombre de aplicación**.

   Ejemplo: **Grupo1** > **Políticas** > **Full Disk Encryption**.

2. Vaya a la política específica.

   Ejemplo: **Común** > **Cliente** > **Permitir al usuario desinstalar**

3. Haga clic con el botón derecho en la política y seleccione **Propiedades**.

Edición de políticas con intervalos

Un ejemplo de edición de políticas con intervalos es la política **Intentos de inicio de sesión fallidos permitidos**. **Intentos de inicio de sesión fallidos permitidos**

controla si se bloquea un dispositivo cuando un usuario sobrepasa el número de intentos fallidos de autenticación permitidos.

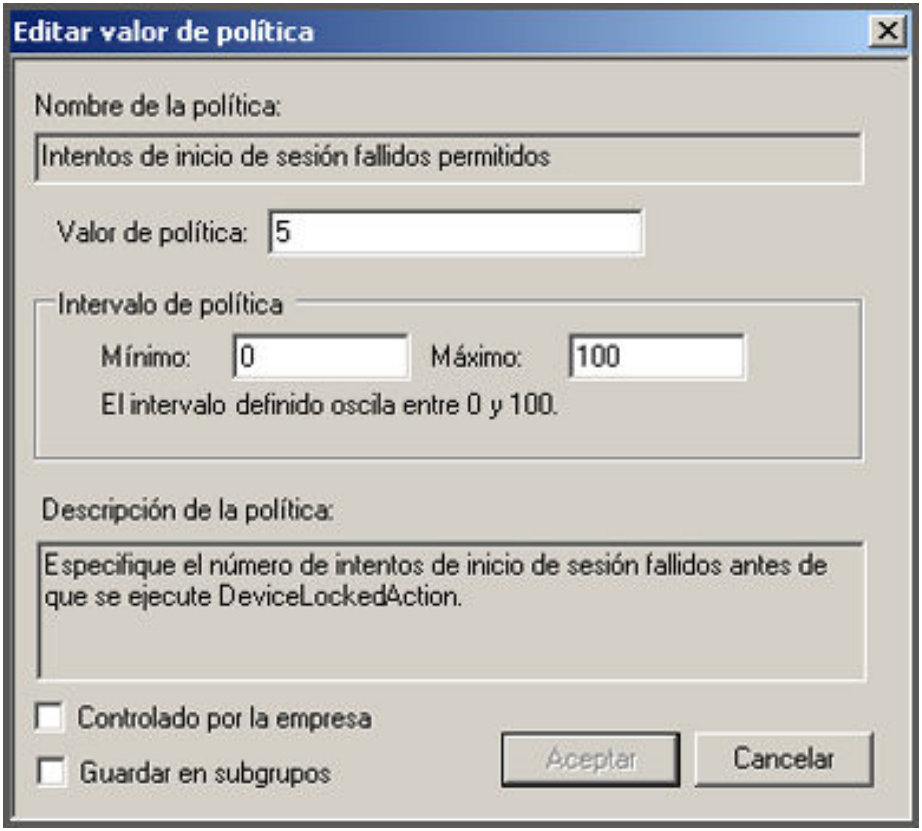


FIGURA 3-2. Ventana de política con intervalos

Mediante los parámetros definidos en los campos **Intervalo de política**, un administrador puede indicar el número de intentos fallidos de autenticación permitidos por usuario en el campo **Valor de política**.

Procedimiento

1. Haga clic con el botón derecho en la política que desea modificar y, a continuación, haga clic en **Propiedades**.
2. En el campo **Intervalo de política mínimo**, especifique el número mínimo de intentos fallidos de autenticación que puede realizar un usuario de este grupo antes de que se bloquee el dispositivo.



Nota

Los valores mínimo y máximo para el intervalo de la política pueden ser iguales a los del intervalo principal, o se pueden modificar. Los valores mínimo y máximo no pueden ampliarse.

3. En el campo **Intervalo de política máximo**, especifique el número máximo de intentos de autenticación que puede realizar un usuario de este grupo antes de que falle la autenticación y se bloquee el dispositivo.
4. En el campo **Valor de política**, especifique el número de intentos fallidos de autenticación permitidos para un usuario de este grupo antes de que se bloquee el dispositivo.
5. Haga clic en **Aceptar** para guardar los cambios realizados en esta ventana.

   El cambio en la política se activará la próxima vez que el cliente de punto final se sincronice con PolicyServer.

Edición de políticas con respuestas de Verdadero/Falso o Sí/No

Algunas políticas solo tienen opciones de Verdadero/Falso o Sí/No. Para este ejemplo, utilizaremos **Omitir arranque previo**.

El administrador de un grupo puede definir si debería aparecer el arranque previo de Full Disk Encryption. Si el grupo principal permite Sí y No, entonces los autenticadores del subgrupo tendrán privilegios para definir el intervalo en Sí y No, solo en Sí o solo en

No. Si el grupo principal tiene el intervalo definido en Sí o en No, entonces el administrador del subgrupo solo podrá seleccionar ese mismo intervalo.

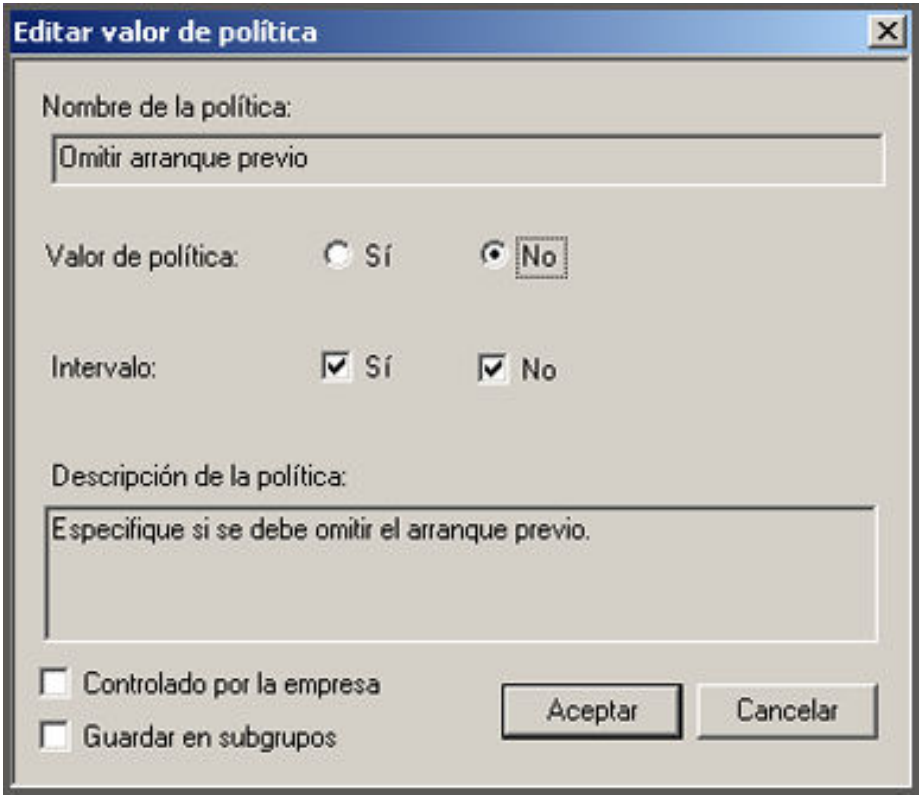


FIGURA 3-3. Política con valores Sí/No

Procedimiento

1. Haga clic con el botón derecho en la política que desea modificar y, a continuación, haga clic en **Propiedades**.
2. El campo **Valor de política** establece si la política está activada.
3. El campo **Intervalo** establece si esta política está disponible para otros usuarios o grupos. Por ejemplo, si un administrador de la empresa ha establecido la política en

No en Políticas empresariales, entonces la política no estará disponible para que ningún otro grupo la establezca en Sí.

4. Haga clic en **Aceptar** para guardar los cambios realizados en esta ventana.

   El cambio en la política se activará la próxima vez que el cliente de punto final se sincronice con PolicyServer.

Edición de políticas con selección múltiple / selección única

Algunas políticas tienen varias opciones disponibles. La política **Acción de dispositivo bloqueado** se edita en una ventana de selección múltiple / selección única. Los administradores solo pueden seleccionar un **Valor de política**. En este ejemplo, el

administrador del grupo debe definir la acción que se realizará cuando un usuario sobrepase el número permitido de intentos de autenticación.

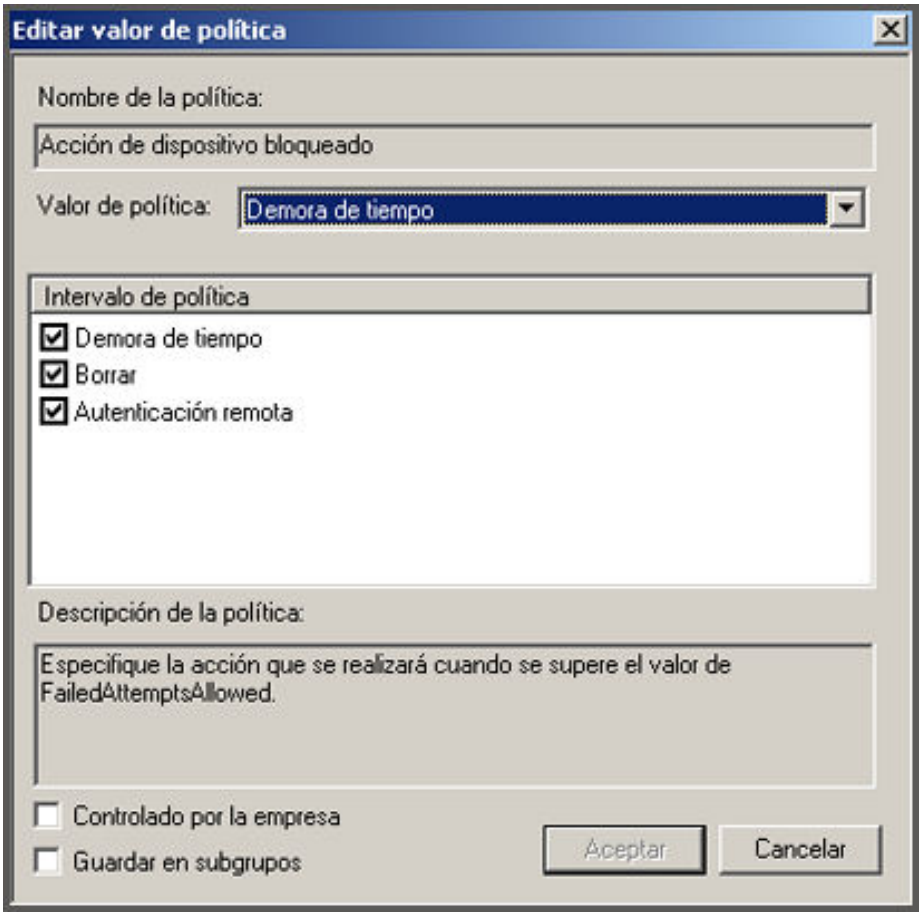


FIGURA 3-4. Política con selección múltiple/selección única

Procedimiento

1. Haga clic con el botón derecho en la política que desea modificar y, a continuación, haga clic en **Propiedades**.

2. Seleccione el valor de configuración predeterminado que desee para la lista desplegable **Valor de política**.

3. Seleccione las opciones disponibles para el área **Intervalo de política**.



Nota

Si elimina una opción, se elimina el valor la lista desplegable **Valor de política**.

4. Haga clic en **Aceptar** para guardar los cambios.

   El cambio en la política se activará la próxima vez que el cliente de punto final se sincronice con PolicyServer.

Edición de políticas con argumentos de cadenas de texto

Algunas políticas tienen una cadena de texto editable para argumentos de matriz simple. La política **Interruptor de borrado de contenido** es un ejemplo de política que proporciona la capacidad de especificar una cadena de texto.

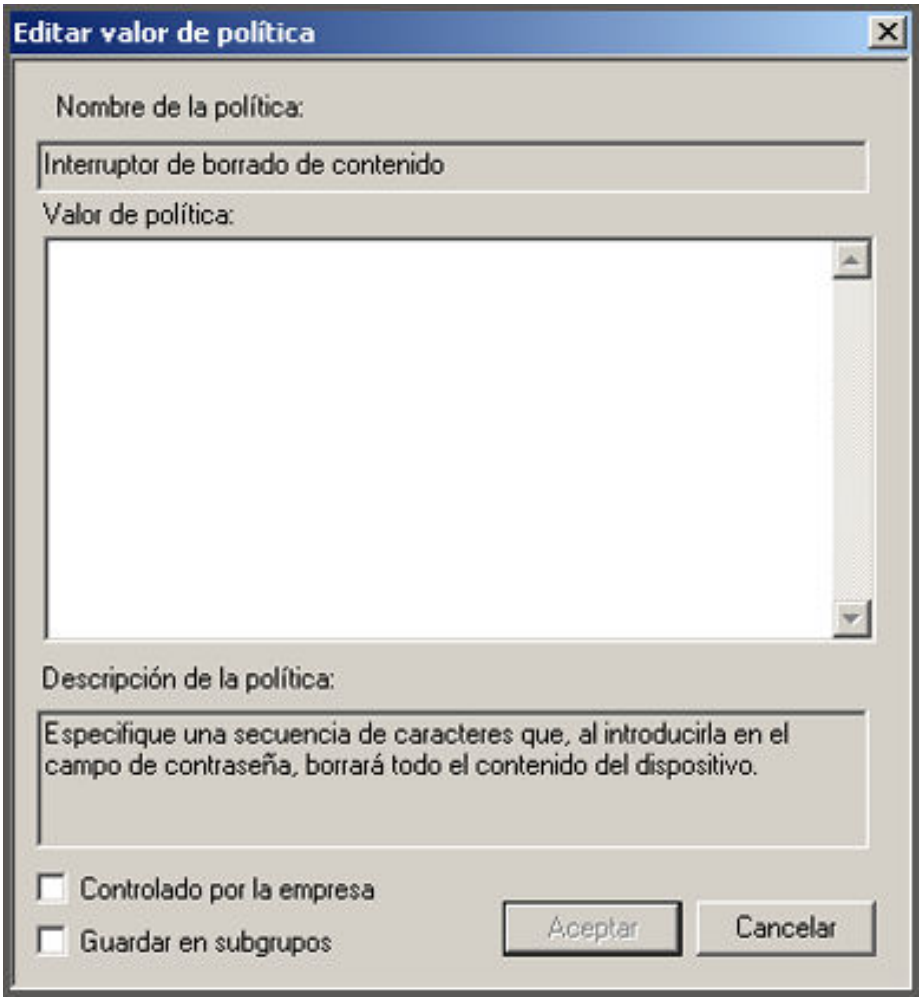


FIGURA 3-5. Política con argumento de cadena de texto

Procedimiento

1. Haga clic con el botón derecho en la política que desea modificar y, a continuación, haga clic en **Propiedades**.
2. Para el campo **Valor de política**, especifique la secuencia de caracteres para esta política.
3. Haga clic en **Aceptar** para guardar los cambios realizados en esta ventana.

   El cambio en la política se activará la próxima vez que el cliente de punto final se sincronice con PolicyServer.

Edición de políticas de varias opciones

Algunas políticas tienen varias opciones almacenadas en subpolíticas que afectan a dicha política. Las políticas de varias opciones están diseñadas para crear líneas separadas en una cadena de texto; cada subpolítica es una nueva línea de la cadena. Por ejemplo, la política **Si se encuentra** muestra cómo devolver un dispositivo encontrado. Un formato de dirección normal muestra el nombre, la dirección de la calle y la ciudad/estado/código postal en tres líneas separadas.



Nota

El número de subpolíticas está limitado por las capacidades de la aplicación de punto final, que generalmente no suele superar las seis líneas de texto.

Procedimiento

1. Haga clic con el botón derecho en la política que desea modificar y, a continuación, haga clic en **Agregar**.

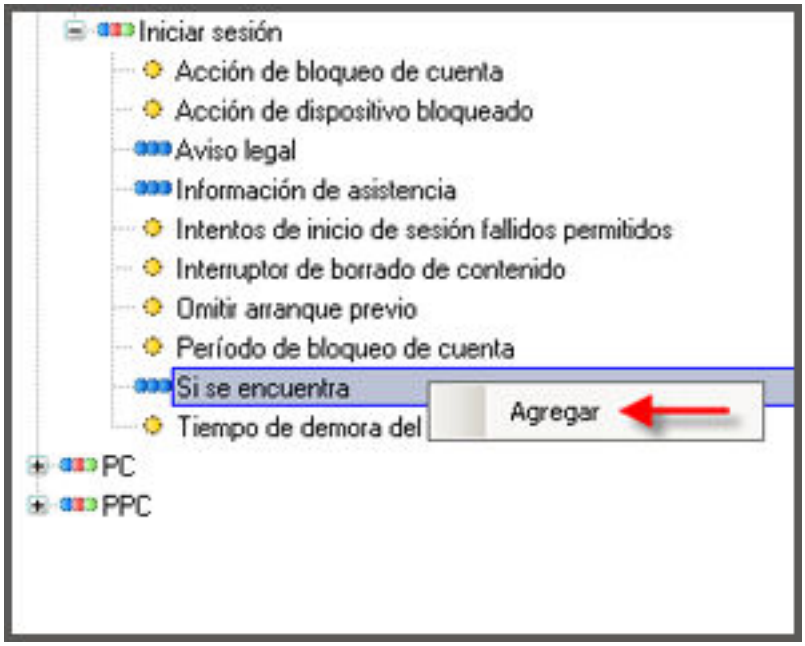


FIGURA 3-6. Política Si se encuentra: Agregar una nueva opción

2. En la ventana de políticas que aparece, especifique los detalles en el campo **Valor de política**.

Nota

Dependiendo de la política, es posible agregar una nueva política y, a continuación, modificarla, haciendo clic con el botón derecho y seleccionando **Propiedades**.

---

3. Haga clic en **Aceptar** para guardar los cambios realizados en esta ventana y repita los pasos si es necesario.

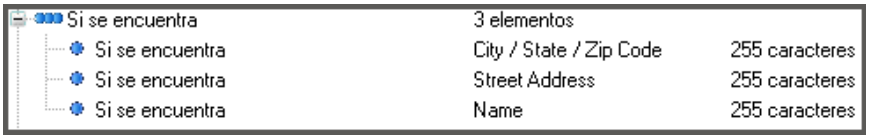


FIGURA 3-7. Política Si se encuentra: Resultados después de agregar varias opciones

4. Para realizar los cambios, haga clic con el botón derecho en la política secundaria y seleccione **Propiedades**.

   El cambio en la política se activará la próxima vez que el cliente de punto final se sincronice con PolicyServer.

Políticas de PolicyServer

Esta sección explica las opciones configurables para todas las políticas de la empresa que afecten a PolicyServer.

Políticas de consola de administración

Políticas que controlan las herramientas de administración, como Administrador de seguridad empresarial y MMC de PolicyServer.

TABLA 3-1. Políticas de consola de administración de PolicyServer

NOMBRE DE LA POLÍTICA	DESCRIPCIÓN	INTERVALO DE VALOR Y VALOR PREDETERMINADO
Tiempo de espera de la consola	Sale de la herramienta de administración después de que el tiempo de espera (en minutos) haya vencido sin actividad.	1-60 Valor predeterminado: 20

Nombre de la política	Descripción	Intervalo de valor y valor predeterminado
Intentos de inicio de sesión fallidos permitidos	Bloquea el inicio de sesión del administrador después de esta cantidad de intentos de inicio de sesión fallidos consecutivos.	0-100 Valor predeterminado: 0
Aviso legal	Contiene el aviso legal que se debe mostrar antes de que el administrador o autenticador pueda usar las herramientas de administración.	1-1024 caracs. Valor predeterminado: N/D

Políticas de administrador

Políticas que controlan los privilegios del administrador de grupo de PolicyServer.

Tabla 3-2. Políticas de administrador de PolicyServer

Nombre de la política	Descripción	Intervalo de valor y valor predeterminado
Agregar dispositivos	Especifique si los administradores de grupo pueden agregar dispositivos.	Sí, No Valor predeterminado: Sí
Agregar usuarios	Especifique si los administradores de grupo pueden agregar nuevos usuarios.	Sí, No Valor predeterminado: Sí
Agregar usuarios a empresa	Especifique si los administradores de grupo pueden agregar nuevos usuarios a la empresa.	Sí, No Valor predeterminado: No

Nombre de la política	Descripción	Intervalo de valor y valor predeterminado
Agregar/modificar grupos	Especifique si los administradores de grupo pueden agregar o modificar subgrupos.	Sí, No Valor predeterminado: Sí
Cambiar políticas	Especifique si los administradores de grupo pueden cambiar políticas.	Sí, No Valor predeterminado: Sí
Copiar y pegar grupos	Especifique si los administradores de grupo pueden copiar y pegar subgrupos.	Sí, No Valor predeterminado: Sí
Eliminar dispositivos	Especifique si los administradores de grupo pueden eliminar dispositivos.	Sí, No Valor predeterminado: Sí
Eliminar grupos	Especifique si los administradores de grupo pueden eliminar subgrupos.	Sí, No Valor predeterminado: Sí
Eliminar usuarios	Especifique si los administradores de grupo pueden eliminar usuarios.	Sí, No Valor predeterminado: Sí
Quitar usuarios de la empresa	Especifique si los administradores de grupo pueden quitar usuarios de la empresa.	Sí, No Valor predeterminado: No

Políticas de autenticador

Políticas que controlan los privilegios y derechos del autenticador del grupo y la empresa.

TABLA 3-3. Políticas de autenticador de PolicyServer

NOMBRE DE LA POLÍTICA	DESCRIPCIÓN	INTERVALO DE VALOR Y VALOR PREDETERMINADO
Agregar dispositivos	Especifique si los autenticadores pueden agregar dispositivos.	Sí, No Valor predeterminado: No
Agregar usuarios	Especifique si los autenticadores pueden agregar nuevos usuarios.	Sí, No Valor predeterminado: No
Agregar usuarios a empresa	Especifique si los autenticadores pueden agregar nuevos usuarios a la empresa.	Sí, No Valor predeterminado: No
Agregar/modificar grupos	Especifique si los autenticadores pueden agregar o modificar subgrupos.	Sí, No Valor predeterminado: No
Copiar y pegar grupos	Especifique si los autenticadores pueden copiar y pegar subgrupos.	Sí, No Valor predeterminado: No
Eliminar dispositivos	Especifique si los autenticadores pueden eliminar dispositivos.	Sí, No Valor predeterminado: No

Nombre de la política	Descripción	Intervalo de valor y valor predeterminado
Eliminar grupos	Especifique si los autenticadores pueden eliminar subgrupos.	Sí, No Valor predeterminado: No
Eliminar usuarios	Especifique si los autenticadores pueden eliminar usuarios.	Sí, No Valor predeterminado: No
Quitar usuarios de la empresa	Especifique si los autenticadores pueden quitar usuarios de la empresa.	Sí, No Valor predeterminado: No

Políticas de alertas del registro

Políticas que controlan los mensajes de correo electrónico enviados sobre sucesos del registro de PolicyServer importantes.

Tabla 3-4. Políticas de alertas del registro de PolicyServer

Nombre de la política	Descripción	Intervalo de valor y valor predeterminado
Dirección de correo electrónico de origen	Especifique la dirección de correo electrónico que se usa como dirección de correo electrónico de origen para el mensaje de correo electrónico de alerta.	Entre 1 y 255 caracteres Valor predeterminado: N/D
Nombre del servidor SMTP	Especifique el servidor SMTP responsable de enviar los mensajes de correo electrónico de alerta.	Entre 1 y 255 caracteres Valor predeterminado: N/D

Políticas de PDA

Políticas que controlan cómo se pueden comunicar los dispositivos PDA con PolicyServer.

TABLA 3-5. Políticas de PDA de PolicyServer

CATEGORÍA	NOMBRE DE LA POLÍTICA	DESCRIPCIÓN	INTERVALO DE VALOR Y VALOR PREDETERMINADO
PDA	Teléfono móvil PDA	Especifique si los dispositivos de teléfono móvil PDA recibirán la notificación del mensaje de instalación a través de un SMS o de un correo electrónico .	SMS, Correo electrónico, Ninguno Valor predeterminado: Ninguno
PDA	Correo electrónico	Configuración de correo electrónico utilizada para enviar la notificación de instalación al usuario.	
PDA > **Correo electrónico**	Nombre del servidor SMTP	Especifique el servidor SMTP responsable de enviar los mensajes de correo electrónico.	Entre 1 y 255 caracteres
PDA > **Correo electrónico**	Asunto	Especifique el texto del asunto que se mostrará al usuario en la línea Asunto del correo electrónico.	Entre 1 y 255 caracteres
PDA	SMS	Especifique si los dispositivos reciben una notificación por SMS si se cambia la configuración del usuario o la política.	Activar, Desactivar Valor predeterminado: Desactivar
PDA > **SMS**	Dominio de correo electrónico	Especifique el dominio del correo electrónico de destino.	Entre 1 y 255 caracteres
PDA > **SMS**	Nombre del servidor SMTP	Especifique el servidor SMTP responsable de enviar las notificaciones SMS.	Entre 1 y 255 caracteres

Categoría	Nombre de la política	Descripción	Intervalo de valor y valor predeterminado
PDA > **SMS**	Correo electrónico de origen	Especifique la dirección de correo electrónico desde la que se enviarán las notificaciones por SMS y correo electrónico.	Entre 1 y 255 caracteres
PDA	Dispositivo PDA anclado a la red	Especifique si los dispositivos inalámbricos, BlueTooth, acoplados o de teléfono móvil PDA recibirán la notificación del mensaje de instalación a través de un correo electrónico.	Correo electrónico, Ninguno Valor predeterminado: Ninguno
PDA	Mensaje de bienvenida	Contiene el archivo del mensaje de bienvenida cuyo contenido se muestra al usuario durante el proceso de descarga.	Entre 1 y 1024 caracteres

Políticas de descarga de Service Pack

Las políticas controlan el momento en que se realizan las descargas automáticas de los Service Pack del cliente.

Tabla 3-6. Políticas de descarga de Service Pack de PolicyServer

Nombre de la política	Descripción	Intervalo de valor y valor predeterminado
Hora de inicio de descarga de Service Pack	Define la hora a la que descargar los Service Packs.	0-23 Valor predeterminado : 0
Hora de finalización de descarga de Service Pack	Define la hora a la que detener la descarga de cualquier Service Pack.	0-23 Valor predeterminado : 0

Políticas del mensaje de bienvenida

Políticas que controlan si enviar un mensaje de bienvenida a los usuarios cuando se les agrega a un grupo.

TABLA 3-7. Políticas del mensaje de bienvenida de PolicyServer

NOMBRE DE LA POLÍTICA	DESCRIPCIÓN	INTERVALO DE VALOR Y VALOR PREDETERMINADO
Mensaje	Contiene el archivo de mensaje de bienvenida.	Entre 1 y 1024 caracteres Valor predeterminado: N/D
Nombre del servidor SMTP	Especifique el servidor SMTP responsable de enviar los mensajes de correo electrónico de bienvenida.	Entre 1 y 255 caracteres Valor predeterminado: N/D
Correo electrónico de origen	Especifique la dirección de correo electrónico que se usa como dirección de correo electrónico de origen para el mensaje de correo electrónico de bienvenida.	Entre 1 y 255 caracteres Valor predeterminado: N/D
Asunto	Línea de asunto del mensaje de bienvenida.	Entre 1 y 255 caracteres Valor predeterminado: N/D

Políticas de Full Disk Encryption

Esta sección explica las opciones configurables para todas las políticas que afectan a los clientes de Full Disk Encryption.

Políticas comunes

Políticas comunes que afectan a Full Disk Encryption, que incluyen iniciar sesión, desinstalar Full Disk Encryption y bloquear dispositivos.

TABLA 3-8. Políticas comunes de Full Disk Encryption

CATEGORÍA	NOMBRE DE LA POLÍTICA	DESCRIPCIÓN	INTERVALO DE VALOR Y VALOR PREDETERMINADO
Cliente	Permitir al usuario desinstalar	Especifique si el usuario puede desinstalar Full Disk Encryption.	Sí, No Valor predeterminado: No
Iniciar sesión	Acción de bloqueo de cuenta	Especifique la acción que se realizará cuando el dispositivo no haya podido comunicarse con PolicyServer tal como se especifica en la política Período de bloqueo de cuenta. • Borrar: se borrará todo el contenido del dispositivo. • Autenticación remota: se requiere que el usuario realice una autenticación remota.	Borrar, Autenticación remota Valor predeterminado: Autenticación remota
Iniciar sesión	Período de bloqueo de cuenta	Especifique el número de días que el cliente puede estar sin mantener la comunicación con PolicyServer.	0-999 Valor predeterminado: 360
Iniciar sesión	Interruptor de borrado de contenido	Especifique una secuencia de caracteres; cuando se escriba se borrará todo el contenido del dispositivo.	Entre 1 y 255 caracteres Valor predeterminado: N/D

Categoría	Nombre de la política	Descripción	Intervalo de valor y valor predeterminado
Iniciar sesión	Acción de dispositivo bloqueado	Especifique la acción que se realizará cuando se bloquee el dispositivo. • Tiempo de demora: la cantidad de tiempo que debe transcurrir antes de que el usuario pueda volver a intentar iniciar una sesión. • Borrar: se borrará todo el contenido del dispositivo. • Autenticación remota: se requiere que el usuario realice una autenticación remota.	Tiempo de demora, Borrar, Autenticación remota Valor predeterminado: Demora de tiempo
Iniciar sesión	Intentos de inicio de sesión fallidos permitidos	Especifique el número de intentos de inicio de sesión que se permiten antes de utilizar el tiempo de demora del bloqueo del dispositivo.	0-100 Valor predeterminado: 5
Inicio de sesión > **Si se encuentra**	Si se encuentra	Especifique la información que se debe mostrar.	Entre 1 y 255 caracteres Valor predeterminado: N/D
Iniciar sesión	Aviso legal	Especifique si se debe mostrar un aviso legal.	Activar/ desactivar Valor predeterminado: Desactivada
Inicio de sesión > **Aviso legal**	Hora de visualización del aviso legal	Especifique cuándo se debe mostrar el aviso legal configurado al usuario.	Instalación, Inicio Valor predeterminado: Inicio

Categoría	Nombre de la política	Descripción	Intervalo de valor y valor predeterminado
Inicio de sesión > **Aviso legal**	Texto del aviso legal	Especifique el cuerpo del aviso legal.	Insertar archivo Valor predeterminado: N/D
Iniciar sesión	Visualización del tiempo del dispositivo de bloqueo	Bloquea el dispositivo durante x minutos si el usuario supera los intentos fallidos permitidos.	1-999,999 Valor predeterminado: 1
Iniciar sesión	Omitir arranque previo	Especifique si se debe omitir el arranque previo.	Sí, No Valor predeterminado: No
Inicio de sesión > **Información de asistencia**	Información de asistencia	Muestre la información del departamento de asistencia o el contacto del administrador.	Valor predeterminado: N/D

Políticas de PC

Políticas que controlan dispositivos o portátiles que ejecutan Full Disk Encryption.

Tabla 3-9. Políticas de PC de Full Disk Encryption

Categoría	Nombre de la política	Descripción	Intervalo de valor y valor predeterminado
Cliente	Permitir recuperación de usuario	Especifique si los usuarios tienen permiso para acceder a las utilidades de recuperación del sistema en el dispositivo.	Sí, No Valor predeterminado: No

Categoría	Nombre de la política	Descripción	Intervalo de valor y valor predeterminado
Cifrado	Cifrar dispositivo	Especifique si se debe cifrar el dispositivo.	Sí, No Valor predeterminado: Sí
Iniciar sesión	Autenticación de símbolo	Las políticas relacionadas con símbolos físicos incluyen tarjetas inteligentes y símbolos de USB. Todas las subpolíticas sólo son visibles cuando se habilita la autenticación de símbolo	Activar, Desactivar Valor predeterminado: Desactivar
Inicio de sesión > **Autenticación de símbolo**	Validación de OCSP	La comprobación de certificados mediante OCSP permite la revocación de certificados no válidos mediante la entidad emisora de certificados (CA). **Nota** Todas las subpolíticas sólo son visibles cuando se habilita la validación de OCSP.	Activar, Desactivar Valor predeterminado: Desactivar
Inicio de sesión > **Autenticación de símbolo** > **Validación de OCSP**	Certificados CA de OCSP	Certificados de entidades emisoras de certificados.	0-1024 bytes Valor predeterminado: N/D

Categoría	Nombre de la política	Descripción	Intervalo de valor y valor predeterminado
Inicio de sesión > **Autenticación de símbolo** > **Validación de OCSP**	Acción de estado de certificado caducado de OCSP	Define la acción que se realizará si el estado de certificado de OCSP ha caducado.	Tiempo de demora, Borrar, Autenticación remota, Denegación de conexión, Permitir acceso Valor predeterminado: Denegación de inicio de sesión
Inicio de sesión > **Autenticación de símbolo** > **Validación de OCSP**	Período de gracia de OCSP	Un período de gracia de días que permite que se realice la autenticación incluso si el servidor OCSP no ha verificado el certificado en ese número de días.	0-365 Valor predeterminado: 7
Inicio de sesión > **Autenticación de símbolo** > **Validación de OCSP**	Respondedores OCSP	Certificados de entidades emisoras de certificados.	Sí, No Valor predeterminado: Sí
Inicio de sesión > **Autenticación de símbolo** > **Validación de OCSP** > **Respondedores OCSP**	Certificado de respondedor OCSP	Certificados de entidades emisoras de certificados	0-1024 bytes Valor predeterminado: N/D

Categoría	Nombre de la política	Descripción	Intervalo de valor y valor predeterminado
Inicio de sesión > **Autenticación de símbolo** > **Validación de OCSP** > **Respondedores OCSP**	URL de respondedor OCSP	Certificados de entidades emisoras de certificados.	0-1024 bytes Valor predeterminado: N/D
Inicio de sesión > **Autenticación de símbolo** > **Validación de OCSP**	Acción de estado de certificado revocado de OCSP	Define la acción que se realizará si el estado de certificado de OCSP es revocado.	Tiempo de demora, Borrar, Autenticación remota, Denegación de conexión, Permitir acceso Valor predeterminado: Denegación de inicio de sesión
Inicio de sesión > **Autenticación de símbolo** > **Validación de OCSP**	Mostrar respuesta correcta de OCSP	Especifique si se debe mostrar si la respuesta de OCSP ha sido correcta.	Sí, No Valor predeterminado: Sí
Inicio de sesión > **Autenticación de símbolo** > **Validación de OCSP**	Acción de estado de certificado desconocido de OCSP	Especifique la acción que se realizará cuando el estado de un certificado OCSP sea desconocido.	Tiempo de demora, Borrar, Autenticación remota, Denegación de conexión, Permitir acceso Valor predeterminado: Denegación de inicio de sesión

Categoría	Nombre de la política	Descripción	Intervalo de valor y valor predeterminado
Iniciar sesión	Transferencia de símbolo	Transfiera el símbolo al escritorio GINA para un procesamiento adicional durante el proceso de inicio.	Sí, No Valor predeterminado: No
Contraseña	Métodos de autenticación permitidos	Especifique el tipo o tipos de métodos de autenticación que se pueden usar.	Fijo, ColorCode, Pin, Remoto, RSA Valor predeterminado: Fijo

Políticas de PPC

Políticas que gobiernan los dispositivos PPC con Full Disk Encryption de bolsillo.

Tabla 3-10. Políticas de PPC con Full Disk Encryption

Categoría	Nombre de la política	Descripción	Intervalo de valor y valor predeterminado
Cifrado	Cifrar citas en PPC	Especifique si la base de datos de citas se debe cifrar en el dispositivo PPC.	Sí, No Valor predeterminado: Sí
Cifrado	Cifrar contactos en PPC	Especifique si la base de datos de contactos se debe cifrar en el dispositivo PPC.	Sí, No Valor predeterminado: Sí
Cifrado	Cifrar dispositivo en PPC	Especifique si se cifrarán todos los soportes externos y el almacenamiento interno del dispositivo PPC.	Sí, No Valor predeterminado: Sí

Categoría	Nombre de la política	Descripción	Intervalo de valor y valor predeterminado
Cifrado	Cifrar correo electrónico en PPC	Especifique si la base de datos de correo electrónico se debe cifrar en el dispositivo PPC.	Sí, No Valor predeterminado: Sí
Cifrado	Cifrar otras bases de datos en PPC	Especifique una lista de bases de datos que cifrar en el dispositivo PPC.	Entre 1 y 255 caracteres Valor predeterminado: N/D
Cifrado > **Cifrar otras bases de datos en PPC**	Cifrar tareas en PPC	Especifique si la base de datos de tareas se debe cifrar en el dispositivo PPC.	Sí, No Valor predeterminado: Sí
PPC	Registro	Políticas que definen el archivo de registro en el dispositivo PPC.	
Registro	Tamaño del archivo de registro de PPC	Especifique el tamaño del archivo de registro en el dispositivo PPC (medido en kilobytes).	5-512 Valor predeterminado: 512
Iniciar sesión	Permitir llamada de emergencia	Especifique si el usuario puede realizar llamadas telefónicas de emergencia desde su dispositivo.	Sí, No Valor predeterminado: No

Categoría	Nombre de la política	Descripción	Intervalo de valor y valor predeterminado
Iniciar sesión	Acción de bloqueo de cuenta en PPC	Especifique la acción que se realizará cuando el dispositivo no haya podido comunicarse con PolicyServer tal como se especifica en la política Período de bloqueo de cuenta. Las acciones son: • Borrar: se borrará todo el contenido del dispositivo. • Autenticación remota: se requiere que el usuario realice una autenticación remota.	Borrar, Autenticación remota Valor predeterminado: Autenticación remota
Iniciar sesión	Tiempo de espera del dispositivo PPC	Especifique la cantidad de minutos que se mostrará la pantalla de autenticación mientras el dispositivo está inactivo.	0-60 Valor predeterminado: 1
Iniciar sesión	Ejecución tras inicio de sesión en PPC	Especifique una aplicación que se iniciará en el dispositivo tras una correcta autenticación.	Entre 1 y 255 caracteres Valor predeterminado: N/D
Contraseña	Métodos de autenticación en PPC	Especifique los métodos de autenticación permitidos en el dispositivo PPC.	Fijo, Código de color, PIN, Remoto Valor predeterminado: Fijo
PPC	Borrado de datos de soportes durante el barrido en PPC	El borrado del dispositivo borra los datos del soporte montado.	Sí, No Valor predeterminado: No

Políticas de FileArmor

Esta sección explica las opciones configurables para todas las políticas de la empresa que afecten a los clientes de FileArmor.

Políticas de equipos

Políticas que controlar los derechos de instalación en dispositivos con FileArmor instalado.

TABLA 3-11. Políticas de equipos de FileArmor

CATEGORÍA	NOMBRE DE LA POLÍTICA	DESCRIPCIÓN	INTERVALO DE VALOR Y VALOR PREDETERMINADO
Equipo	Permitir al usuario desinstalar	Esta política especifica si un usuario que no es administrador puede desinstalar la aplicación de punto final.	Sí, No Valor predeterminado: Sí

Políticas de cifrado

Políticas que controlan cómo se gestiona el cifrado en dispositivos con FileArmor.

TABLA 3-12. Políticas de cifrado de FileArmor

CATEGORÍA	NOMBRE DE LA POLÍTICA	DESCRIPCIÓN	INTERVALO DE VALOR Y VALOR PREDETERMINADO
	Permitir eliminación segura	Especifique si desea permitir que el usuario elimine archivos.	Sí, No Valor predeterminado: Sí

Categoría	Nombre de la política	Descripción	Intervalo de valor y valor predeterminado
	Desactivar unidad óptica	Desactive el acceso a unidades de CD o DVD.	Sí, No Valor predeterminado: No
	Clave de cifrado utilizada	• Clave del usuario: elija una clave única para el usuario. • Clave de grupo: elija una clave única para el grupo, de forma que todos los usuarios del grupo también tendrán acceso a los archivos. • Clave de empresa: elija una clave única para la empresa, de forma que todos los usuarios de la empresa también tendrán acceso a los archivos.	Clave de usuario, Clave de grupo, Clave de empresa Valor predeterminado: Clave de grupo
	Método de cifrado permitido	Elija los métodos permitidos para cifrar los archivos: 1. Clave de usuario 2. Clave de grupo 3. Contraseña creada por el usuario 4. Certificados digitales	Clave de usuario única, Clave única de grupo, Cifrar con contraseña estática, Cifrar con certificado Valor predeterminado: Todos
Soportes extraíbles	Cifrado completo del dispositivo	Especifique se si cifrarán todos los archivos y carpetas del soporte extraíble.	Sí, No Valor predeterminado: No

Categoría	Nombre de la política	Descripción	Intervalo de valor y valor predeterminado
Soportes extraíbles	Dispositivos USB permitidos	Especifique los dispositivos USB permitidos.	Cualquiera, KeyArmor Valor predeterminado: Cualquiera
Soportes extraíbles	Desactivar unidad USB	Desactivar la unidad USB cuando no haya una sesión iniciada, desactivar siempre y no desactivar nunca la unidad.	Siempre, Desconectado, Nunca Valor predeterminado: Desconectado
Soportes extraíbles	Carpetas que cifrar en soportes extraíbles	Se asigna la letra de unidad y el valor de política corresponde a un dispositivo de soportes extraíbles válido. Las carpetas que no existen se crearán. Si no se especifica una letra de unidad, todos los dispositivos de soportes extraíbles conectados al dispositivo al iniciar sesión utilizarán los valores de la política.	Entre 1 y 255 caracteres Valor predeterminado: N/D
Soportes extraíbles	Cifrado completo del dispositivo	Especifique si se cifrarán todos los archivos y carpetas del soporte extraíble.	Sí, No Valor predeterminado: No

Categoría	Nombre de la política	Descripción	Intervalo de valor y valor predeterminado
	Especifique carpetas que cifrar	Enumere las carpetas que se cifrarán en la unidad de disco duro. Las carpetas que no existen se crearán. Además se debe asignar una letra de unidad válida al disco duro. Un valor de política correcto es C:\EncryptedFolder.	Entre 1 y 255 caracteres Valor predeterminado: `%DESKTOP%\FileArmor Encrypted`

Políticas de inicio de sesión

Políticas de seguridad que controlan el inicio de sesión en FileArmor.

Tabla 3-13. Políticas de inicio de sesión de FileArmor

Categoría	Nombre de la política	Descripción	Intervalo de valor y valor predeterminado
	Métodos de autenticación permitidos	Especifique el tipo o tipos de autenticación que se pueden usar	Fijo, Código de colores, PIN, Tarjeta inteligente, RSA Valor predeterminado: Fijo

Categoría	Nombre de la política	Descripción	Intervalo de valor y valor predeterminado
	Acción de dispositivo bloqueado	Acción que se realizará cuando se bloquee el dispositivo	Tiempo de demora, Autenticación remota Valor predeterminado: Demora de tiempo
	Intentos de inicio de sesión fallidos permitidos	Número de intentos de inicio de sesión que se permiten antes de utilizar el tiempo de demora del bloqueo del dispositivo. 0 permite intentos ilimitados.	0-100 Valor predeterminado: 5
Aviso legal	Hora de visualización del aviso legal	Especifique cuándo se debe mostrar el aviso legal configurado al usuario. **Nota** Esta política solo se encuentra disponible para PolicyServer 3.1.3 (o posterior). Además, el aviso legal no se mostrará en los puntos finales en los que se ejecute FileArmor 3.1.3 o versiones anteriores.	Instalación, Inicio Valor predeterminado: Inicio

Categoría	Nombre de la política	Descripción	Intervalo de valor y valor predeterminado
Aviso legal	Texto del aviso legal	Especifique el cuerpo del aviso legal. **Nota** Esta política solo se encuentra disponible para PolicyServer 3.1.3 (o posterior). Además, el aviso legal no se mostrará en los puntos finales en los que se ejecute FileArmor 3.1.3 o versiones anteriores.	Insertar archivo Valor predeterminado: N/D
	Tiempo de demora del bloqueo del dispositivo	Bloquea el dispositivo durante x minutos si el usuario supera los intentos fallidos permitidos.	0-999,999 Valor predeterminado: 1

Políticas de contraseña

Políticas que controlan contraseñas de FileArmor.

Tabla 3-14. Políticas de contraseñas de FileArmor

Nombre de la política	Descripción	Intervalo de valor y valor predeterminado
Forzar comunicación con el servidor	Hace que FileArmor se comunique con el servidor después de un período de X días. 0 hará que FileArmor sea independiente	0-999 Valor predeterminado: 360

Nombre de la política	Descripción	Intervalo de valor y valor predeterminado
Símbolo físico requerido	Haga que los usuarios utilicen un símbolo físico (tarjetas inteligentes) para iniciar sesión.	Sí, No Valor predeterminado: No

Políticas de MobileSentinel

En esta sección se describen las opciones configurables para MobileSentinel. Full Disk Encryption usa políticas de MobileSentinel.

Políticas comunes

Políticas para todos los dispositivos que usan MobileSentinel.

Tabla 3-15. Políticas comunes de MobileSentinel

Categoría	Nombre de la política	Descripción	Intervalo de valor y valor predeterminado
Común	Conformidad	Políticas de conformidad para todos los dispositivos.	
Común > **Conformidad**	Tiempo de espera de sincronización	Especifique el número de días que permite que un dispositivo inalámbrico no se sincronice con el PolicyServer. El dispositivo estará obligado a comunicarse con PolicyServer para su sincronización cuando transcurra el número especificado de días.	0-65.535 días Valor predeterminado: 1

Categoría	Nombre de la política	Descripción	Intervalo de valor y valor predeterminado
Común	Conformidad de red	Especifique el acceso a los recursos de red corporativos garantizando que los dispositivos cumplen la política de la empresa.	
Común > **Conformidad de red**	Dirección de red de conformidad	Especifique la dirección IP de la red que permite al dispositivo volver a sincronizarse con PolicyServer si no está en conformidad. Cuando un dispositivo no está en conformidad, esta será la única red a la que pueda acceder el dispositivo hasta que vuelva a estar en conformidad.	Entre 1 y 225 caracteres Valor predeterminado: N/D
Común > **Conformidad de red**	Máscara de red de red de conformidad	Especifique la dirección de la máscara de red para la dirección de red de conformidad (política Dirección de red de conformidad). Esta máscara y la dirección se utilizan para limitar el acceso de los dispositivos a los recursos de red fuera de los valores introducidos hasta que el dispositivo esté en conformidad.	Entre 1 y 225 caracteres Valor predeterminado: N/D
Común > **Conformidad de red**	Dirección del servidor de conformidad	Especifique la dirección de PolicyServer que se usará como host de los dispositivos inalámbricos de este grupo. La dirección del servidor para dispositivos inalámbricos es el servidor al que llaman los dispositivos, cuando el dispositivo recibe una solicitud de sincronización o cuando el dispositivo detecta que debe sincronizarse con el servidor para asegurarse de que se hayan actualizado las políticas.	Entre 1 y 225 caracteres Valor predeterminado: N/D

Políticas de PPC

Políticas específicas para el dispositivo PPC de MobileSentinel.

TABLA 3-16. Políticas de PPC de MobileSentinel

CATEGORÍA	NOMBRE DE LA POLÍTICA	DESCRIPCIÓN	INTERVALO DE VALOR Y VALOR PREDETERMINADO
PPC	Conformidad	Políticas específicas para el dispositivo PPC.	
PPC > **Conformidad**	Lista de objetos de conformidad en PPC	Especifique los objetos requeridos en el dispositivo PPC. El enrutamiento de red estará limitado a la red de conformidad si estos objetos no están presentes en el dispositivo.	Activar, Desactivar Valor predeterminado: Desactivar
PPC > **Lista de objetos de conformidad en PPC**	Restricción de red de conformidad en PPC	Determine si restringir el acceso a la red si el dispositivo no está en conformidad.	Sí, No Valor predeterminado: Sí
PPC > **Lista de objetos de conformidad en PPC**	Restauración automática de objeto en PPC	Establezca el valor de la política en Sí para que el objeto que falta en el dispositivo se restaure automáticamente. Defina este valor en No para dirigir al usuario a la dirección URL especificada en la política URL de corrección de PPC.	
PPC > **Lista de objetos de conformidad en PPC** > **Restauración automática de objeto en PPC**	Objeto de restauración automática en PPC	Especifique el objeto que se restaurará en el dispositivo PPC si se activa la política de restauración automática en PPC.	

Categoría	Nombre de la política	Descripción	Intervalo de valor y valor predeterminado
PPC > **Lista de objetos de conformidad en PPC** > **Restauración automática de objeto en PPC**	Indicador de ejecución del objeto de restauración automática en PPC	Especifique las acciones que se realizarán en el objeto de corrección.	Copiar, Ejecutar Valor predeterminado: Copiar
PPC > **Lista de objetos de conformidad en PPC**	Información de conformidad del objeto en PPC	Especifique la información para usuarios si el objeto especificado no está en conformidad.	Entre 1 y 255 caracteres Valor predeterminado: N/D
PPC > **Lista de objetos de conformidad en PPC**	Nombre del objeto de PPC	Especifique el nombre de ruta completo para el objeto de conformidad.	Entre 1 y 255 caracteres Valor predeterminado: N/D
PPC > **Lista de objetos de conformidad en PPC**	Versión del objeto de PPC	Especifique el número de la versión mínima para el objeto de conformidad. Si este valor de política se deja en blanco, no se comprobará la conformidad de la versión del objeto.	Entre 1 y 255 caracteres Valor predeterminado: N/D
PPC > **Lista de objetos de conformidad en PPC**	URL de corrección de PPC	Especifique la dirección de la URL de corrección que se mostrará si la política Restauración automática de objeto en PPC se establece en No.	Entre 1 y 255 caracteres Valor predeterminado: N/D
PPC	Administración de dispositivos	Políticas específicas de la recopilación de los datos del dispositivo.	

Categoría	Nombre de la política	Descripción	Intervalo de valor y valor predeterminado
PPC > **Administración del dispositivo**	Recopilar intervalo de atributos del dispositivo	Recopile información clave sobre el hardware y el software cada X días; 0 = desactivado.	0-365 días Valor predeterminado: 30
PPC > **Administración del dispositivo**	Recopilar intervalo de información del directorio	Realice una instantánea de los archivos y directorios cada X días; 0 = desactivado.	0-365 días Valor predeterminado: 7
PPC	Desactivar Bluetooth	Desactive o active el uso de la radio BlueTooth.	Sí, No Valor predeterminado: No
PPC	Desactivar nuevas aplicaciones en PPC	Desactive o active la adición de nuevas aplicaciones mediante programas de instalación de Windows Mobile.	Sí, No Valor predeterminado: No
PPC	Desactivar nuevas aplicaciones en PPC	Desactive o active la adición de nuevas aplicaciones mediante programas de instalación de Windows Mobile.	Sí, No Valor predeterminado: No
PPC	Desactivar OBEX en PPC	Desactive o active el OBEX entrante mediante infrarrojos y BlueTooth.	Sí, No Valor predeterminado: No

Políticas de KeyArmor

Esta sección explica las opciones configurables para todas las políticas de la empresa que controlan dispositivos de KeyArmor.

Políticas antivirus

Políticas de seguridad para el control de antivirus en dispositivos de KeyArmor.

TABLA 3-17. Políticas antivirus de KeyArmor

NOMBRE DE LA POLÍTICA	DESCRIPCIÓN	INTERVALO DE VALOR Y VALOR PREDETERMINADO
Acción de archivo infectado	Indica qué acción de corrección realizar con cada archivo infectado encontrado.	Eliminar archivo, Eliminar dispositivo Valor predeterminado: Eliminar archivo
Reparar archivo infectado primero	Indica si intentar reparar los archivos infectados encontrados antes de realizar la acción especificada por la política de acción con archivo infectado.	Sí, No Valor predeterminado: Sí
Frecuencia de actualización	Define la frecuencia de actualización del antivirus en horas. Un valor de 0 indica que nunca se solicitarán actualizaciones.	Entre 0 y 9.999 horas Valor predeterminado: 1
Fuente de actualización	Una lista ordenada de direcciones URL del servidor del proveedor con las que contactar para obtener actualizaciones. Si la lista está vacía, se usará la ubicación predeterminada definida por la aplicación.	Entre 1 y 255 caracteres Valor predeterminado: N/D

Políticas de seguridad de KeyArmor

Políticas de seguridad para controlar KeyArmor.

TABLA 3-18. Políticas de KeyArmor

NOMBRE DE LA POLÍTICA	DESCRIPCIÓN	INTERVALO DE VALOR Y VALOR PREDETERMINADO
Interruptor de borrado de contenido	Especifique una secuencia de caracteres que, cuando se escriba, se borrará todo el contenido del dispositivo.	Entre 1 y 255 caracteres Valor predeterminado: N/D
Tiempo de espera de inactividad	Si no se accede al dispositivo de KeyArmor en X minutos, se cerrará la sesión en el dispositivo	1 - 999 Valor predeterminado:15

Políticas de inicio de sesión

Políticas de seguridad que controlan el inicio de sesión en KeyArmor.

TABLA 3-19. Políticas de inicio de sesión de KeyArmor

NOMBRE DE LA POLÍTICA	DESCRIPCIÓN	INTERVALO DE VALOR Y VALOR PREDETERMINADO
Permitir solo un usuario por dispositivo	Esta política determina si solo un usuario o varios usuarios pueden acceder a un dispositivo. El valor SÍ en esta política indica que solo un usuario puede tener acceso al dispositivo en un momento dado. **Nota** Esta política no afecta a las funciones de administrador o autenticador.	Sí, No Valor predeterminado: No

Nombre de la política	Descripción	Intervalo de valor y valor predeterminado
Métodos de autenticación permitidos	Especifique el tipo o tipos de autenticación que se pueden usar.	Fijo, Código de colores, PIN, Tarjeta inteligente, RSA Valor predeterminado: Fijo
Acción de dispositivo bloqueado	Especifique la acción que se realizará cuando el dispositivo no haya podido comunicarse con PolicyServer tal como se especifica en la política de tiempo de demora del bloqueo del dispositivo.	Borrar, Autenticación remota, Tiempo de demora Valor predeterminado: Autenticación remota
Intentos de inicio de sesión fallidos permitidos	Número de intentos de inicio de sesión que se permiten antes de utilizar el tiempo de demora del bloqueo del dispositivo. 0 permite intentos ilimitados.	0 - 100 Valor predeterminado: 5
Tiempo de demora del bloqueo del dispositivo	Bloquea el dispositivo durante x minutos si el usuario supera los intentos fallidos permitidos.	1 -999,999 Valor predeterminado: 5

Nombre de la política	Descripción	Intervalo de valor y valor predeterminado
Sincronización de contraseñas	Esta política determina si usuarios de un grupo pueden establecer una contraseña y usarla en otros dispositivos sin necesidad de registrarse mediante una contraseña de un único uso. Esta política solo afecta a los tipos de contraseña fija, de PIN, de código de colores y de certificado. Los esquemas de contraseñas de terceros, como son las contraseñas de dominio de Microsoft Windows y RSA SecurID, no se ven afectados.	Sí, No Valor predeterminado: No

Políticas de mensajes de notificación

Mensajes que se mostrarán a los usuarios del dispositivo de KeyArmor.

Tabla 3-20. Políticas de mensajes de notificación de KeyArmor

Nombre de la política	Descripción	Intervalo de valor y valor predeterminado
Si se encuentra	Especifique la información que se mostrará en el dispositivo durante el bloqueo del dispositivo.	Entre 1 y 4096 caracteres Valor predeterminado: N/D
Aviso legal	Avisos legales que mostrar al usuario.	Insertar archivo con entre 1 y 255 caracteres Valor predeterminado: N/D
Mostrar aviso legal al insertar	Seleccione si se mostrará al usuario una notificación como primera pantalla cuando se inserta el dispositivo KeyArmor en un dispositivo.	Sí, No Valor predeterminado: No

Nombre de la política	Descripción	Intervalo de valor y valor predeterminado
Información de asistencia	Muestre la información del departamento de asistencia o información de contacto del administrador.	Entre 1 y 4096 caracteres Valor predeterminado: N/D

Políticas de conexión de PolicyServer

Políticas para conectarse a PolicyServer con dispositivos de KeyArmor.

Tabla 3-21. Políticas de conexión de PolicyServer

Nombre de la política	Descripción	Intervalo de valor y valor predeterminado
Acción si no hay contacto	Acción que se llevará a cabo cuando el dispositivo de KeyArmor no se haya conectado a PolicyServer en el tiempo especificado por Tiempo de desconexión antes de conexión forzosa.	Tiempo de demora, Autenticación remota, Borrado Valor predeterminado: Autenticación remota
Debe estar conectado a PolicyServer	Fuerce al usuario a conectarse a PolicyServer para acceder a los archivos en USB.	Sí, No Valor predeterminado: No
Tiempo de desconexión antes de conexión forzosa	Cantidad de tiempo en días antes de que el usuario deba conectarse a PolicyServer. 0 indica que el dispositivo de KeyArmor no necesita conectarse a PolicyServer.	0 - 999 Valor predeterminado: 360
Acción secundaria si no hay contacto	Acción que se llevará a cabo cuando el dispositivo de KeyArmor no se haya autenticado en PolicyServer y haya transcurrido el Período de acción secundaria.	Borrado, Autenticación remota, Ninguna Valor predeterminado: Ninguno

Nombre de la política	Descripción	Intervalo de valor y valor predeterminado
Período de acción secundaria	Período de tiempo secundario en una cantidad de días X antes de que se aplique la acción secundaria.	0 - 999 Valor predeterminado: 0

Políticas de DriveArmor

Esta sección explica las opciones configurables para todas las políticas de la empresa que afecten a los clientes de Full Disk Encryption.

Importante

Las políticas de DriveArmor solo están disponibles en PolicyServer 3.1.3, si PolicyServer se actualizó desde una versión anterior que tenía las políticas de DriveArmor configuradas.

Políticas de autenticación

Políticas que gobiernan la autenticación en dispositivos de DriveArmor.

Tabla 3-22. Políticas de autenticación de DriveArmor

Categoría	Nombre de la política	Descripción	Intervalo de valor y valor predeterminado
Inicio de sesión local	Métodos de autenticación permitidos	Especifique el tipo o tipos de métodos de autenticación que se pueden usar.	Fijo, Código de color, PIN Valor predeterminado: Todos

Categoría	Nombre de la política	Descripción	Intervalo de valor y valor predeterminado
Inicio de sesión local	Acción de dispositivo bloqueado	Especifique la acción que se realizará cuando se bloquee el dispositivo. Las acciones son: • Borrar: se borrará todo el contenido del dispositivo. • Autenticación remota: se requiere que el usuario realice una autenticación remota. • Tiempo de demora: realiza la acción de la política de tiempo de demora del bloqueo del dispositivo.	Tiempo de demora, Borrar, Autenticación remota Valor predeterminado: Demora de tiempo
Inicio de sesión local	Intentos fallidos permitidos	Especifique el número de intentos de inicio de sesión que se permiten antes de utilizar el tiempo de demora del bloqueo del dispositivo.	0-255 Valor predeterminado: 10
Inicio de sesión local	Tiempo de demora del bloqueo del dispositivo	Bloquea el dispositivo durante x minutos si el usuario supera las reglas de la política Intentos fallidos permitidos.	1-1000000 Valor predeterminado: 1
Autenticación	Inicio de sesión de red	Especifique políticas relacionadas con la autenticación en el dispositivo que puede incluir la red.	
Inicio de sesión de red	Autenticación RSA	Especifique si se verificará a los usuarios en un servidor RSA ACE mediante SecurID.	Sí, No Valor predeterminado: No

Categoría	Nombre de la política	Descripción	Intervalo de valor y valor predeterminado
Autenticación	Autenticación de símbolo	La comprobación de certificados mediante OCSP permite la revocación de certificados no válidos a través de la entidad emisora de certificados (CA). Las subpolíticas solo son visibles cuando se habilita esta política.	Sí, No Valor predeterminado: N/D
Autenticación de símbolo	Validación de OCSP	La comprobación de certificados mediante OCSP permite la revocación de certificados no válidos a través de la entidad emisora de certificados (CA). Las subpolíticas solo son visibles cuando se habilita esta política.	Sí, No Valor predeterminado: N/D
Autenticación de símbolo > **Validación de OCSP**	Certificados CA de OCSP	Certificados de entidades emisoras de certificados.	0-1024 Valor predeterminado: N/D
Autenticación de símbolo > **Validación de OCSP**	Respondedores OCSP	Certificados de entidades emisoras de certificados.	Sí, No Valor predeterminado: Sí
Validación de OCSP > **Respondedores OCSP**	Certificado de respondedor OCSP	Certificados de entidades emisoras de certificados.	0-1024 Valor predeterminado: N/D
Validación de OCSP > **Respondedores OCSP**	URL de respondedor OCSP	Certificados de entidades emisoras de certificados.	0- 1024 Valor predeterminado: N/D

Categoría	Nombre de la política	Descripción	Intervalo de valor y valor predeterminado
Autenticación de símbolo	Transferencia de símbolo	Transfiera el símbolo al escritorio GINA para un procesamiento adicional durante el proceso de inicio.	Sí, No Valor predeterminado: No

Nota

OCSP son las siglas de Online Certificate Status Protocol (protocolo de estado de certificados en línea).

Políticas de comunicaciones

Especifique políticas que controlen la comunicación y la información de DriveArmor.

Tabla 3-23. Políticas de comunicaciones de DriveArmor

Categoría	Nombre de la política	Descripción	Intervalo de valor y valor predeterminado
Comunicaciones	Acción de bloqueo de cuenta	Especifique la acción que se realizará cuando el dispositivo no haya podido comunicarse con PolicyServer tal como se especifica en la política Período de bloqueo de cuenta. • Borrar: se borrará todo el contenido del dispositivo • Autenticación remota: se requiere que el usuario realice una autenticación remota • Ignorar: no realizar ninguna acción	Borrar, Autenticación remota, Ignorar Valor predeterminado: Ignorar

Categoría	Nombre de la política	Descripción	Intervalo de valor y valor predeterminado
Comunicaciones	Período de bloqueo de cuenta	Especifique el número de días que el cliente puede estar sin mantener la comunicación con PolicyServer.	0-1000000 Valor predeterminado: 360
Comunicaciones	Información	Especifique políticas que proporcionen información al usuario.	
Información	Si se encuentra	Especifique la información que se mostrará en el dispositivo durante el bloqueo del dispositivo.	Entre 1 y 1024 caracteres Valor predeterminado: N/D
Información	Aviso legal	Especifique si se debe mostrar un aviso legal.	
Información > **Aviso legal**	Hora de visualización del aviso legal	Especifique cuándo se debe mostrar el aviso legal configurado al usuario.	Instalación, Inicio Valor predeterminado: Inicio
Información > **Aviso legal**	Texto del aviso legal	Especifique el cuerpo del aviso legal.	Insertar archivo Valor predeterminado: N/D
Información	Información de asistencia	Muestre la información del departamento de asistencia o información de contacto del administrador.	Entre 1 y 1024 caracteres Valor predeterminado: N/D

Categoría	Nombre de la política	Descripción	Intervalo de valor y valor predeterminado
Comunicaciones	Intervalo de sincronización	Especifique con qué frecuencia (en minutos) DriveArmor se comunica con PolicyServer desde el dispositivo para recibir información actualizada.	0-1000000 Valor predeterminado: 120

Políticas de dispositivo

Especifique políticas que controlen las acciones genéricas en el dispositivo con DriveArmor instalado.

Tabla 3-24. Políticas de dispositivo de DriveArmor

Nombre de la política	Descripción	Intervalo de valor y valor predeterminado
Permitir al usuario acceso de administración	Especifique si los usuarios pueden acceder a las utilidades de administración del sistema en el dispositivo.	Sí, No Valor predeterminado: No
Permitir al usuario desinstalar	Especifique si un usuario estándar de DriveArmor puede desinstalar DriveArmor.	Sí, No Valor predeterminado: No
Interruptor de borrado de contenido	Especifique una secuencia de caracteres; cuando se escriba se destruirá el dispositivo.	Entre 1 y 255 caracteres Valor predeterminado: N/D
Omitir arranque previo	Especifique si se debe omitir el arranque previo.	Sí, No Valor predeterminado: No

Políticas comunes

Esta sección explica las opciones configurables para todas las políticas de la empresa que afecten a todos los productos de Endpoint Encryption.

Política de agente

TABLA 3-25. Políticas comunes de agentes

NOMBRE DE LA POLÍTICA	DESCRIPCIÓN	INTERVALO DE VALOR Y VALOR PREDETERMINADO
Intervalo de sincronización	Especifique con qué frecuencia (en minutos) se comunica la aplicación con PolicyServer desde el dispositivo para recibir información actualizada.	1-1440 Valor predeterminado: 30

Políticas de autenticación

Especifique políticas que controlan la autenticación en dispositivos desde todas las aplicaciones de Endpoint Encryption.

TABLA 3-26. Políticas comunes de autenticación

CATEGORÍA	NOMBRE DE LA POLÍTICA	DESCRIPCIÓN	INTERVALO DE VALOR Y VALOR PREDETERMINADO
Inicio de sesión local	Contraseña de administrador	Especifique las políticas relacionadas con la autenticación local solo en el dispositivo.	

Categoría	Nombre de la política	Descripción	Intervalo de valor y valor predeterminado
Inicio de sesión local > **Contraseña de administrador**	Tipos de caracteres permitidos	Especifique si las contraseñas pueden contener caracteres alfabéticos, numéricos, especiales o una combinación de estos caracteres.	Alfabético, Numérico, Especial Valor predeterminado : Todos
Inicio de sesión local > **Contraseña de administrador**	Puede contener el nombre de usuario	Especifique si se puede incluir el nombre de usuario en la contraseña.	Sí, No Valor predeterminado : Sí
Inicio de sesión local > **Contraseña de administrador**	Caracteres consecutivos permitidos	Especifique la cantidad de caracteres consecutivos permitidos en una contraseña.	0-255 Valor predeterminado : 3
Inicio de sesión local > **Contraseña de administrador**	Longitud mínima	Especifique la longitud mínima permitida para contraseñas.	0-255 Valor predeterminado : 6
Inicio de sesión local > **Contraseña de administrador**	Retención del historial de contraseñas	Especifique el número de contraseñas anteriores que el usuario no puede usar.	0-255 Valor predeterminado : 0
Inicio de sesión local > **Contraseña de administrador**	Cantidad de caracteres requerida	Especifique la cantidad de caracteres alfabéticos que se deben usar en una contraseña.	0-255 Valor predeterminado : 0
Inicio de sesión local > **Contraseña de administrador**	Cantidad de caracteres en minúscula requerida	Especifique la cantidad de caracteres en minúscula que se deben usar en una contraseña.	0-255 Valor predeterminado : 0

Categoría	Nombre de la política	Descripción	Intervalo de valor y valor predeterminado
Inicio de sesión local > **Contraseña de administrador**	Cantidad de números requerida	Especifique la cantidad de caracteres numéricos que se deben usar en una contraseña.	0-255 Valor predeterminado : 0
Inicio de sesión local > **Contraseña de administrador**	Cantidad de caracteres especiales requerida	Especifique la cantidad de caracteres especiales que se deben usar en una contraseña.	0-255 Valor predeterminado : 0
Inicio de sesión local > **Contraseña de administrador**	Cantidad de caracteres en mayúscula requerida	Especifique la cantidad de caracteres en mayúscula que se deben usar en una contraseña.	0-255 Valor predeterminado : 0
Inicio de sesión local	Autoayuda	Especifique las políticas que se usan para la autoayuda.	
Inicio de sesión local > **Autoayuda**	Cantidad de preguntas	Especifique la cantidad de preguntas que se deben responder correctamente para autenticar al usuario.	1-6 Valor predeterminado : 1
Inicio de sesión local > **Autoayuda**	Pregunta personal	Especifique la pregunta o preguntas personales utilizadas para la autoayuda.	1-1024 Valor predeterminado : N/D
Inicio de sesión local	Contraseña del usuario	Especifique las políticas que se usan para las contraseñas de usuarios.	
Inicio de sesión local > **Contraseña de usuario**	Permitir cambio de contraseña sin conexión	Especifique si los usuarios pueden cambiar su contraseña sin estar conectados a PolicyServer.	Sí, No Valor predeterminado : No

Categoría	Nombre de la política	Descripción	Intervalo de valor y valor predeterminado
Inicio de sesión local > **Contraseña de usuario**	Tipos de caracteres permitidos	Especifique si las contraseñas pueden contener caracteres alfabéticos, numéricos, especiales o una combinación de estos caracteres.	Alfabético, Numérico, Especial Valor predeterminado : Todos
Inicio de sesión local > **Contraseña de usuario**	Puede contener el nombre de usuario	Especifique si se puede incluir el nombre de usuario en la contraseña.	Sí, No Valor predeterminado : Sí
Inicio de sesión local > **Contraseña de usuario**	Cambiar contraseña cada	Especifique (en días) cuándo forzar a un usuario a cambiar su contraseña.	1-1000000 Valor predeterminado : 60
Inicio de sesión local > **Contraseña de usuario**	Caracteres consecutivos permitidos	Especifique la cantidad de caracteres consecutivos permitidos en una contraseña.	0-255 Valor predeterminado : 3
Inicio de sesión local > **Contraseña de usuario**	Longitud mínima	Especifique la longitud mínima permitida para contraseñas.	0-255 Valor predeterminado : 6
Inicio de sesión local > **Contraseña de usuario**	Retención del historial de contraseñas	Especifique el número de contraseñas anteriores que el usuario no puede usar.	0-255 Valor predeterminado : 0
Inicio de sesión local > **Contraseña de usuario**	Cantidad de caracteres requerida	Especifique la cantidad de caracteres alfabéticos que se deben usar en una contraseña.	0-255 Valor predeterminado : 0

Categoría	Nombre de la política	Descripción	Intervalo de valor y valor predeterminado
Inicio de sesión local > **Contraseña de usuario**	Cantidad de caracteres en minúscula requerida	Especifique la cantidad de caracteres en minúscula que se deben usar en una contraseña.	0-255 Valor predeterminado: 0
Inicio de sesión local > **Contraseña de usuario**	Cantidad de números requerida	Especifique la cantidad de caracteres numéricos que se deben usar en una contraseña.	0-255 Valor predeterminado: 0
Inicio de sesión local > **Contraseña de usuario**	Cantidad de caracteres especiales requerida	Especifique la cantidad de caracteres especiales que se deben usar en una contraseña.	0-255 Valor predeterminado: 0
Inicio de sesión local > **Contraseña de usuario**	Cantidad de caracteres en mayúscula requerida	Especifique la cantidad de caracteres en mayúscula que se deben usar en una contraseña.	0-255 Valor predeterminado: 0
Inicio de sesión local > **Contraseña de usuario**	Nombre de usuario distingue entre mayúsculas y minúsculas	Especifique si el nombre de usuario distingue entre mayúsculas y minúsculas	Sí, No Valor predeterminado: No
Inicio de sesión de red	Nombre distintivo	Opcional: Especifique el nombre distintivo del servidor de autenticación. Si no se especifica ningún nombre distintivo, se utilizará la convención de nomenclatura predeterminada del servidor LDAP.	1-255 Valor predeterminado: N/D
Inicio de sesión de red	Autenticación de dominios	Especifica si se deben usar las credenciales de Windows para autenticarse.	Sí, No Valor predeterminado: No

Categoría	Nombre de la política	Descripción	Intervalo de valor y valor predeterminado
Inicio de sesión de red	Nombre del dominio	Nombre de NetBIOS del dominio para inicio de sesión único. El nombre predeterminado es el valor de NetBIOS que utiliza PolicyServer.	1-255 Valor predeterminado: N/D
Inicio de sesión de red	Nombre de host	Especifique el nombre de host. El nombre de host puede ser un nombre de dominio.	1-255 Valor predeterminado: N/D
Inicio de sesión de red	Número de puerto	Opcional: 0 = usar predeterminada. Especifica el puerto que se usará para la conexión. Si no se especifica ningún número de puerto, el proveedor LDAP usa el número de puerto predeterminado.	0-65535 Valor predeterminado: 0
Inicio de sesión de red	Tipo de servidor	Tipo de servidor utilizado para autenticar las solicitudes del usuario del cliente.	LDAP, LDAProxy Valor predeterminado: LDAP
Autenticación	Recordar usuario entre inicios de sesión	Recordar el último nombre de usuario usado y mostrarlo en la pantalla de autenticación.	Sí, No Valor predeterminado: Sí

Capítulo 4

Trabajar con grupos, usuarios y dispositivos

Endpoint Encryption utiliza tanto la autenticación basada en funciones como la basada en identidades para proteger los datos en los puntos finales. La configuración adecuada de usuarios, grupos y dispositivos garantiza que los datos permanezcan cifrados para los usuarios no autorizados y, de este modo, se evite el riesgo de una pérdida de datos debido a una liberación accidental de información o a un sabotaje deliberado.

En este capítulo se describen los siguientes temas:

- *Trabajar con grupos en la página 4-2*
- *Trabajar con grupos sin conexión en la página 4-5*
- *Trabajar con usuarios en la página 4-10*
- *Trabajar con contraseñas en la página 4-24*
- *Trabajar con dispositivos en la página 4-31*

Trabajar con grupos

Los grupos se administran en MMC de PolicyServer y se componen de los siguientes tipos:

TABLA 4-1. Tipos de grupos de PolicyServer

GRUPO	DESCRIPCIÓN
Grupos superiores	Son los grupos de mayor nivel dentro de la empresa. Cada grupo superior tiene un único nodo por debajo de la empresa.
Subgrupos	Son grupos creados dentro de un grupo superior. Un subgrupo heredará las políticas de su grupo principal. • La herencia de políticas solo sucede cuando se crea un subgrupo. • Los cambios en las políticas de un grupo de nivel superior no se filtran hacia abajo a los subgrupos existentes. • Las políticas de subgrupos no pueden ser más permisivas que las de los grupos principales.

Nota

- Los subgrupos heredan todas las políticas existentes del grupo principal. No obstante, los administradores pueden agregar usuarios y dispositivos de forma independiente.
- Al agregar un usuario a un subgrupo, el usuario no se agrega de forma automática al grupo superior. Sin embargo, puede agregar un mismo usuario tanto al grupo superior como al subgrupo.

Adición de un grupo superior

Los grupos simplifican la administración de aplicaciones, usuarios, políticas, subgrupos y dispositivos activados. Un grupo superior es el grupo que está en el nivel más alto.

Nota

Las cuentas de administrador o autenticador no se pueden agregar a grupos. Para crear un administrador de grupo, agregue un usuario y cambie sus permisos en el grupo.

Procedimiento

1. En el panel izquierdo, haga clic con el botón derecho en el nombre de la empresa y, a continuación, haga clic en **Agregar grupo superior**.



FIGURA 4-1. Adición de un grupo superior

Aparecerá la pantalla **Añadir nuevo grupo**.

2. Proporcione el nombre y la descripción del grupo.

3. Seleccione **Admitir dispositivos heredados** solamente si usa dispositivos heredados que no admitan codificación Unicode. Algunos dispositivos heredados no podrán comunicarse con PolicyServer mediante Unicode. Asigne los dispositivos Unicode y los dispositivos heredados a grupos distintos.

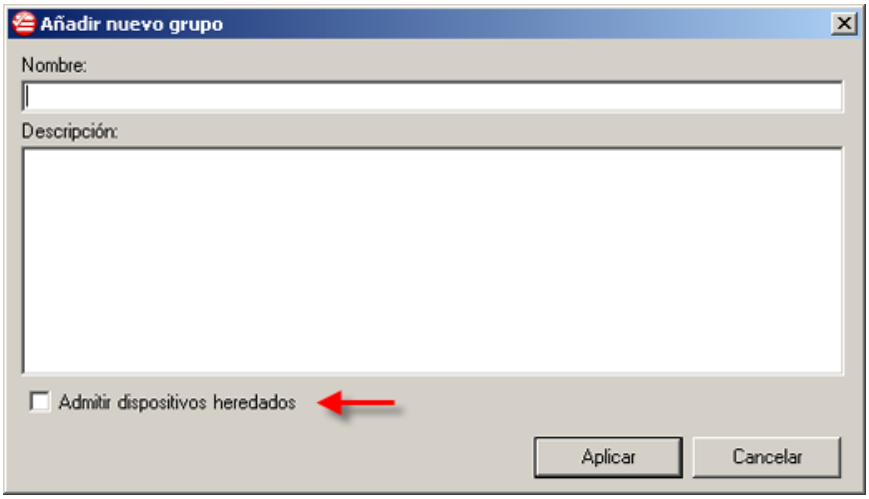


FIGURA 4-2. Añadir nuevo grupo

4. Haga clic en **Aplicar**.
5. En el mensaje de confirmación, haga clic en **Aceptar**.

   El nuevo grupo se agrega a la estructura de árbol del panel izquierdo.

Agregar un subgrupo

Los subgrupos heredan todas las políticas existentes del grupo principal. No obstante, los administradores pueden agregar usuarios y dispositivos de forma independiente.

Procedimiento

1. En la estructura de árbol del panel de la izquierda, haga clic con el botón derecho en un grupo y, a continuación, haga clic en**Agregar**.

   Aparecerá la pantalla **Añadir nuevo grupo**.

2. Siga los pasos en *Adición de un grupo superior en la página 2-5*, excepto el primer paso.

El nuevo grupo se agrega a la estructura de árbol dentro de la jerarquía del grupo superior.

Modificar un grupo

Procedimiento

1. En la estructura de árbol del panel de la izquierda, haga clic con el botón derecho en un grupo y, a continuación, haga clic en**Modificar**.

   Aparecerá la pantalla **Modificar grupo**.

2. Especifique los cambios y haga clic en **Aplicar**.

Eliminación de un grupo

Use la estructura de árbol para eliminar un grupo. Si elimina un grupo superior, también se eliminarán todos los subgrupos.

Procedimiento

1. En la estructura de árbol del panel de la izquierda, haga clic con el botón derecho en un grupo y, a continuación, haga clic en**Eliminar**.

   Aparecerá un mensaje de **Advertencia de PolicyServer**.

2. Haga clic en **Sí** para eliminar el grupo.

   El grupo seleccionado ya no volverá a aparecer en la estructura de árbol.

Trabajar con grupos sin conexión

Un grupo sin conexión es un grupo de clientes de punto final que no se conectan con PolicyServer durante la instalación. Las políticas, usuarios y dispositivos del grupo se

pueden exportar a un archivo y entregarlo a los clientes sin conexión. Cuando el grupo requiere cambios, se deben exportar estos a un nuevo archivo y entregar de nuevo al cliente de punto final sin conexión.

Las políticas se actualizan automáticamente cuando un cliente de punto final sin conexión se conecta a PolicyServer.



¡ADVERTENCIA!

Para los clientes de Full Disk Encryption que nunca se conectarán con PolicyServer, realice una instalación no administrada. No se requiere ningún grupo sin conexión ya que las políticas se administran mediante la Consola de recuperación.

Creación de un grupo sin conexión

Los grupos se pueden exportar para permitir la instalación de Full Disk Encryption y FileArmor en dispositivos que no necesitan o no pueden comunicarse con PolicyServer. Los archivos de instalación de la aplicación cliente deben estar disponibles desde el servidor en el que está instalado PolicyServer.



Nota

Los grupos exportados deben contener un usuario como mínimo. El nombre del grupo también debe ser solo alfanumérico.



¡ADVERTENCIA!

Los grupos sin conexión solo funcionan para DataArmor SP7 y versiones anteriores. Para los clientes de Full Disk Encryption que no se conectarán con PolicyServer, realice una instalación no administrada. Las políticas se administran mediante la Consola de recuperación.

Procedimiento

1. En el panel izquierdo, haga clic con el botón derecho en el grupo y seleccione **Exportar**.

   Aparecerá el Asistente de exportación de grupos de PolicyServer.

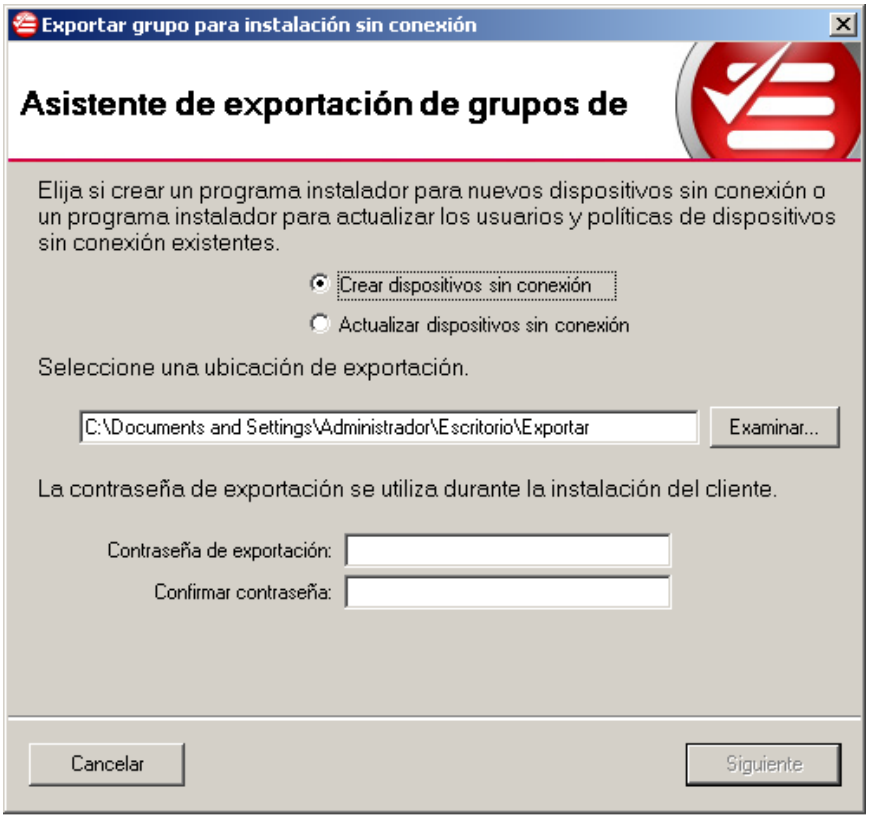


FIGURA 4-3. Asistente de exportación de grupos de PolicyServer

2. Seleccione **Crear dispositivos sin conexión**, especifique la ubicación de exportación y exporte la contraseña, y haga clic en **Siguiente**.

Nota

La contraseña de exportación se usa para autenticar el ejecutable en el cliente de punto final.

---

3. Haga clic en **Agregar** para examinar y cargar los programas de instalación de clientes de Endpoint Encryption.

TABLA 4-2. Nombres de archivos de instalación de Endpoint Encryption

ARCHIVO DE INSTALACIÓN	OBJETIVO
`DataArmorInstaller.exe`	Instala versiones antiguas de la aplicación cliente de Full Disk Encryption: DataArmor. DataArmor 3.0.12.861 o anterior funcionará con los grupos sin conexión. Para obtener información detallada sobre instalaciones administradas, consulte el Manual de instalación.
`TMFDEInstall.exe`	Instala la aplicación cliente de Full Disk Encryption. Esto no funcionará para todos los dispositivos sin conexión. Para obtener información detallada sobre instalaciones administradas, consulte el Manual de instalación.
`FASetup.msi`	Instala la aplicación cliente de FileArmor para sistemas operativos de 32 bits.
`FASetup(x64).msi`	Aplicación cliente de FileArmor para sistemas operativos de 64 bits.

Agregue todos los programas de instalación que sean necesarios. Por ejemplo, es posible que un grupo requiera Full Disk Encryption y FileArmor.

4. Haga clic en **Siguiente**.

5. En función del tipo de licencia, especifique el número de dispositivos en el que se instalará. El número de licencias disponibles se reduce con cada dispositivo.

6. Opcionalmente, especifique un **Prefijo de nombre de dispositivo**. PolicyServer usa el número de prefijo del dispositivo para generar un ID de dispositivo y una clave de cifrado de dispositivo únicos para cada dispositivo de este grupo.

7. Haga clic en **Siguiente**.

   Comienza la creación del grupo sin conexión.

8. Haga clic en **Finalizado** para generar el archivo de exportación en la ubicación especificada.

En el escritorio, se crea un archivo ejecutable generado llamado `Export`. Use este archivo para distribuir cambios en los grupos entre los clientes sin conexión.

Actualizar un grupo sin conexión

Siga estos pasos para crear una actualización para un grupo sin conexión.



¡ADVERTENCIA!

Para los clientes de Full Disk Encryption que no se conectarán con PolicyServer, realice una instalación no administrada. Las políticas se administran mediante la Consola de recuperación.

Procedimiento

1. En el panel izquierdo, haga clic con el botón derecho en el grupo y seleccione **Exportar**.

   Aparecerá el Asistente de exportación de grupos de PolicyServer.

2. Seleccione **Crear dispositivos sin conexión**.

3. Especifique la contraseña de exportación.

   Nota

   La contraseña de exportación se usa para autenticar el ejecutable en el cliente de punto final.

4. Haga clic en **Examinar** para especificar una ubicación en la que almacenar el

5. Haga clic en **Siguiente**.

   Comienza la creación del grupo sin conexión.

6. Haga clic en **Finalizado**.

   El archivo de exportación se generará en la ubicación especificada.

7. Instale el software en el dispositivo mediante la secuencia de comandos o el ejecutable generado. Para obtener más detalles, consulte la Guía de instalación de Endpoint Encryption.

Trabajar con usuarios

Para proporcionar una autenticación basada en identidad, Endpoint Encryption ofrece diferentes niveles de usuario, agregar o importar usuarios, asignar usuarios a grupos, administrar usuarios y eliminar usuarios.

Agregar usuarios a PolicyServer

Use los siguientes métodos para agregar usuarios a Endpoint Encryption:

- Agregar usuarios manualmente, de uno en uno
- Importar en bloque a muchos usuarios con un archivo CSV
- Usar un Explorador de directorio externo con Active Directory

Agregar un nuevo usuario empresarial

Nota

- El hecho de agregar un usuario a la empresa no asigna el usuario a ningún grupo.
- Agregar un usuario a un grupo lo agrega al grupo y a la empresa.

Procedimiento

1. Seleccione la empresa y abra **Usuarios**.
2. En el panel derecho, haga clic con el botón derecho en el espacio en blanco y seleccione **Agregar usuario**.

   Aparecerá la pantalla **Agregar nuevo usuario**.

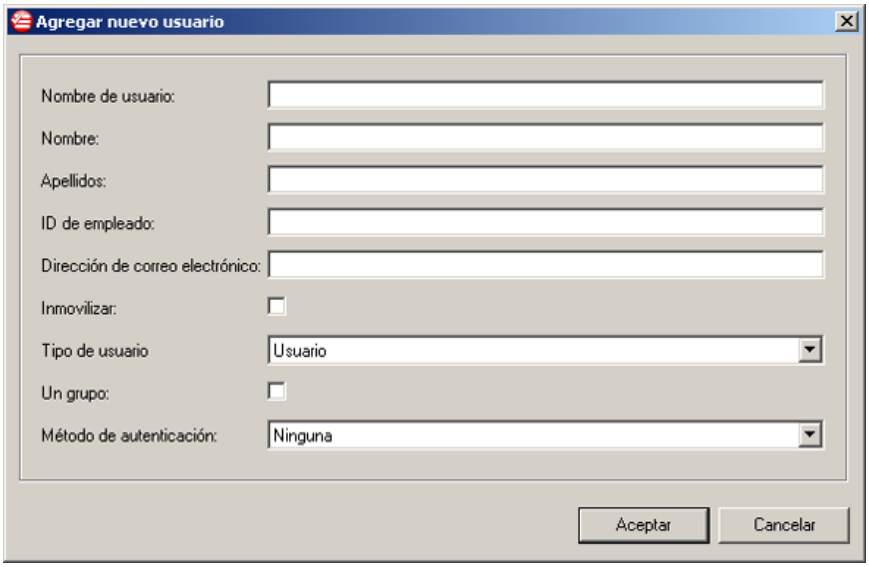


FIGURA 4-4. Pantalla Agregar nuevo usuario

3. Especifique la información de usuario. La información obligatoria es el nombre de usuario, el nombre y el apellido.

4. Solo seleccione **Inmovilizar** si la cuenta debiera estar temporalmente desactivada. Mientras esté inmovilizada, el usuario no podrá iniciar sesión en dispositivos.

5. Use el campo **Tipo de usuario** para definir los privilegios de la nueva cuenta. Los administradores y autenticadores empresariales no se pueden agregar a grupos.

6. Seleccione **Un grupo** para desactivar al usuario de la pertenencia a varios grupos.

7. Seleccione el **Método de autenticación**.

Nota

El método de autenticación predeterminado para los usuarios en **Ninguno**.

---

8. Haga clic en **Aceptar**.

Se ha agregado el nuevo usuario a esta empresa de PolicyServer. El usuario no podrá iniciar sesión en un dispositivo hasta que se agregue a un grupo.

Importación de usuarios desde un archivo CSV

Use un archivo con valores separados por comas (CSV) para importar varios usuarios de forma simultánea.

Use el siguiente formato:

```
nombre de usuario (requerido), nombre, apellido, ID de
empleado, dirección de correo electrónico.
```

Incluya una coma para los campos sin datos.



Nota

Cuando se usa la función para la importación en bloque de usuarios, todos los usuarios del archivo se agregan al mismo grupo. Cree un archivo para cada grupo de usuarios que desee importar.

Procedimiento

1. En el panel izquierdo, seleccione un grupo y, a continuación, haga clic en **Usuarios**.
2. En el panel derecho, haga clic con el botón derecho en el espacio en blanco y seleccione **Importar en bloque usuarios agregados**.

   Aparecerá la ventana para abrir archivos.
3. Busque el archivo CSV y haga clic en **Abrir**.
4. En el mensaje de confirmación, haga clic en **Aceptar**.

   Los usuarios del archivo se agregarán al grupo y a la empresa.

Importación de usuarios de Active Directory

Agregue usuarios de Active Directory a grupos de PolicyServer existentes mediante el Explorador de directorio externo. PolicyServer mantiene un directorio de usuarios independiente de la base de datos de Active Directory. Esto permite a PolicyServer proporcionar una seguridad absoluta a través del acceso a todos los dispositivos, privilegios de usuario y métodos de autenticación.

Para más información sobre la configuración de la integración de Active Directory, consulte la Guía de instalación de Endpoint Encryption.

Procedimiento

1. En el panel izquierdo, abra **Usuarios empresariales**, haga clic con el botón derecho en el panel derecho (espacio en blanco) y, a continuación, seleccione **Explorador de directorio externo**.

   Aparecerá la ventana **Importación de usuarios de Active Directory**.

2. Haga clic en **Edición** > **Conectar a dominio**.

3. Especifique el nombre de host del servidor LDAP de Active Directory.

4. Especifique un nombre de usuario y una contraseña con acceso al dominio de Active Directory.

5. Haga clic en **Aceptar**.

   Las cuentas de usuario se cargan en el panel derecho.

6. Haga clic en **Archivo** y seleccione **Agregar a empresa** o **Agregar a grupo**, según donde vaya a agregar los usuarios.

7. Haga clic en **Aceptar** para agregar los usuarios a la ubicación especificada.

   Aparecerá una ventana de confirmación.

8. Haga clic en **Aceptar** para confirmar.

   Aparecerá un mensaje sobre el estado de la importación.

9. Haga clic en **Aceptar**.

Encontrar un usuario

Resulta más rápido buscar los usuarios en el nivel de grupo; no obstante, esto es a costa de buscar en toda la empresa.

Procedimiento

1. En el panel izquierdo, abra **Usuarios empresariales** o expanda el grupo y haga clic en **Usuarios**.
2. En la esquina superior del panel derecho, haga clic en **Buscar**.

   Aparecerá la ventana **Filtro de búsqueda de usuarios**.

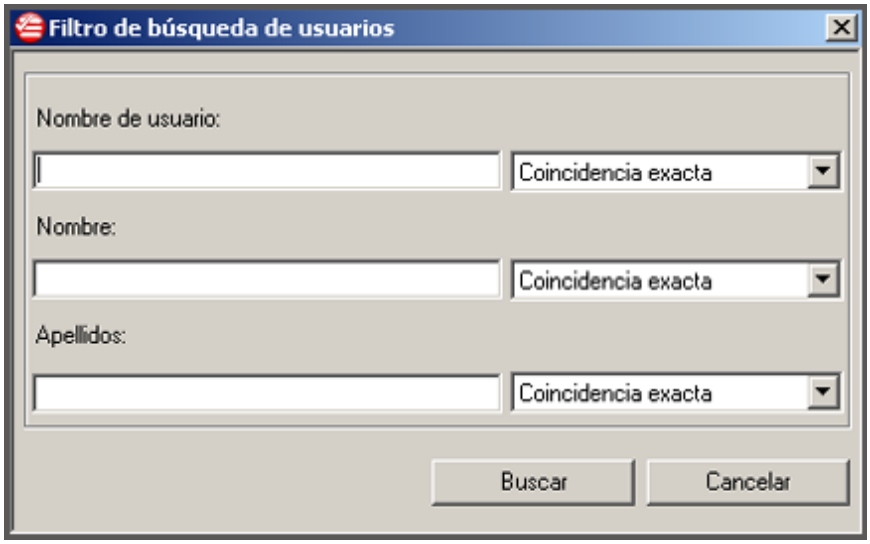


FIGURA 4-5. Ventana Filtro de búsqueda de usuarios

3. Especifique los detalles de búsqueda y haga clic en **Buscar**.

   Aparecerán todas las cuentas que coincidan con los criterios de búsqueda.

Nota

Si hay muchos usuarios, use el **Contador de páginas** para ir de una página a otra, o haga clic en **Borrar** para quitar todos los resultados.

Modificación de un usuario

Cualquier administrador de grupo puede cambiar la información de perfil de un usuario.

Nota

- Los cambios a nivel empresarial se aplican al usuario de forma universal, pero los cambios a nivel de grupo se aplican solamente en dicho grupo.

Procedimiento

1. Abra **Usuarios empresariales**.
2. En el panel derecho, haga clic con el botón derecho en el usuario y seleccione **Modificar usuario**.

   Aparecerá la pantalla **Modificar usuario**.
3. Realice los cambios necesarios. Si el método de autenticación cambia a **Contraseña fija**, proporcione la contraseña de usuario predeterminada.
4. Haga clic en **Aceptar**.
5. En el mensaje de confirmación, haga clic en **Aceptar**.

Ver la pertenencia a grupo de un usuario

Los administradores pueden ver los grupos de un usuario - si el usuario pertenece a varios grupos.

Procedimiento

1. Abra **Usuarios empresariales**.
2. Haga clic con el botón derecho en el usuario y seleccione **Lista de grupos**.

   Aparecerá la lista **Pertenencia a grupo**.

Agregar un nuevo usuario a un grupo

Nota

- El hecho de agregar un usuario a la empresa no asigna el usuario a ningún grupo.
- Agregar un usuario a un grupo lo agrega al grupo y a la empresa.

Procedimiento

1. Seleccione el grupo y abra **Usuarios**.
2. En el panel derecho, haga clic con el botón derecho en el espacio en blanco y seleccione **Agregar nuevo usuario**.

   Aparecerá la pantalla **Agregar nuevo usuario**.

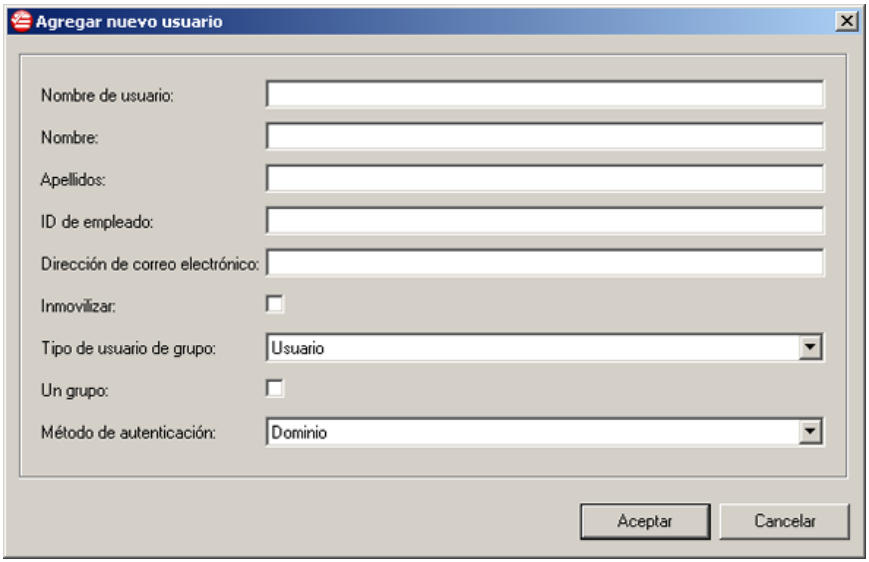


FIGURA 4-6. Pantalla Agregar nuevo usuario

3. Especifique la información de usuario. La información obligatoria es el nombre de usuario, el nombre y el apellido.

4. Solo seleccione **Inmovilizar** si la cuenta debiera estar temporalmente desactivada. Mientras esté inmovilizada, el usuario no podrá iniciar sesión en dispositivos.

5. Use el campo **Tipo de usuario de grupo** para definir los privilegios de la nueva cuenta. Los administradores y autenticadores empresariales no se pueden agregar a grupos.

6. Seleccione **Un grupo** para desactivar al usuario de la pertenencia a varios grupos.

7. Seleccione el **Método de autenticación**.

Nota

El método de autenticación predeterminado para los usuarios en **Ninguno**.

---

8. Haga clic en **Aceptar**.

El nuevo usuario se agrega al grupo seleccionado **y** a la empresa. El usuario ya puede iniciar una sesión en un dispositivo.

Agregar un usuario existente a un grupo

Un usuario se puede agregar a varios grupos.

Procedimiento

1. En el panel izquierdo, seleccione un grupo y, a continuación, haga clic en **Usuarios**.
2. En el panel derecho, haga clic con el botón derecho en el espacio en blanco y seleccione **Agregar usuario existente**.

   Aparecerá la pantalla **Agregar usuarios a grupo**.

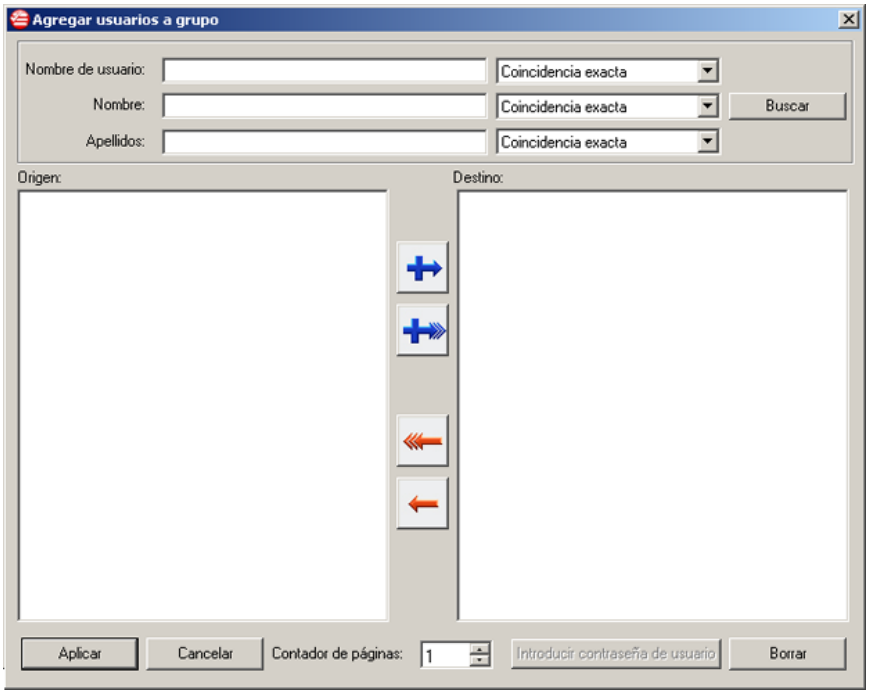


FIGURA 4-7. Pantalla Agregar usuarios a grupo

3. Especifique los detalles del usuario y haga clic en **Buscar**.

   Si hay alguna coincidencia, el campo **Fuente** se rellena con las cuentas.

4. Seleccione las cuentas de usuario de la lista y haga clic en la **flecha azul** para agregarlas. Consulte *Capítulo 2, Tabla 2-3: Iconos para agregar/eliminar usuarios en la página 2-12* para obtener controles adicionales.

TABLA 4-3. Iconos para agregar/eliminar usuarios

ICONOS CENTRALES	DESCRIPCIÓN
	Agregue un único usuario seleccionado al campo **Destino**.

Iconos centrales	Descripción
	Agregue todos los usuarios encontrados basados en el criterio de búsqueda al campo **Destino**.
	Elimine un único usuario seleccionado del campo **Destino**.
	Elimine todos los usuarios del campo **Destino**.

5. Para cambiar la contraseña de un usuario:

   a. En el campo **Destino**, resalte el usuario.

   b. Haga clic en **Introducir contraseña de usuario** ubicada en la parte inferior de la ventana.

   c. En la ventana que aparece, especifique el método de autenticación del usuario.

   d. Haga clic en **Aplicar**.

6. Haga clic en **Aplicar**.

   El usuario se ha agregado al grupo. Si el usuario solo pertenece a este grupo, podrá iniciar sesión en el cliente de punto final.

Cambiar el grupo predeterminado de un usuario

El primer grupo de la lista es el grupo predeterminado de un usuario.

Nota

El usuario debe disponer de permisos de instalación en su grupo predeterminado. Para ver información detallada, *Permitir al usuario instalar en un grupo en la página 4-21*.

.

Procedimiento

1. Abra **Usuarios empresariales**.
2. Haga clic con el botón derecho en el usuario y seleccione **Lista de grupos**.

   Aparecerá la lista **Pertenencia a grupo**.
3. Haga clic con el botón derecho en el usuario y seleccione **Mover arriba**.

   Se ha cambiado el grupo predeterminado del usuario.

Permitir al usuario instalar en un grupo

Esta opción permite a los usuarios instalar dispositivos de Endpoint Encryption en un grupo al que pertenecen, sin que se requiera la aprobación del administrador.



Nota

La configuración predeterminada es **No permitir al usuario instalar en este grupo**.

Procedimiento

1. Abra **Usuarios empresariales**.
2. Haga clic con el botón derecho en el usuario y seleccione **Lista de grupos**.

   Aparecerá la lista **Pertenencia a grupo**.
3. Haga clic con el botón derecho en el usuario y seleccione **Permitir al usuario instalar en este grupo**.

   Ahora, el usuario ya puede instalar dispositivos en este grupo.

Eliminación de usuarios individuales de un grupo



¡ADVERTENCIA!

Antes de eliminar una cuenta de administrador o autenticador de un grupo, reasigne esa función a otro usuario. Si no lo hace así, solo los administradores y autenticadores de nivel empresarial podrán realizar cambios en el nivel de grupo.

Procedimiento

1. Seleccione el grupo y haga clic en **Usuarios**.
2. En el panel derecho, haga clic con el botón derecho en el usuario y seleccione **Quitar usuario**.

   Aparecerá un mensaje de advertencia.
3. Para eliminar el usuario también de la empresa, active **Quitar de la empresa**.

   Nota

   La eliminación de un usuario de la empresa también elimina a dicho usuario de todos los grupos y subgrupos.
4. Haga clic en **Sí**.

   Se ha quitado al usuario.

Eliminación de todos los usuarios de un grupo



¡ADVERTENCIA!

Antes de eliminar una cuenta de administrador o autenticador de un grupo, reasigne esa función a otro usuario. Si no lo hace así, solo los administradores y autenticadores de nivel empresarial podrán realizar cambios en el nivel de grupo.

Procedimiento

1. Seleccione un grupo y, a continuación, haga clic en **Usuarios**.
2. En el panel derecho, haga clic con el botón derecho en el usuario y seleccione **Eliminar todos los usuarios**.

   Aparecerá un mensaje de advertencia.
3. Para eliminar todos los usuarios de la empresa también, active **Quitar de la empresa**.

   Nota

   La eliminación de un usuario de la empresa también elimina a dicho usuario de todos los grupos y subgrupos.
4. Haga clic en **Sí**.

Restauración de un usuario eliminado

Todos los usuarios eliminados se almacenan en la Papelera de reciclaje en el nivel de empresa. Los grupos no tienen una Papelera de reciclaje. La restauración de un usuario no vuelve a agregar el usuario a los grupos a los que estaba asignado anteriormente.

Procedimiento

1. Expanda la Papelera de reciclaje.
2. Abra **Usuarios eliminados**.

   El panel derecho carga todos los dispositivos eliminados.
3. Haga clic con el botón derecho en el usuario y seleccione **Restaurar usuario**.

   El usuario se vuelve a agregar a la empresa, pero no pertenece a ningún grupo.

Trabajar con contraseñas

Cuando un usuario olvida su contraseña o extravía un dispositivo, el usuario puede restablecer su contraseña haciendo uso de los métodos definidos por políticas empresariales o de grupo. Los siguientes métodos de restablecimiento de contraseñas están disponibles:

- Microsoft Windows Active Directory
- PolicyServer MMC
- Ayuda remota
- Autoayuda

Todas estas opciones implican el establecimiento de la política en el nivel empresarial y, a continuación, en el nivel del grupo siempre que sea necesario. Use la política Información de asistencia para proporcionar información relacionada con la asistencia a usuarios acerca de restablecimiento de contraseñas.

Restablecimiento de una contraseña de autenticador o administrador de empresa

Solo los administradores empresariales pueden restablecer las contraseñas de un administrador empresarial. Un autenticador con los mismos permisos de grupo o superiores puede restablecer la contraseña de un administrador o autenticador de ese mismo grupo.



Consejo

Trend Micro recomienda tener como mínimo tres cuentas de administrador empresarial en todo momento como protección ante posibles pérdidas de contraseñas. Si se pierde la contraseña de cuenta de un administrador empresarial, es posible restablecer la contraseña mediante Autoayuda.

Procedimiento

1. Inicie sesión en MMC de PolicyServer con una cuenta de administrador empresarial.

2. Abra **Usuarios empresariales**.
3. Haga clic con el botón derecho en la cuenta de administrador o autenticador de empresa con la contraseña perdida y seleccione **Cambiar contraseña**.

   Aparecerá la ventana **Cambiar contraseña**.
4. Seleccione un Método de autenticación.
5. Especifique la contraseña (si se le solicita).
6. Haga clic en **Aplicar**.

   Se ha restablecido la contraseña de la cuenta.



Nota

La opción **El usuario debe cambiar la contraseña en el siguiente inicio de sesión** solo está disponible después de que el cliente de punto final actualice las políticas.

Restablecimiento de una contraseña de autenticador o administrador de grupo

Todos los cambios de contraseña son solo para el grupo. Si un administrador desea tener solo una contraseña, entonces solo debería pertenecer a un grupo superior.

Procedimiento

1. Inicie sesión en MMC de PolicyServer con una cuenta de administrador de grupo.
2. Seleccione el grupo y abra **Usuarios**.
3. Haga clic con el botón derecho en la cuenta de administrador o autenticador de grupo con la contraseña perdida y seleccione **Cambiar contraseña**.

   Aparecerá la ventana **Cambiar contraseña**.
4. Seleccione un Método de autenticación.
5. Especifique y confirme la contraseña (si se le solicita).

6. Haga clic en **Aplicar**.

   Se ha restablecido la contraseña de la cuenta.

> **Nota**
>
> La opción **El usuario debe cambiar la contraseña en el siguiente inicio de sesión** solo está disponible después de actualizaciones de clientes.

Restablecer la contraseña de un usuario

Cuando vaya a restablecer la contraseña de un usuario, seleccione la casilla de verificación **El usuario debe cambiar la contraseña en el siguiente inicio de sesión** para exigir que el usuario cambie su contraseña en el siguiente inicio de sesión. Una vez que el usuario inicie sesión y cambie la contraseña, deberá cambiar también la contraseña para todos los dispositivos.

> **Nota**
>
> Trend Micro recomienda utilizar la autenticación de dominio.

Restablecimiento a una contraseña fija

Procedimiento

1. Abra **Usuarios empresariales** o expanda el grupo y abra **Usuarios**.
2. Seleccione usuarios del panel derecho.

   Mantenga pulsada la tecla Mayús para seleccionar varios usuarios. La selección múltiple solo está disponible en el nivel de grupo.
3. Haga clic con el botón derecho y seleccione **Cambiar contraseña**.

   Aparecerá la ventana **Cambiar contraseña**.
4. Para el **Método de autenticación**, seleccione **Contraseña fija**
5. Especifique y confirme la contraseña.

6. Haga clic en **Aplicar**.

   El usuario deberá cambiar su contraseña la siguiente vez que inicie sesión.

Restablecimiento de la contraseña de un usuario con Active Directory

Trend Micro recomienda usar Active Directory para restablecer la contraseña de un usuario, especialmente si el usuario tiene acceso a la Asistencia técnica de la empresa, tiene conexión a red o si Inicio de sesión único de Windows (SSO) está activado.

Consulte el manual del sistema operativo Windows correspondiente para obtener más información sobre cómo restablecer la una contraseña de usuario de dominio con Active Directory.

Uso de la asistencia para la contraseña de autoayuda

Esta tarea explica cómo configurar políticas para autoayuda. Los usuarios que han olvidado sus contraseñas pueden usar autoayuda para autenticarse sin la intervención del equipo de asistencia técnica. Use las políticas Cantidad de preguntas y Pregunta personal para establecer el número de preguntas personales y las preguntas que el usuario debe responder, respectivamente. Las preguntas de autoayuda se responden durante la autenticación inicial del usuario y cuando los usuarios cambian sus contraseñas.

Para obtener detalles sobre el uso de la autoayuda, consulte *Autoayuda en la página 1-19*.



Nota

La autoayuda requiere conexión de red a PolicyServer.

Procedimiento

1. Abra **Políticas empresariales** o expanda el grupo y, a continuación, abra **Políticas**.
2. Vaya a **Común** > **Autenticación** > **Inicio de sesión local** > **Autoayuda**.

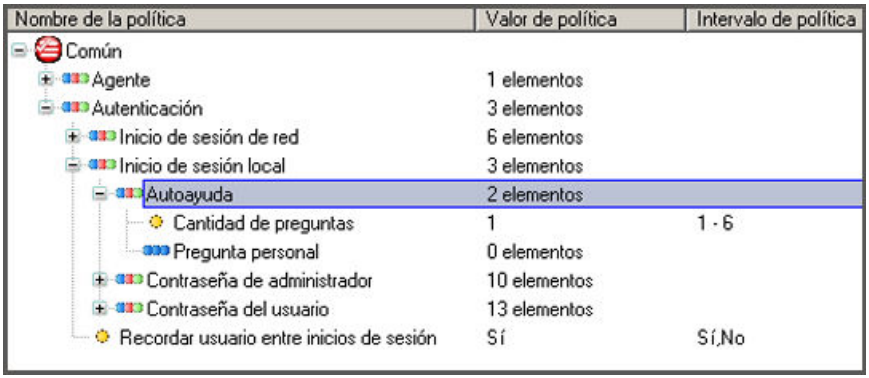


FIGURA 4-8. Política Autoayuda

3. Abra **Cantidad de preguntas** para establecer el número requerido de preguntas que los usuarios deben responder.

¡ADVERTENCIA!

No establezca una **Cantidad de preguntas** mayor que seis. En caso contrario, los usuarios no podrán iniciar sesión.

---

4. Haga clic con el botón derecho en **Pregunta persona** y seleccione **Agregar** para definir una pregunta que el usuario debe responder. Repita este paso hasta que estén definidas todas las preguntas personales.

   La siguiente vez que inicien sesión los usuarios, se les pedirá que definan sus respuestas a las preguntas personales.

Asistencia para restablecer contraseñas con Ayuda remota

Restablezca las contraseñas olvidadas con Ayuda remota. Un usuario que tiene una cuenta bloqueada o ha olvidado su contraseña debe restablecerla antes de iniciar sesión con la nueva contraseña. Ayuda remota requiere que el usuario se ponga en contacto con la Asistencia técnica para responder a una pregunta personal. Ayuda remota no requiere que exista conectividad de red con PolicyServer.

Procedimiento

1. Inicie sesión en MMC de PolicyServer con una cuenta de administrador empresarial o de administrador/autenticador de grupo dentro del mismo grupo de políticas que el usuario.
2. Solicite al usuario que haga clic en **Ayuda** > **Ayuda remota** desde su cliente de punto final.
3. Solicite al usuario que le diga el **ID de dispositivo** que aparece.



FIGURA 4-9. Asistencia mediante Ayuda remota

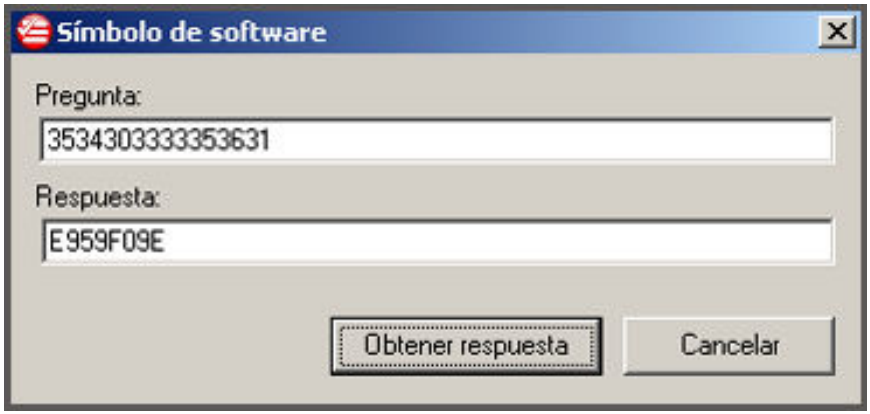
4. En MMC de PolicyServer, abra **Dispositivos empresariales** o expanda el grupo del usuario y abra **Dispositivos**, icono en el grupo del usuario.
5. En el panel derecho, haga clic con el botón derecho en el dispositivo del usuario y seleccione **Símbolo de software**.

Aparecerá la ventana **Símbolo de software**.

6. Solicite al usuario que le lea el campo **Pregunta** de 16 dígitos y escríbalo en el campo **Pregunta** de la ventana **Símbolo de software**.

7. Haga clic en **Obtener respuesta**.

   El campo **Respuesta** se llena con una cadena de 8 caracteres.



8. Diga al usuario la cadena de 8 caracteres del campo **Respuesta**.

9. El usuario escribe la cadena en el campo **Respuesta** en el punto final y hace clic en **Iniciar sesión**.

10. El sistema solicita al usuario que escriba una nueva contraseña.

Configuración de la información de asistencia

La política Información de asistencia especifica la información sobre la asistencia técnica de una organización. La política Información de asistencia se puede configurar de forma exclusiva para cada grupo.

Procedimiento

1. Inicie sesión en MMC de PolicyServer con una cuenta de administrador empresarial o de administrador/autenticador de grupo dentro del mismo grupo de políticas que el usuario.
2. Expanda el grupo de un usuario y vaya a **Políticas** > **Full Disk Encryption** > **Común** > **Inicio de sesión**.
3. Haga clic con el botón derecho en la política **Información de asistencia** y seleccione **Agregar**.
4. Especifique la información de asistencia (número de teléfono, ubicación).
5. Haga clic en **Aceptar**.

Trabajar con dispositivos

Los dispositivos son equipos de sobremesa, portátiles, smartphones y cualquier otro punto final que tenga Full Disk Encryption, FileArmor o KeyArmor instalado. Los dispositivos se agregan de forma automática a la empresa cuando se instala la aplicación Endpoint Encryption.

Nota

Cada dispositivo solo puede formar parte de un grupo.

Agregar un dispositivo a un grupo

Procedimiento

1. En el panel izquierdo, expanda el grupo deseado y haga clic en **Dispositivos**.
2. En el panel derecho, haga clic con el botón derecho en el espacio en blanco y seleccione **Agregar dispositivo**.

Aparecerá la pantalla **Agregar dispositivos a grupo**.

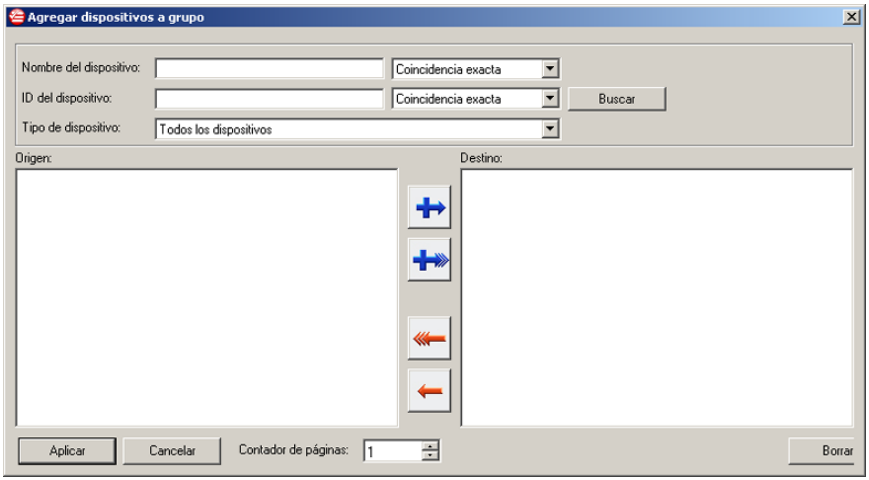


FIGURA 4-10. Pantalla Agregar dispositivos a grupo

3. Escriba los detalles del dispositivo y haga clic en **Buscar**.

   Si hay alguna coincidencia, el campo **Fuente** se rellena con las cuentas.

4. Seleccione el dispositivo de la lista y haga clic en la **flecha azul** para agregarlo. Consulte la tabla para obtener controles adicionales.

TABLA 4-4. Iconos para agregar/eliminar dispositivos

ICONOS CENTRALES	DESCRIPCIÓN
	Agregue un único dispositivo al campo **Destino**.
	Agregue todos los dispositivos encontrados basados en el criterio de búsqueda al campo **Destino**.

Iconos centrales	Descripción
	Elimine un único dispositivo del campo **Destino**.
	Elimine todos los dispositivos del campo **Destino**.

5. Haga clic en **Aplicar** para agregar el dispositivo al grupo seleccionado.

   El dispositivo se agrega al grupo.

Eliminación de un dispositivo de un grupo

Eliminar un dispositivo de un grupo solo elimina el dispositivo del grupo seleccionado.

¡ADVERTENCIA!

Para eliminar un dispositivo de todos los grupos, elimínelo de la empresa. Antes de eliminar un dispositivo de la empresa, compruebe que se haya descifrado el dispositivo y que se hayan desinstalado todos los productos de Trend Micro. Si no lo hace así, puede dar lugar a una pérdida irreversible de los datos.

Procedimiento

1. Seleccione el grupo y abra **Dispositivos**.
2. En el panel derecho, haga clic con el botón derecho en el dispositivo y seleccione **Quitar dispositivo**.

   Aparece un mensaje de advertencia.
3. Haga clic en **Sí**.

   El dispositivo se ha eliminado.

Eliminación de un dispositivo de una empresa

Al eliminar un dispositivo de una empresa, se elimina de todos los grupos y de la empresa. El dispositivo seguirá funcionando siempre que las políticas de conexión y contraseña estén actualizadas en el dispositivo. Si el dispositivo cae en este estado, no se podrán recuperar los archivos. Para mitigar el riesgo, descifre el dispositivo inmediatamente, desinstale Full Disk Encryption y, a continuación, vuelva a instalar Full Disk Encryption como cliente no administrado.

¡ADVERTENCIA!

Compruebe que se haya descifrado el dispositivo y que se hayan desinstalado todas las aplicaciones de Trend Micro antes de eliminar un dispositivo de la empresa. Si no lo hace así, puede dar lugar a una pérdida irreversible de los datos.

Para obtener información sobre la eliminación de un dispositivo de un determinado grupo, pero no de la empresa, consulte *Eliminación de un dispositivo de un grupo en la página 4-33*.

Nota

Vaya a la Papelera de reciclaje para volver a agregar el dispositivo eliminado a la empresa.

Procedimiento

1. Desinstale la aplicación de cliente de punto final del dispositivo. Para más información sobre la desinstalación de clientes de punto final, consulte la Guía de instalación de Endpoint Encryption.
2. Abra **Dispositivos empresariales**.
3. En el panel derecho, haga clic con el botón derecho en el dispositivo y seleccione **Quitar dispositivo**. Busque y haga clic en el dispositivo seleccionado.

   Aparecerá un mensaje de advertencia.
4. Haga clic en **Sí**.

El dispositivo se ha eliminado.

Ver el contenido del directorio

Use la opción de listado de directorios para ver una instantánea de todas las aplicaciones descargadas en el dispositivo seleccionado.

Procedimiento

1. Abra **Dispositivos empresariales** o expanda un grupo y abra **Dispositivos**.
2. En el panel derecho, haga clic con el botón derecho en el dispositivo y seleccione **Listado de directorio**.

   La ventana **Instantánea de directorio de dispositivo** muestra todas las aplicaciones descargadas en el dispositivo.

Ver atributos del dispositivo

Use la opción Atributos del dispositivo (memoria, sistema operativo, vida de la batería, etc.) para ver una instantánea actual del dispositivo seleccionado.

Procedimiento

1. Abra **Dispositivos empresariales** o expanda un grupo y abra **Dispositivos**.
2. En el panel derecho, haga clic con el botón derecho en el dispositivo y seleccione **Listado de directorio**.

Aparecerá la ventana **Atributos del dispositivo**.

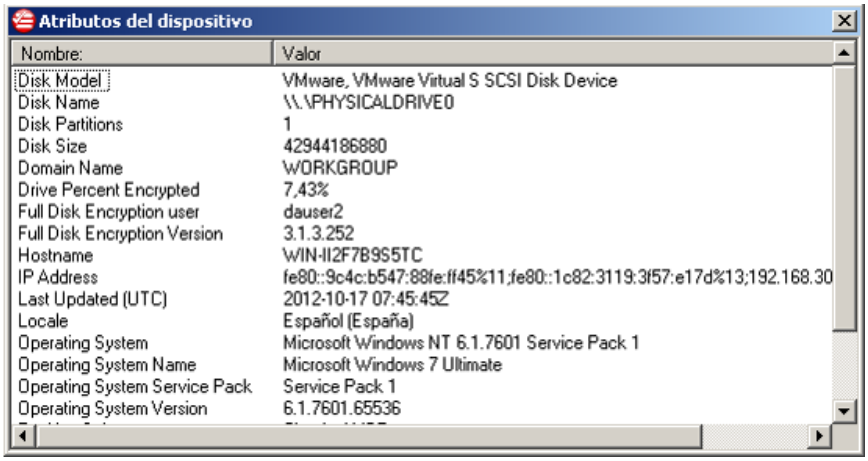


FIGURA 4-11. Lista de atributos del dispositivo

Ver listado de directorio

Use el listado de directorio para ver solamente la estructura de directorios de dispositivos KeyArmor.

Procedimiento

1. Abra **Dispositivos empresariales** o expanda un grupo y abra **Dispositivos**.
2. En el panel derecho, haga clic con el botón derecho en el dispositivo y seleccione **Listado de directorio**.

   Aparecerá la ventana **Instantánea de directorio de dispositivo**.

Eliminación de un dispositivo

La eliminación de un dispositivo elimina completamente todos los datos que contiene. Para DriveArmor, Full Disk Encryption y KeyArmor, el comando Eliminar se emite cuando el dispositivo se comunica con PolicyServer.



¡ADVERTENCIA!

La eliminación de un dispositivo no se puede deshacer. Realice una copia de seguridad de todos los datos antes de llevar a cabo esta acción.

Procedimiento

1. Abra **Dispositivos empresariales** o expanda un grupo y abra **Dispositivos**.
2. En el panel derecho, haga clic con el botón derecho en el dispositivo y seleccione **Eliminar dispositivo**.
3. En el mensaje de advertencia, haga clic en **Sí**.
4. En el mensaje de confirmación, haga clic en **Aceptar**.

Bloqueo de un dispositivo

El bloqueo de un dispositivo reinicia el dispositivo y lo sitúa en un estado que requiere Ayuda remota. Para DriveArmor, Full Disk Encryption y KeyArmor, el comando Bloquear se emite cuando el dispositivo se comunica con PolicyServer.

Bloquee un dispositivo para evitar que un usuario se autentique en el dispositivo hasta que se realice una autenticación de Ayuda remota correcta.

Procedimiento

1. Abra **Dispositivos empresariales** o expanda un grupo y abra **Dispositivos**.
2. En el panel derecho, haga clic con el botón derecho en el dispositivo y seleccione **Bloquear dispositivo**.
3. En el mensaje de advertencia, haga clic en **Sí**.

4. En el mensaje de confirmación, haga clic en **Aceptar**.

Reiniciar un dispositivo

Use Restablecimiento parcial para reiniciar un dispositivo. Para DriveArmor, Full Disk Encryption y KeyArmor, el comando Restablecimiento parcial se emite cuando el dispositivo se comunica con PolicyServer.

Procedimiento

1. Abra **Dispositivos empresariales** o expanda un grupo y abra **Dispositivos**.
2. En el panel derecho, haga clic con el botón derecho en el dispositivo y seleccione **Restablecimiento parcial**.
3. En el mensaje de advertencia, haga clic en **Sí**.
4. En el mensaje de confirmación, haga clic en **Aceptar**.

Restauración de un dispositivo eliminado

Todos los dispositivos eliminados se almacenan en la Papelera de reciclaje en el nivel de empresa. Los grupos no tienen una Papelera de reciclaje. La restauración de un dispositivo no vuelve a agregar el dispositivo a los grupos a los que estaba asignado anteriormente.

Procedimiento

1. Expanda la Papelera de reciclaje.
2. Abra **Dispositivos eliminados**.

   El panel derecho carga todos los dispositivos eliminados.
3. Haga clic con el botón derecho en el dispositivo y seleccione **Restaurar dispositivo**.

El dispositivo se vuelve a agregar a la empresa, pero no pertenece a ningún grupo.

Capítulo 5

Trabajar con Full Disk Encryption

Full Disk Encryption proporciona seguridad de datos completa de punto final mediante una autenticación segura obligatoria y cifrado de disco completo. Full Disk Encryption protege no solo los archivos de datos, sino también todas las aplicaciones, la configuración del registro, los archivos temporales, los archivos de intercambio, las colas de impresión y los archivos eliminados. Hasta que el usuario se valide, la autenticación segura de arranque previo restringe el acceso al sistema operativo host vulnerable.

En este capítulo se describen los siguientes temas:

- *Herramientas de Endpoint Encryption en la página 5-2*
- *Autenticación en el arranque previo de Full Disk Encryption en la página 5-2*
- *Conectividad de Full Disk Encryption en la página 5-15*
- *Consola de recuperación de Full Disk Encryption en la página 5-16*
- *Métodos de recuperación de Full Disk Encryption en la página 5-26*
- *CD de reparación en la página 5-28*

Herramientas de Endpoint Encryption

TABLA 5-1. Herramientas de Endpoint Encryption

HERRAMIENTA	OBJETIVO
Consola de recuperación	• Recuperar un dispositivo en caso de un error del sistema operativo principal. • Solucionar problemas de red. • Administrar usuarios y registros.
Ayuda de la línea de comandos	• Cree valores cifrados para proteger las credenciales al crear una secuencia de comandos de instalación.
Ayuda del instalador de la línea de comandos	• Generar secuencias de comandos para instalaciones automáticas. • Cree valores cifrados para proteger las credenciales al crear una secuencia de comandos de instalación.
DAAutoLogin	• Se usa para crear revisiones para Windows. DAAutoLogin permite una omisión temporal del arranque previo de Endpoint Encryption.
CD de reparación	• Use este CD de arranque para descifrar la unidad antes de la eliminación de Full Disk Encryption en caso de que el disco resulte dañado. • El CD de reparación solo debe utilizarse si los métodos de eliminación estándar no son posibles. Un síntoma típico de un disco dañado es una pantalla en negro.

Autenticación en el arranque previo de Full Disk Encryption

Después de instalar Full Disk Encryption, se muestra el arranque previo de Full Disk Encryption antes de que se cargue Windows. El arranque previo de Full Disk Encryption desempeña un papel importante garantizando que sólo los usuarios autorizados pueden tener acceso a los dispositivos y, cuando esté conectado a

PolicyServer, actualizando las políticas de seguridad local. Desde esta pantalla, se puede realizar una serie de tareas:

- Autenticación en un punto final
- Cambiar las contraseñas
- Inicio de sesión en la consola de recuperación



FIGURA 5-1. Pantalla de arranque previo de Full Disk Encryption

Opciones de menú

Hay varias opciones disponibles en el menú superior izquierdo del arranque previo de Full Disk Encryption.

TABLA 5-2. Opciones de menú del arranque previo de Full Disk Encryption

ELEMENTO DE MENÚ	DESCRIPCIÓN
Autenticación	Cambiar el método de autenticación utilizado para iniciar la sesión.

Elemento de menú	Descripción
Comunicación	Sincronizar de forma manual con PolicyServer. **Nota** Los puntos finales no administrados muestran un valor nulo.
Equipo	Ver información acerca de Full Disk Encryption, cambiar el diseño del teclado, acceder al teclado en pantalla o reiniciar/apagar el dispositivo.

Conectividad de red

El icono de conexión de red ( ) se muestra en la esquina superior derecha cuando Full Disk Encryption está instalado como cliente administrado. El icono solo se resalta si el dispositivo está conectado a la red y tiene comunicación con PolicyServer. Cuando Full Disk Encryption se instala como cliente no administrado, el icono de red no se muestra nunca.

Teclado en pantalla

Acceda al teclado en pantalla desde el arranque previo de Full Disk Encryption navegando hasta:

Menú > Equipo > Teclado en pantalla

Para insertar el cursor en el campo deseado cuando se muestre el teclado, haga clic en **Enfocar** en la esquina inferior derecha del teclado.

Cambiar el diseño del teclado

Cambiar el diseño del teclado afecta tanto a las pulsaciones de teclas como al teclado en pantalla. Una vez que arranque Windows, el diseño del teclado se establecerá en función del sistema operativo Windows.

Procedimiento

1. Desplácese a **Menú** > **Equipo** > **Cambiar diseño del teclado**.

   Aparece la pantalla **Seleccionar el idioma del teclado (diseño)**.

2. Seleccione un diseño del teclado.

3. Haga clic en **Aceptar**.

Cambiar métodos de autenticación

Procedimiento

1. En el arranque previo de Full Disk Encryption, seleccione **Cambiar la contraseña tras iniciar sesión**.

2. Especifique el nombre de usuario y la contraseña.

3. Haga clic en **Iniciar sesión**.

   Aparecerá la ventana **Cambiar contraseña**.

4. En el menú superior izquierdo, seleccione **Autenticación** y elija el método de autenticación que desee.

   Aparece la ventana **Contraseña nueva** para el método de autenticación elegido.

5. Asigne y confirme la nueva contraseña y, a continuación, haga clic en **Siguiente**.

   El dispositivo arranca en Windows.

Cambiar las contraseñas

Procedimiento

1. En el arranque previo de Full Disk Encryption, seleccione **Cambiar la contraseña tras iniciar sesión**.

2. Especifique el nombre de usuario y la contraseña
3. Haga clic en **Iniciar sesión**.

   Aparecerá la ventana **Cambiar contraseña**.
4. Asigne y confirme la nueva contraseña y haga clic en **Siguiente**.

   El dispositivo arranca en Windows.

ColorCode

ColorCode™ es un método de autenticación diseñado para ser recordado fácilmente. En lugar de utilizar números o letras para una contraseña, la autenticación por código de

color consta de una secuencia de colores creada por el usuario (por ejemplo: rojo, rojo, azul, amarillo, azul y verde).



FIGURA 5-2. Inicio de sesión de ColorCode

Crear una contraseña de código de colores

El recuento total (número total de pasos en el código de colores) se define mediante PolicyServer. El recuento total es seis.

Procedimiento

1. Cambiar el método de autenticación a código de colores.

Nota

Para obtener información detallada acerca de cómo cambiar los métodos de autenticación, consulte *Cambiar métodos de autenticación en la página 5-5*.

Aparecerá la pantalla **Cambiar contraseña de código de colores**.

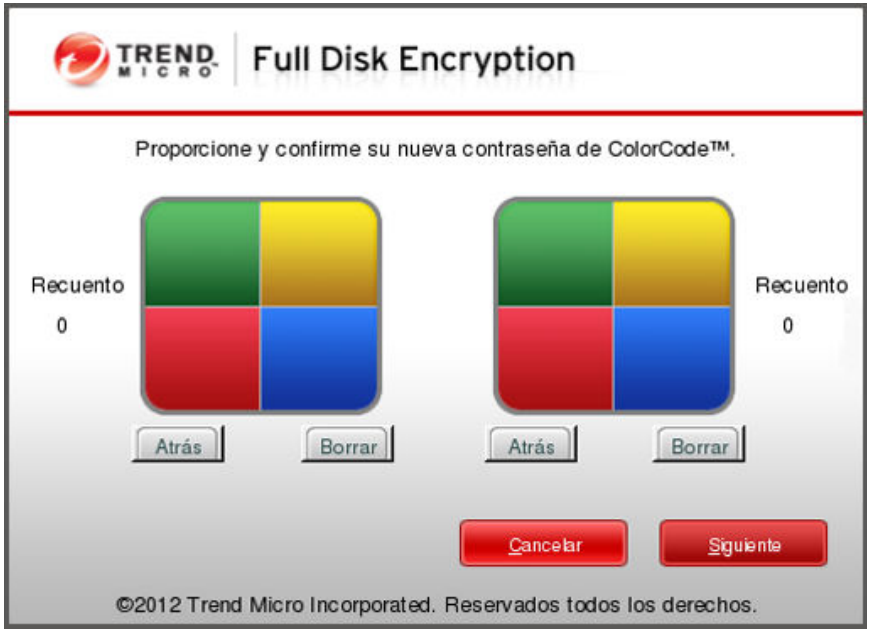


FIGURA 5-3. Pantalla Cambiar contraseña de código de colores

2. Elija el primer color haciendo clic en él mediante el cuadrado de la izquierda.

   El recuento aumenta en 1.

3. Haga clic en más colores de la secuencia.

Consejo

Si ha habido un error, haga clic en **Atrás** para eliminar el último color que agregó, o haga clic en **Borrar** para volver a comenzar.

4. Una vez completa la secuencia, confirme la contraseña del código de colores usando el cuadrado de la izquierda.

5. Haga clic en **Siguiente** para finalizar.

Ayuda remota

Utilice Ayuda remota cuando un usuario se bloquea en un cliente de punto final debido a que se han realizado demasiados intentos de inicio de sesión fallidos o porque el período comprendido desde la última sincronización de PolicyServer ha sido demasiado largo.

En cada política de la aplicación, establezca la acción en **Autenticación remota**.

TABLA 5-3. Políticas que afectan a la autenticación remota

POLÍTICA	DESCRIPCIÓN
Iniciar sesión > **Período de bloqueo de cuenta**	Número de días que un dispositivo no se puede comunicar con PolicyServer antes de llamar a una acción de bloqueo de cuenta.
Iniciar sesión > **Acción de bloqueo de cuenta**	Acción que tiene lugar cuando transcurre el período de bloqueo de cuenta. Las acciones de bloqueo de cuenta son: borrar, autenticación remota.
Iniciar sesión > **Intentos de inicio de sesión fallidos permitidos**	Número de intentos de inicio de sesión fallidos que se permiten antes de ejecutar la acción definida en Acción de dispositivo bloqueado
Iniciar sesión > **Acción de dispositivo bloqueado**	Acción que tiene lugar cuando se excede el valor de la política Intentos de inicio de sesión fallidos permitidos. Las acciones incluyen: tiempo de demora, borrar, autenticación remota.

Uso de la Ayuda remota para desbloquear Full Disk Encryption

Importante

- Al reiniciar el dispositivo de punto final se reinicia el código de pregunta.
- Al sincronizar manualmente las políticas con PolicyServer también se restablece el código de pregunta.
- El código de pregunta y el código de respuesta no distinguen entre mayúsculas y minúsculas.

Procedimiento

1. En el arranque previo de Full Disk Encryption, vaya a **Menú** > **Autenticación** > **Ayuda remota**.
2. Proporcione el **Código de pregunta** al administrador de PolicyServer.
3. Escriba el **Código de respuesta** proporcionado por el Administrador de PolicyServer.
4. Haga clic en **Iniciar sesión**.

   Aparecerá la ventana **Cambiar contraseña**.

   Nota

   Si la cuenta utiliza la autenticación de dominio, el dispositivo arrancará directamente en Windows.

5. Especifique y confirme la nueva contraseña y, a continuación, haga clic en **Siguiente**.

   El dispositivo arranca en Windows.

Tarjeta inteligente

La autenticación de tarjetas inteligentes requiere tanto un PIN como una tarjeta física para confirmar la identidad de un usuario. Inserte la tarjeta inteligente antes de proporcionar un PIN.

Importante

Para activar la autenticación de tarjetas inteligentes para todos los clientes de Endpoint Encryption, habilite la siguiente política: **Full Disk Encryption** > **Equipo** > **Iniciar sesión** > **Autenticación de símbolo**.

Tarjetas inteligentes compatibles

Fabricante de tarjetas	Nombre del producto	Grabado por láser en el reverso de la tarjeta
Axalto	Axalto Cyberflex Access 64k v1 soft mask 4 versión 1	Axalto Access 64KV2
	Axalto Cyberflex Access 64k v1 soft mask 4 versión 2	Axalto Access 64KV2
Gemalto	Cyberflex Access v2c 64K	Gemalto Access 64KV2
	Interfz dual Gemalto GemCombiXpresso R4	Gemalto GCX4 72K DI
	Gemalto TOP DL GX4 144K	Gemalto TOP DL GX4 144K
Gemplus	GemXpresso (GXP) PRO 64 K	Gemplus GXP3 64V2N
Oberthur	CosmopolIC v4 32K	Oberthur CosmopolIC v4
	Galactic v1 32K	OCS Gal 2.1
	ID-One Cosmo v5.2D 64k	Oberthur C.S. Cosmo64 V5.2D
	ID-One Cosmo v5.2 72k	Oberthur ID One V5.2
	ID-One Cosmo v5.2D 72k	Oberthur ID One V5.2 Dual

Fabricante de tarjetas	Nombre del producto	Grabado por láser en el reverso de la tarjeta
RSA	RSA 5100	
	RSA 5200	
	RSA 6100	
	RSA SID 800	
Schlumberger (Axalto)	Tarjeta Cyberflex 32k v2 con Softmask 7 versión 2	Schlumberger Access 32K V2

Autenticación con una tarjeta inteligente

Procedimiento

1. Inserte la tarjeta inteligente en el lector.
2. Conecte el lector al dispositivo.
3. Proporcione el nombre de usuario y la contraseña fija.
4. Haga clic en **Continuar**.

   Aparecerá una ventana de mensaje.
5. Haga clic en **Continuar**.
6. En la ventana **Registrar símbolo**:
   a. Escriba el nuevo PIN proporcionado por el administrador.
   b. Confirme el nuevo PIN.
   c. Seleccione el tipo de tarjeta inteligente en la lista desplegable de símbolos.
   d. Haga clic en **Continuar** para terminar de registrar el símbolo y acceda al equipo.

Autoayuda

Utilice la autoayuda para autenticar cuando los usuarios han olvidado sus credenciales. La autoayuda requiere que los usuarios respondan a las preguntas personales predefinidas. La autoayuda también se puede utilizar en lugar de la contraseña fija o de otros métodos de autenticación.

Importante

PolicyServer debe configurarse para poder utilizar la autenticación de autoayuda. Para obtener más información, consulte *Descripción de políticas en la página 3-1*.

¡ADVERTENCIA!

Se puede mostrar un máximo de seis preguntas para clientes de punto final. No cree más de seis preguntas en PolicyServer o de lo contrario los usuarios no podrán iniciar sesión.

Configuración de autoayuda

Si está activada la política de autoayuda, se pedirá al usuario que defina las respuestas a las preguntas de autoayuda después de que iniciar sesión por primera vez. Si el usuario cambia su contraseña, debe volver a definir las respuestas a las preguntas de autoayuda.

Nota

Las respuestas de autoayuda se almacenan en el dispositivo. Si un usuario inicia sesión en otro dispositivo de Full Disk Encryption, el usuario debe definir las respuestas de autoayuda para ese dispositivo.

Procedimiento

1. Proporcione el nombre de usuario y la contraseña.
2. Haga clic en **Iniciar sesión**.

   Aparecerá la ventana **Autoayuda**.
3. Defina las respuestas para todas las preguntas de autoayuda.

4. Haga clic en **Siguiente**.

   El dispositivo arranca en Windows.

Uso de la autoayuda

Procedimiento

1. En el menú de la parte superior izquierda del arranque previo de Full Disk Encryption, vaya a **Menú** > **Autenticación** > **Autoayuda**.

   Aparecerá la ventana **Autoayuda**.

2. Proporcione respuestas a todas las preguntas de autoayuda.

3. Haga clic en **Iniciar sesión**.

4. Defina la nueva contraseña y, a continuación, haga clic en **Siguiente**.

   El dispositivo arranca en Windows.

Cambiar las respuestas de autoayuda

Procedimiento

1. En el arranque previo de Full Disk Encryption, proporcione las credenciales, seleccione **Cambiar la contraseña tras iniciar sesión** y, a continuación, haga clic en **Iniciar sesión**.

   Aparecerá la ventana **Cambiar contraseña**.

2. Asigne y confirme la nueva contraseña y, a continuación, haga clic en **Siguiente**.

   Aparecerá la ventana **Autoayuda**.

3. Defina nuevas respuestas para todas las preguntas de autoayuda y, a continuación, haga clic en **Siguiente**.

El dispositivo arranca en Windows.

Conectividad de Full Disk Encryption

Endpoint Encryption utiliza un proceso de cifrado aprobado FIPS 140-2 para los datos que se transfieren entre el arranque previo de Full Disk Encryption y PolicyServer. Los clientes Full Disk Encryption que disponen de conectividad de red con PolicyServer pueden recibir actualizaciones de políticas y cargar datos de auditoría desde el cliente de punto final. Todas las comunicaciones cliente-servidor se cifran internamente y se pueden enviar a través de conexiones no seguras como Internet.

Los administradores del sistema tienen flexibilidad para determinar las opciones de conectividad para su organización. Los administradores pueden colocar PolicyServer dentro de una DMZ (zona desmilitarizada) para tener acceso tanto a las redes internas como a Internet.

TABLA 5-4. Requisitos de conectividad de Full Disk Encryption

RECURSO	FUNCIÓN
PolicyServer	Las políticas de seguridad actualizadas de PolicyServer se pueden enviar al arranque previo de Full Disk Encryption o mediante la conectividad establecida en Windows, LAN, VPN, etc.
acceso TCP/IP	La conectividad de red para dispositivos PC requiere disponer de acceso completo de red TCP/IP; no se puede utilizar el acceso de marcación o telefónico con PolicyServer durante la autenticación previa al arranque.
Puerto 80	Las comunicaciones de Full Disk Encryption utilizan el puerto 80 de forma predeterminada. Para cambiar el número de puerto predeterminado, vaya a la consola de recuperación y actualice PolicyServer.

Actualización de clientes de Full Disk Encryption

Los clientes Full Disk Encryption reciben automáticamente las políticas de seguridad actualizadas desde PolicyServer en intervalos determinados por la política. Siga estos pasos para sincronizar manualmente las políticas:

Procedimiento

1. En el menú de la parte superior izquierda del arranque previo de Full Disk Encryption, vaya a **Comunicaciones** > **Sincronizar políticas**.
2. Vaya a **Equipo** > **Acerca de Full Disk Encryption**. Se muestra la marca de tiempo de la última sincronización de políticas de PolicyServer.

Consola de recuperación de Full Disk Encryption

La consola de recuperación ayuda a los administradores a recuperar un dispositivo en caso de error del sistema operativo principal, a solucionar problemas de conectividad de red y a administrar políticas para clientes no administrados.



¡ADVERTENCIA!

Utilice la consola de recuperación antes de ejecutar las utilidades estándar de reparación y diagnóstico de Windows.

TABLA 5-5. Funciones de la consola de recuperación

ELEMENTO DE LA CONSOLA	DESCRIPCIÓN
Descifrar disco	Eliminar el cifrado de la unidad de disco. Utilice la consola de recuperación del arranque previo de Full Disk Encryption para obtener acceso a Descifrar disco.

Elemento de la consola	Descripción
Montar particiones	Proporcionar acceso a las particiones cifradas para la administración de archivos. Utilice la consola de recuperación del arranque previo de Full Disk Encryption para obtener acceso a Montar particiones. **Nota** Montar particiones solo se encuentra disponible en los dispositivos con cifrado de software. Esta opción aparece desactivada si el dispositivo dispone de cifrado de hardware.
Restaurar arranque	Recuperar el MBR con un estado anterior a la instalación de Full Disk Encryption. Utilice la consola de recuperación del arranque previo de Full Disk Encryption para obtener acceso a Restaurar arranque. **Nota** Restaurar arranque solo se encuentra disponible en los dispositivos con cifrado de software. Esta opción aparece desactivada si el dispositivo dispone de cifrado de hardware.
Administrar usuarios	Agregar o eliminar usuarios desde el dispositivo cuando no esté conectado a PolicyServer.
Administrar políticas	Modificar las políticas de los dispositivos que no están administrados por PolicyServer o que, aunque estén administrados, se encuentran desconectados temporalmente de PolicyServer. Si el dispositivo está administrado, los cambios en las políticas se sobrescribirán la próxima vez que se comunique con PolicyServer.
Ver registros	Buscar y visualizar los diferentes registros de Full Disk Encryption. **Nota** Los registros solo están disponibles cuando se accede a la consola de recuperación desde Windows.
Configuración de red	Comprobar, probar y modificar la configuración de red.

Elemento de la consola	Descripción
Salir	Salir de la consola de recuperación.

Acceso a la consola de recuperación

Solo las cuentas de administrador de grupo o autenticador pueden acceder a la consola de recuperación. Para conceder a los usuarios acceso a la consola de recuperación, establezca **PC** > **Cliente** > **Permitir recuperación de usuario** en **Sí**.

Procedimiento

1. Arranque el dispositivo.
2. Cuando aparezca el arranque previo de Full Disk Encryption, indique el nombre de usuario y la contraseña.
3. Seleccione la opción **Consola de recuperación** e inicie sesión.

   Se mostrará la consola de recuperación.

Acceso a la consola de recuperación desde Windows

Procedimiento

1. En Windows, vaya al directorio de instalación de Full Disk Encryption. La ubicación predeterminada es `C:\Archivos de programa\Trend Micro \Full Disk Encryption\`
2. Abra `RecoveryConsole.exe`.

   Se muestra la ventana **Consola de recuperación**.
3. Proporcione el nombre de usuario y la contraseña, y haga clic en **Iniciar sesión**.

   La consola de recuperación se abre en la página **Descifrar disco**.

Uso de Descifrar disco

Al seleccionar Descifrar disco, se descifra un disco duro de Full Disk Encryption cifrado, pero no se quita ninguno de los controladores de cifrado. Si usa Descifrar unidad, deshabilite DrAService antes de iniciar Windows.



¡ADVERTENCIA!

Lea este procedimiento antes de utilizar la función. Si se realiza incorrectamente, se puede producir una pérdida de datos. No utilice la opción Descifrar disco para quitar Full Disk Encryption de un dispositivo que está funcionando con normalidad. Utilice `TMFDEUninstall.exe` en su lugar.

Procedimiento

1. En el arranque previo de Full Disk Encryption, seleccione **Consola de recuperación**, proporcione las credenciales y, a continuación, haga clic en **Inicio de sesión**.

   La consola de recuperación se abre en la página **Descifrar disco**.

2. Haga clic en **Descifrar** para empezar a descifrar la unidad.

   El descifrado comienza inmediatamente y la página Descifrar disco mostrará el progreso de descifrado.

3. Una vez finalizado el descifrado, haga clic en **Salir** para reiniciar el dispositivo.

4. Si inicia una clave de CD, DVD o USB de la herramienta de reparación:

   a. Después de salir de Full Disk Encryption, pulse **F12** (o el botón correspondiente para entrar en las opciones de arranque).

   b. Inserte el CD/DVD de la herramienta de reparación y seleccione la unidad de CD/DVD desde la pantalla de opciones de inicio.

   c. Continúe con las acciones de recuperación establecidas.

5. Si el inicio se realiza en Windows:

   a. Mantenga presionada la tecla F8 y seleccione **Modo normal** antes de que el sistema comience el inicio en Windows.

¡ADVERTENCIA!

Si no aparece la pantalla de opciones de ararnque de Windows, apague inmediatamente el dispositivo. Si Windows se inicia normalmente (no en el modo normal), DrAService volverá a iniciar inmediatamente el cifrado de la unidad. Las acciones de recuperación realizadas en este momento pondrían causar daños irreparables en los datos de la unidad.

6. Abra **Administración del dispositivo** y vaya a **Servicios y aplicaciones** > **Servicios.**.

   Aparecerá la ventana **Administración del dispositivo**.

7. Busque y haga doble clic en DrAService para abrir la ventana **Propiedades de DrAService**.

8. En la pestaña **General**, cambie el **tipo de inicio** a `Desactivado`.

9. Haga clic en **Aplicar** y, a continuación, en **Aceptar**.

10. Arranque el dispositivo.

11. Inicie sesión en el arranque previo de Full Disk Encryption y, después, en Windows.

Qué hacer a continuación

Una vez finalizadas todas las acciones de recuperación, establezca **DrAService** en **Automático**. El dispositivo vuelve a cifrar automáticamente el disco duro después del siguiente arranque.

Montar particiones

Use Montar particiones para copiar archivos entre la unidad de disco duro cifrada y un dispositivo de almacenamiento antes de copiar o volver a formatear el disco duro. El contenido cifrado en la unidad se muestra en el panel izquierdo y se puede montar un dispositivo sin cifrar en el panel derecho. Use copiar y pegar para mover los archivos de un panel a otro. Se cifrarán los archivos copiados en la unidad cifrada. Los archivos copiados desde la unidad cifrada estarán sin cifrar.

Restaurar arranque

La opción Restaurar arranque restaura el arranque original en el dispositivo, cuando el dispositivo se ha descifrado completamente y sólo está disponible desde el arranque previo de Full Disk Encryption.

Descifre el disco antes de restaurar el registro de arranque maestro (MBR).



¡ADVERTENCIA!

No utilice Descifrar disco sin haber leído antes las instrucciones. Se puede producir una pérdida de datos.

Procedimiento

1. Inicie sesión en la consola de recuperación.
2. Haga clic en **Descifrar disco** y haga clic en **Descifrar**.
3. Cambie a la opción Restaurar arranque.

   Se muestra una ventana de confirmación de **Sustituir MBR**.
4. Haga clic en **Sí** para sustituir el MBR.

   Se muestra un mensaje que confirma la sustitución de MBR.
5. Haga clic en **Salir**.

   El dispositivo arranca en Windows.

Administrar usuarios de Full Disk Encryption

Administre o quite usuarios de la caché de arranque previo o cambie la contraseña de un usuario almacenada en caché. Esta opción es útil cuando Full Disk Encryption no se puede conectar a PolicyServer. Tanto el arranque previo de Full Disk Encryption como la consola de recuperación de Windows pueden utilizar esta opción.

Nota

- Administrar usuarios sólo está disponible cuando no esté conectado a PolicyServer.
- Los cambios realizados a los usuarios a través de la consola de recuperación se sobrescribirán cuando Full Disk Encryption se conecte a PolicyServer.

Algunas consideraciones para las contraseñas:

- Las contraseñas asignadas, ya sea en una nueva cuenta o en una existente, son contraseñas fijas.
- La caducidad de contraseña de usuario se puede especificar directamente mediante el calendario de caducidad de contraseña.
- El valor predeterminado de un nuevo usuario será la fecha determinada por la política Cambiar contraseña cada, ubicada en: **Común** > **Autenticación** > **Contraseña de usuario**.

Nota

Establezca la fecha en la fecha actual o en una fecha anterior para forzar un cambio de contraseña inmediato; si se establece en el futuro especificará un cambio en esa fecha.

Editar usuarios

Para la edición de usuarios en la consola de recuperación se aplican todas las reglas de PolicyServer. Para obtener información detallada acerca de las reglas, consulte *Agregar usuarios a PolicyServer en la página 4-10*.

Procedimiento

1. Seleccione el usuario de la lista de usuarios.
2. Actualice la información deseada.
3. Seleccione el tipo de usuario: Administrador, autenticador o usuario.
4. Establezca la fecha de caducidad de la contraseña.

5. Haga clic en **Guardar**.

   El usuario se ha actualizado.

Agregar usuarios

Procedimiento

1. Haga clic en **Agregar usuario**.
2. Proporcione el nombre de usuario y la contraseña, y confirme la contraseña.
3. Seleccione el método de autenticación desde la lista desplegable **Tipo de autenticación**.
4. Establezca la fecha de caducidad de la contraseña.
5. Haga clic en **Guardar**.

   El nuevo usuario aparecerá en la Lista de usuarios. Aparecerá una ventana de confirmación.
6. Haga clic en **Aceptar** para cerrar la ventana de confirmación.

   Se ha agregado el nuevo usuario.

Eliminar usuarios

Procedimiento

1. Seleccione un usuario de la lista de usuarios.
2. Haga clic en **Eliminar usuario**.

   Aparecerá una ventana de confirmación de eliminación de usuario.
3. Haga clic en **Sí**.

El usuario se ha eliminado de la lista de usuarios.

Administrar políticas

Utilice Administrar políticas para establecer varias políticas para la consola de recuperación de Full Disk Encryption. Para obtener información detallada sobre estas políticas, consulte *Descripción de políticas en la página 3-1*.

Nota

La opción Administrar políticas solo está disponible cuando no hay conexión con PolicyServer; los cambios se sobrescribirán la próxima vez que Full Disk Encryption se conecte a PolicyServer.

Ver registros

Ver registros permite que un administrador revise los registros y muestre los datos en función de los criterios específicos. Esta opción está disponible en la consola de recuperación con Windows. No está disponible en el arranque previo de Full Disk Encryption.

Para obtener más información sobre cómo ver los registros de Full Disk Encryption, consulte *Acceso a la consola de recuperación desde Windows en la página 5-18*.

Configuración de red

Utilice Configuración de red para comprobar, probar o cambiar las opciones de red que utiliza el arranque previo de Full Disk Encryption. Hay tres pestañas: **IPv4**, **IPv6** y **PolicyServer**.

Nota

Una novedad de Full Disk Encryption 3.1.3 es la capacidad de cambiar PolicyServer o la empresa sin tener que quitar y reinstalar Full Disk Encryption.

Administración de la configuración de red

La opción **Obtener configuración de Windows** está seleccionada de forma predeterminada tanto para IPv4 como para IPv6. Anule la selección de este control para configurar manualmente la configuración de red.

- Si selecciona **DHCP** (IPv4) u **Obtener dirección automáticamente** (IPv6) se utilizará la dirección IP asignada automáticamente.
- Si selecciona **IP estática** se activarán todos los campos de esta sección.
- En la pestaña **IPv6**, si selecciona **IP estática** cuando el campo Dirección IP está vacío, se creará una dirección IP única en la dirección de hardware del equipo.

Administración de la configuración de PolicyServer

Procedimiento

1. Abra la pestaña **PolicyServer**. Hay dos campos de texto: **Servidor actual**y **Empresa actual**.
   - Para cambiar la empresa actual:
     a. Haga clic en **Cambiar empresa**.
     b. En el mensaje de advertencia que aparece, haga clic en **Sí**.
     c. Especifique el nombre de usuario, la contraseña, la empresa y el nombre de servidor y, a continuación, haga clic en **Guardar**.

     ¡ADVERTENCIA!

     El cambio de empresa requiere que se configuren de nuevo las políticas, volver a crear los grupos y eliminar cualquier contraseña almacenada en caché, el historial de contraseñas y los registros de auditoría.
   - Para cambiar el servidor actual:
     a. Haga clic en **Cambiar servidor**.
     b. En el mensaje de advertencia, haga clic en **Sí**.

c. Especifique la dirección del nueov servidor y haga clic en **Guardar**.

2. Haga clic en **Cancelar** para volver a la pantalla de opciones del menú Consola de recuperación.

Métodos de recuperación de Full Disk Encryption

Una vez que un dispositivo está totalmente cifrado mediante Full Disk Encryption, pueden darse casos en los que un administrador necesite realizar acciones de restauración del sistema:

- Se ha perdido la contraseña del administrador local
- El entorno de Windows está dañado

Importante

Para el cifrado de software, las herramientas de recuperación de datos estándar (Disco de recuperación de Windows, ERD Commander, UBCD) no pueden tener acceso a un sistema Full Disk Encryption 3.1.3 cifrado; por lo tanto, el sistema debe descifrarse antes de llevar a cabo cualquier acción de recuperación.

Los métodos de recuperación de datos están disponibles para los administradores y autenticadores de Endpoint Encryption, de forma que puedan recuperar los datos cuando el dispositivo no funcione correctamente. Full Disk Encryption debe estar instalado.

TABLA 5-6. Métodos de recuperación para dispositivos protegidos con Full Disk Encryption

MÉTODOS DE RECUPERACIÓN	DESCRIPCIÓN	CUÁNDO UTILIZARLO
Desinstalación de Full Disk Encryption	La desinstalación de Full Disk Encryption elimina Full Disk Encryption del dispositivo. Una vez finalizada la desinstalación, puede continuar con la acción de recuperación establecida en Windows.	El entorno de Windows funciona con normalidad.
Consola de recuperación	La opción **Consola de recuperación** > **Descifrar disco** de Full Disk Encryption permite a los administradores descifrar el disco duro seleccionado de forma instantánea o guardar la imagen del disco duro descifrado en medios extraíbles. **Nota** Este método no se recomienda si Windows está funcionando con normalidad.	El arranque previo de Full Disk Encryption se carga, pero no Windows.
CD de reparación	El CD de reparación es un CD de arranque que se utiliza para descifrar una unidad dañada cuando no es posible arrancar el dispositivo desde Full Disk Encryption. Un síntoma típico de un disco dañado es una pantalla en negro. **¡ADVERTENCIA!** No lo use si Windows funciona con normalidad.	• El arranque previo de Full Disk Encryption no se carga. • Full Disk Encryption no puede autenticarse.

Nota

Para descifrar la unidad, el usuario debe tener derechos de administrador de empresa o de grupo de Endpoint Encryption y tener derechos de administrador en Windows.

CD de reparación

El CD de reparación de Full Disk Encryption es un disco de arranque que sirve para descifrar completamente un dispositivo si el equipo no se puede iniciar.

Nota

- Si se ha producido daño físico (sectores defectuosos) en la unidad de disco duro, la unidad no se podrá descifrar completamente o podrá quedar inutilizable.
- Compruebe que el cable de unidad del disco duro está conectado correctamente.

Hay disponibles varias opciones tras el arranque desde el CD de reparación:

TABLA 5-7. Opciones del CD de reparación

OPCIÓN	DESCRIPCIÓN
Recuperación	Inicia la consola de recuperación.
Desbloquear	Permite desbloquear un dispositivo que ha sido bloqueado porque: • se han realizado demasiados intentos de inicio de sesión • no hay ninguna comunicación con PolicyServer para un período de tiempo especificado **Nota** La opción de desbloqueo solo está disponible cuando la política Autenticación remota está definida en **Bloqueada**.
Reiniciar	Reinicia el dispositivo.

Opción	Descripción
Opciones avanzadas	Proporciona acceso a opciones avanzadas: • Eliminar el arranque previo de Full Disk Encryption • Borrar • Forzar descifrado

Tabla 5-8. Opciones avanzadas del CD de reparación

Opción avanzada	Descripción
Eliminar el arranque previo de Full Disk Encryption	Elimina la pantalla de autenticación del arranque previo de Full Disk Encryption del dispositivo. **¡ADVERTENCIA!** Esta acción no se puede deshacer y la unidad no se descifra. Utilice Descifrar disco para eliminar el cifrado.
Borrar	Elimina todos los datos de la unidad.
Volver al principal	Volver a las opciones estándar del CD.
Forzar descifrado	Permite a un administrador descifrar la unidad cuando no se inicia Full Disk Encryption.

¡ADVERTENCIA!

Podría producirse una pérdida de datos si las Opciones avanzadas no se utilizan correctamente.

Recuperación de datos con el CD de reparación

Utilice el CD de reparación para intentar recuperar los datos de un dispositivo cifrado. Sin embargo, hay una serie de consideraciones a tener en cuenta antes de intentar descifrar el disco:

- Utilice únicamente el CD de reparación si el dispositivo está cifrado, o ha comenzado el cifrado.

- Si el dispositivo contiene datos importantes, realice una imagen de copia de seguridad antes de continuar. Para obtener instrucciones, vaya a http://esupport.trendmicro.com/solution/en-us/1059802.aspx.
- No intente descifrar un portátil a no ser que esté conectado a una fuente de alimentación de CA.
- Si el CD de reparación no arranca, compruebe que el dispositivo tiene la última versión de la BIOS instalada. Actualice la BIOS del sistema si fuese necesario.
- El descifrado de la unidad mediante este método tarda al menos tanto como el proceso de cifrado inicial.
- Si se detecta un sector defectuoso, puede que se ralentice el progreso visible. Deje que el CD continúe el descifrado y póngase en contacto con Asistencia de Trend Micro antes de interrumpir el proceso.



¡ADVERTENCIA!

No interrumpa el proceso una vez iniciado el descifrado desde el CD o puede que produzca una pérdida de datos irreversible.

Descifrar un disco mediante el CD de reparación

Procedimiento

1. Encienda el sistema conectado a la red.
   a. Presione inmediatamente **F12** (o el botón correspondiente para especificar las opciones de inicio).
   b. Inserte el CD de reparación y seleccione la unidad de CD o DVD en la pantalla de opciones de inicio.

      El dispositivo se inicia en el entorno del CD de reparación.
2. En el arranque previo de Full Disk Encryption, seleccione **Consola de recuperación**.
3. Proporcione el nombre de usuario y la contraseña.

4. Haga clic en **Iniciar sesión**.

   Se mostrará la consola de recuperación.

5. Seleccione **Descifrar disco** para empezar a descifrar completamente el dispositivo.

6. Cuando finalice el descifrado, haga clic en **Salir** para volver al menú del CD de reparación.

7. Haga clic en **Reiniciar** para reiniciar el dispositivo.

Nota

Retire el CD para poder iniciar el dispositivo con normalidad.

---

8. Inicie sesión en el arranque previo de Full Disk Encryption.

9. Inicie sesión en Windows y continúe con el método preferido de recuperación.

Limpieza de los archivos de Full Disk Encryption

El descifrado de una unidad elimina los cambios del MBR y otros elementos esenciales que se usan para proteger el dispositivo. Para el cifrado por de software, descifre el disco completamente antes de desinstalar Full Disk Encryption. En caso contrario, es posible que se bloquee el sistema operativo.

¡ADVERTENCIA!

Si se ejecuta el MSI para realizar la desinstalación en una máquina que no es DriveTrust, no se encontrará el sistema operativo cuando el cliente reinicie el equipo.

Procedimiento

1. Desde una línea de comandos:

   a. Ejecute `msiexec.exe /X{17BACE08-76BD-4FF5-9A06-5F2FA9EBDDEA}`

2. Desde Windows:

a. Abra **regedit** en Windows y busque la siguiente clave: `HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{17BACE08-76BD-4FF5-9A06-5F2FA9EBDDEA}`.

b. Vaya a la clave `UninstallString`: `msiexec.exe /x {17BACE08-76BD-4FF5-9A06-5F2FA9EBDDEA}`.

c. Copie la cadena.

d. Abra **Ejecutar...** y pegue la cadena en el campo de texto **Abrir**.

e. Haga clic en **Aceptar**.

Aparecerá la ventana **Instalador de Windows**.

f. En la confirmación de desinstalación, haga clic en **Sí**.

Nota

Si aparece la ventana **Control de cuentas de usuario**, haga clic en **Permitir**.

g. Cuando se le pida que desactive DrAService, seleccione la segunda opción de botón de radio, **No cerrar las aplicaciones**, y, a continuación, haga clic en **Aceptar**.

3. Cuando se le pida que reinicie el dispositivo, haga clic en **Sí**. En caso contrario, reinicie el dispositivo manualmente.

Capítulo 6

Trabajar con FileArmor

FileArmor protege los archivos y carpetas individuales en discos duros y dispositivos de medios extraíbles (unidades USB). Los administradores pueden configurar políticas que especifiquen las carpetas y unidades que se cifrarán en el dispositivo y políticas sobre los datos cifrados en los medios extraíbles. El cifrado se realiza después de llevarse a cabo la autenticación.

FileArmor también puede proteger archivos diferentes con claves diferentes, lo que permite a los administradores configurar políticas de acceso a un dispositivo y políticas independientes para acceder a determinados archivos. Esto resulta útil en entornos en los que varios usuarios acceden a un punto final.

En este capítulo se describen los siguientes temas:

- *Menú del icono de la bandeja del sistema de FileArmor en la página 6-8*
- *Autenticación de FileArmor en la página 6-2*
- *Cifrado de FileArmor en la página 6-11*
- *Eliminación segura de FileArmor en la página 6-16*

Autenticación de FileArmor

En esta sección se explica cómo autenticar mediante FileArmor y los aspectos particulares del uso de FileArmor. Todos los métodos de autenticación de Endpoint Encryption están disponibles en FileArmor. Consulte *Funciones y autenticación de cuentas en la página 1-12* para obtener información detallada sobre los métodos de autenticación.

Primera autenticación con FileArmor

Cuando se inicia FileArmor por primera vez, se necesita un registro inicial para identificar PolicyServer. El método de autenticación predeterminado es la contraseña fija. Hay otras opciones disponibles en función de la configuración de las políticas.

Procedimiento

1. Haga clic con el botón derecho en el icono de la bandeja de FileArmor y seleccione **Registro**.
2. Proporcione el nombre de usuario y la contraseña.
3. Especifique la dirección IP de PolicyServer (o el nombre de host) y la empresa de PolicyServer.
4. Haga clic en **Aceptar**.

   Aparecerá la pantalla **Cambiar la contraseña**.
5. Seleccione el método de autenticación que desee en la lista desplegable.
6. Especifique y confirme la nueva contraseña y, a continuación, haga clic en **Aceptar**.

Nota

Sin la autenticación en FileArmor se le denegará el acceso a los archivos y medios extraíbles.

Autenticación de dominio de FileArmor

Para lograr una integración y un uso del proceso de autenticación de dominio/inicio de sesión único (Single Sign-On, SSO) de FileArmor sin problemas, asegúrese de que se cumplen los requisitos siguientes:

- El usuario pertenece a un grupo cuya política **Común** > **Autenticación** > **Autenticación de dominio** está establecida en **Sí**
- En el nivel de grupo, vaya a **Común** > **Autenticación** > **Inicio de sesión de red** y establezca el nombre de host y el nombre de dominio.
- PolicyServer y todos los dispositivos que utilizan la autenticación de dominio están en el mismo dominio.
- La cuenta de usuario se configura tanto en Active Directory como en PolicyServer. El nombre de usuario distingue entre mayúsculas y minúsculas y debe coincidir exactamente.



Nota

El inicio de sesión único (SSO) de FileArmor requiere que la siguiente política esté habilitada: **Común** > **Autenticación** > **Inicio de sesión de red** > **Autenticación de dominio**.

Autenticación mediante autenticación de dominio

Habilite la autenticación de dominio en:

Nombre del grupo > **Políticas** > **Común** > **Autenticación** > **Inicio de sesión de red** > **Autenticación de dominio**.

Procedimiento

1. Elija **Autenticación de dominio** como tipo de autenticación.
2. Proporcione el nombre de usuario y la contraseña de la cuenta de dominio.
3. Haga clic en **Aceptar**.

Nota

- Los usuarios de dominio no pueden cambiar las contraseñas y FileArmor no puede cambiar una contraseña de dominio de Windows. Esa funcionalidad se controla con Active Directory.
- La autenticación de dominio no se puede usar con un PIN de tarjeta inteligente.
- Los usuarios de dominio disponen de Ayuda remota. Sin embargo, la contraseña de dominio debe restablecerse en Active Directory si se olvida.

Autenticación con tarjeta inteligente de FileArmor

Para usar la autenticación con tarjeta inteligente, asegúrese de que se cumplen los requisitos siguientes:

- Política de FileArmor **Iniciar sesión** > **Contraseña** > **Símbolo físico requerido** = **Sí**.
- El lector de tarjetas inteligentes está conectado y la tarjeta inteligente está insertada.

Nota

FileArmor solo admite tarjetas inteligentes CASC y PIC

- ActivClient 6.1 con todos los Service Packs y actualizaciones debe estar instalado.
- Especifique el PIN de la tarjeta inteligente en el campo de contraseña.

¡ADVERTENCIA!

Si no proporciona una contraseña correcta, se enviará un error de contraseña y la tarjeta inteligente podría bloquearse.

Autenticación con una tarjeta inteligente

La autenticación por tarjeta inteligente de FileArmor solo está disponible si se habilita mediante política. En PolicyServer, marque Tarjeta inteligente como opción de

autenticación en **FileArmor** > **Iniciar sesión** > **Métodos de autenticación permitidos**.

Procedimiento

1. En FileArmor, abra FileArmor y seleccione **Tarjeta inteligente** en la lista desplegable de opciones de autenticación.
2. Proporcione el nombre de usuario.
3. Proporcione el PIN de tarjeta inteligente o la contraseña fija (si corresponde).
4. Haga clic en **Aceptar**.

Autenticación por código de color de FileArmor

La autenticación por código de color de FileArmor solo está disponible si se habilita mediante política. La política está disponible en: **Nombre del grupo** > **Políticas** > **FileArmor** > **Iniciar sesión** > **Métodos de autenticación permitidos**

Procedimiento

1. Seleccione **ColorCode** en la lista desplegable de métodos de autenticación.
2. Introduzca una combinación de códigos de color única.
3. Haga clic en **Aceptar**.

Autenticación con PIN de FileArmor

La autenticación por PIN de FileArmor solo está disponible si se habilita mediante política. La política está disponible en: **Nombre del grupo** > **Políticas** > **FileArmor** > **Iniciar sesión** > **Métodos de autenticación permitidos**.

Procedimiento

1. Seleccione **PIN** en la lista desplegable de métodos de autenticación.

2. Especifique la combinación del PIN.
3. Haga clic en **Aceptar**.

Cambio de contraseña en FileArmor

Para cambiar la contraseña, el usuario debe autenticarse en FileArmor con una cuenta de usuario. Las cuentas de administrador o autenticador no pueden cambiar la contraseña. La contraseña se puede cambiar a cualquiera de los métodos admitido por las políticas de PolicyServer.

Procedimiento

1. Haga clic con el botón derecho en el icono de la bandeja de FileArmor y seleccione **Cambiar la contraseña**.
2. Especifique la contraseña y haga clic en **Siguiente**
3. Seleccione uno de los métodos de autenticación disponibles, proporcione y confirme la nueva contraseña y haga clic en **Aceptar**.

   La nueva contraseña se actualiza y se muestra un mensaje de confirmación.

Restablecimiento forzoso de contraseña

FileArmor evita el acceso no autorizado a archivos y carpetas cifrados bloqueando los archivos protegidos si se realizan demasiados intentos fallidos de autenticación o si el punto final no se ha comunicado con PolicyServer durante un tiempo especificado. En función de la política, FileArmor bloquea el acceso del usuario o aplica un tiempo de demora antes de poder realizar intentos de autenticación.

Desbloqueo de un dispositivo

Si un usuario ha excedido el número de intentos de autenticación y hay establecidas políticas para aplicar la autenticación remota, FileArmor bloquea las carpetas de Endpoint Encryption y notifica al usuario que se necesita Ayuda remota. La Ayuda

remota se utiliza para desbloquear FileArmor y requiere la asistencia del autenticador de empresa o de grupo.

Procedimiento

1. Haga clic con el botón derecho en el icono de la bandeja de FileArmor y seleccione **Ayuda remota**.

   Aparecerá la ventana **Ayuda remota**.



FIGURA 6-1. Ayuda remota de FileArmor

2. Especifique el nombre del usuario.
3. Haga clic en **Obtener pregunta**.
4. Escriba la **Respuesta** proporcionada por el autenticador de empresa o de grupo.
5. Haga clic en **Iniciar sesión**.

El usuario se autentica en FileArmor y se muestra una notificación.

Demora de tiempo

Si un usuario excede el número de intentos de autenticación y la política está establecida para aplicar un tiempo de demora temporal que no se puede omitir y debe expirar antes de permitir la autenticación.

Después de exceder el número permitido de intentos de autenticación fallidos, FileArmor bloquea el dispositivo y notifica al usuario que el dispositivo está bloqueado. La capacidad para iniciar sesión o restablecer la contraseña está deshabilitada durante el tiempo de demora. La duración del tiempo de demora se determina mediante directiva. Una vez transcurrido el tiempo de demora, el usuario se puede autenticar.

Menú del icono de la bandeja del sistema de FileArmor

Una vez instalado FileArmor, se muestra un icono () en la bandeja del sistema. El icono proporciona acceso a numerosas funciones de FileArmor. Haga clic con el botón derecho en el icono para mostrar las opciones del menú.

TABLA 6-1. Opciones del icono de la bandeja del sistema de FileArmor

ELEMENTO DE MENÚ	FUNCIÓN
Registrar	Primer registro del usuario de FileArmor en PolicyServer. Para conocer más detalles, consulte *Primera autenticación con FileArmor en la página 6-2*.
Iniciar sesión / Cerrar sesión	Autenticación en PolicyServer.
Cambiar contraseña	Permite que usuarios autenticados sin dominio cambien su contraseña. Para conocer más detalles, consulte *Cambio de contraseña en FileArmor en la página 6-6*.

Elemento de menú	Función
Ayuda remota	Desbloquee FileArmor usando la opción Ayuda remota para autenticarse si se olvidó la contraseña, si se realizaron demasiados intentos fallidos de autenticación o si el dispositivo no se ha comunicado con PolicyServer durante un tiempo especificado. Para conocer más detalles, consulte *Restablecimiento forzoso de contraseña en la página 6-6*.
Sincronización con PolicyServer	Descargue manualmente actualizaciones de políticas de PolicyServer. Útil para probar la conectividad con PolicyServer. Para conocer más detalles, consulte *Sincronización con PolicyServer en la página 6-9*.
Sincronización con el archivo sin conexión de PolicyServer	Consulte *Sincronización con archivos sin conexión de PolicyServer en la página 6-10* para obtener más información.
Ocultar notificación	Silencia todas las notificaciones de FileArmor.
Acerca de FileArmor	Muestra información de FileArmor, incluida la versión, la última hora de sincronización y el usuario autenticado. Para conocer más detalles, consulte *Menú del icono de la bandeja del sistema de FileArmor en la página 6-8*.
Cerrar la bandeja	Quita temporalmente el icono de la bandeja de FileArmor.

Sincronización con PolicyServer

Los clientes de punto final pueden descargar manualmente nuevas políticas de FileArmor abriendo el icono de FileArmor en la bandeja y seleccionando **Sincronizar con PolicyServer**.

Nota

- Los clientes no necesitan autenticarse en políticas de sincronización.
- Si no hay disponible una conexión de red o PolicyServer, se muestra un error **No se puede sincronizar con el servidor**.

Sincronización con archivos sin conexión de PolicyServer

Las actualizaciones sin conexión funcionan con FileArmor 3.0.13.2447 o versiones posteriores y ahora funcionan con las instalaciones x64 de FileArmor. Si se genera la actualización, las actualizaciones sin conexión reemplazarán la contraseña de usuario existente con la nueva contraseña fija.

Las contraseñas sincronizadas no reemplazarán la contraseña de usuario cuando se produzca la actualización para mantener la misma funcionalidad de los dispositivos administrados.

Se necesita una contraseña fija para añadir un usuario a un cliente de punto final sin conexión. El proceso sin conexión generará dos archivos:

- El primer archivo, con la extensión .exe, se usa para actualizar los dispositivos de Full Disk Encryption existentes.
- El segundo, con la extensión de la actualización de políticas, se utiliza para actualizar FileArmor.



Nota

Las directivas de Blackberry se eliminan de todas las nuevas instalaciones sin conexión en las que Blackberry no estaba habilitado por el archivo de licencia. Esto reducirá significativamente el tamaño del archivo.

Cambiar PolicyServer

El PolicyServer al que se conecta FileArmor se puede actualizar en la ventana Acerca de.

Procedimiento

1. Haga clic con el botón derecho en el icono de la bandeja de FileArmor y seleccione **Acerca de FileArmor**.

   Se muestra la ventana **Acerca de**.

2. Haga clic en **Editar PolicyServer**.

3. Especifique el nuevo nombre de host o dirección IP de PolicyServer.
4. Haga clic en **Aceptar**.

   Ahora, el nuevo PolicyServer administra FileArmor.

Cifrado de FileArmor

Los archivos se pueden cifrar con políticas de FileArmor definidas localmente o con políticas definidas por PolicyServer. El método utilizado depende de las necesidades de la empresa y del usuario final en lo que respecta al acceso a archivos y del nivel de seguridad requerido.

Para cifrar automáticamente los archivos, puede guardarlos en varias ubicaciones:

- Una carpeta del dispositivo
- Una carpeta que se encuentra en un medio extraíble
- Un dispositivo multimedia extraíble completamente cifrado

Otra opción para cifrar los archivos es hacer clic con el botón derecho en el archivo y seleccionar una de las siguientes opciones del menú contextual de FileArmor:

TABLA 6-2. Opciones del menú contextual de FileArmor

ELEMENTO DE MENÚ	DESCRIPCIÓN
Archivar	Crea una copia cifrada del archivo especificado.
Archivar y grabar	Crea una copia cifrada del archivo especificado y la graba en un CD/DVD.

Cifrado de clave local de FileArmor

La función de clave local permite al usuario cifrar los archivos de forma que nadie más pueda verlos.

Nota

- Establezca **FileArmor** > **Cifrado** > **Método de cifrado permitido** en **Clave de usuario única**.
- Solo el usuario que ha creado los archivos de clave local puede acceder a ellos en un dispositivo FileArmor.
- Cuando se cifra un archivo, FileArmor crea un archivo nuevo. El archivo original permanece sin cifrar en su ubicación original.

¡ADVERTENCIA!

En función del sistema operativo Windows, un usuario podría ver el contenido de la carpeta si cambia a un usuario diferente sin reiniciar Windows. Aunque se pueden ver los nombres de archivo y el contenido de la carpeta, el contenido de los archivos no está disponible. Esto se debe al que el sistema operativo Windows almacena en caché la estructura de archivos para acelerar las búsquedas.

Creación de una clave local

Procedimiento

1. Haga clic con el botón derecho en el archivo que desee y seleccione **FileArmor** > **Archivo** > **Clave local**.

   Los archivos o carpetas originales permanecen sin cambios y se pueden guardar o eliminar.

Cifrado de clave compartida de FileArmor

Los archivos se pueden cifrar para que solo los vean los miembros de un grupo de políticas mediante la función Clave compartida.

- Solo el usuario que ha creado los archivos de clave local puede acceder a ellos en un dispositivo FileArmor.
- Establezca dos políticas: **Métodos de cifrado permitidos** en **Clave única de grupo** y **Clave de cifrado utilizada** en **Clave de grupo**.

- Para que un usuario de FileArmor que esté en la empresa de PolicyServer pueda ver los archivos cifrados, establezca **Clave de cifrado utilizada** en **Clave de empresa**.
- Cuando se cifra un archivo, FileArmor crea un archivo nuevo. El archivo original permanece sin cifrar en su ubicación original.



¡ADVERTENCIA!

En función de la configuración de los permisos en Windows, un usuario puede ver el contenido de la carpeta cifrada si cambia a un usuario diferente sin reiniciar Windows. Aunque se pueden ver los nombres de archivo y el contenido de la carpeta, el contenido de los archivos no está disponible. Esto se debe al que el sistema operativo Windows almacena en caché la estructura de archivos para acelerar las búsquedas.

Creación de una clave compartida

Haga clic con el botón derecho en el archivo que desee y seleccione **FileArmor** > **Archivo** > **Clave compartida**. Los archivos o carpetas originales permanecen sin cambios y se pueden guardar o eliminar.

Cifrado de contraseñas fijas de FileArmor

FileArmor puede crear archivos cifrados usando una contraseña fija. Opcionalmente, el archivo cifrado puede ser autoextraíble, lo que significa que los destinatarios no necesitan FileArmor para descifrar el archivo. Tenga en cuenta lo siguiente:

- No hay ninguna funcionalidad disponible para recuperar la contraseña con los archivos autoextraíbles. Si olvida la contraseña, el archivo cifrado no se puede recuperar.
- Debido a una limitación de Windows, los archivos ejecutables (autoextraíbles) no pueden ser mayores de 2GB.

Creación de una clave de contraseña fija

Procedimiento

1. Haga clic con el botón derecho en el archivo que desee y seleccione **FileArmor** > **Archivo** > **Contraseña fija**.
2. Proporcione la contraseña fija y confirme.

   Nota

   Marque **Datos cifrados de salida como un archivo de extracción automática** si fuera necesario.

3. Haga clic en **Aceptar**.

   El archivo está cifrado.

4. Para descifrar el archivo, haga doble clic en él para descifrar el archivo, proporcione la contraseña de archivo y haga clic en **Aceptar**.
5. Para los archivos autoextraíbles, haga doble clic en el archivo, proporcione la contraseña de archivo, seleccione la ubicación de extracción, elija si desea abrir el destino después de la extracción o sobrescribir los archivos existentes y haga clic en **Continuar**.

   Los archivos o carpetas originales permanecen sin cambios y se pueden guardar o eliminar.

Cifrado de certificado digital de FileArmor

FileArmor puede cifrar archivos con certificados digitales (tarjetas inteligentes) del almacén de certificados de Windows.

Creación de una clave de certificado digital

Procedimiento

1. Haga clic con el botón derecho en el archivo que desee y seleccione **FileArmor** > **Archivo** > **Certificado**.
2. Seleccione un **Almacén de certificados** y haga clic en **Recopilar certificados**.
3. Seleccione uno o varios certificados y haga clic en **Aceptar**.



Nota

Los certificados se recopilan del almacén de certificados de Windows.

4. Seleccione una unidad óptica que contenga un CD/DVD en blanco.
5. Haga clic en **Aceptar**.

   Los archivos o carpetas originales permanecen sin cambios y se pueden guardar o eliminar.

Archivar y grabar de FileArmor

La función **Archivar y grabar** de FileArmor se puede utilizar para escribir archivos cifrados en CD/DVD. Los archivos son autoextraíbles y se pueden cifrar con una contraseña fija o con un certificado digital.

Grabar un archivo con una contraseña fija

Procedimiento

1. Haga clic con el botón derecho y seleccione **FileArmor** > **Archivar y grabar** > **Contraseña fija** en el menú contextual de FileArmor.
2. Proporcione una contraseña y confirme.

3. Seleccione una unidad que contenga un disco grabable.
4. Haga clic en **Aceptar**.

   El archivo autoextraíble se graba en el CD/DVD.

Grabar un archivo con un certificado

Procedimiento

1. Haga clic con el botón derecho y seleccione **FileArmor** > **Archivar y grabar** > **Certificado** en el menú contextual de FileArmor.
2. Seleccione un **Almacén de certificados** y haga clic en **Recopilar certificados**.
3. Seleccione uno o varios certificados y haga clic en **Aceptar**.
4. Seleccione una unidad óptica que contenga un CD/DVD en blanco.
5. Haga clic en **Aceptar**.

   El archivo autoextraíble se graba en el CD/DVD.

Eliminación segura de FileArmor

FileArmor dispone de una función de eliminación segura que borra y limpia los archivos seleccionados y el historial de archivos de tu dispositivo.

Procedimiento

1. Haga clic con el botón derecho y vaya a **FileArmor** > **Eliminación segura**.
2. Haga clic en **Sí** para eliminar el archivo de forma permanente.

Capítulo 7

Trabajar con KeyArmor

Las unidades flash USB de KeyArmor protegen los datos con cifrado de hardware siempre activado y protección antivirus y antimalware integrada para satisfacer los requisitos de cumplimiento y las estrictas normas gubernamentales. Con KeyArmor, los administradores tienen visibilidad y control total de quién, cuándo, dónde y cómo se utilizan las unidades flash USB en su organización.

En este capítulo se describen los siguientes temas:

- *Características de KeyArmor en la página 7-4*
- *Autenticación en KeyArmor en la página 7-2*
- *Uso de KeyArmor en la página 7-6*

Autenticación en KeyArmor

La autenticación en KeyArmor proporciona a los usuarios diversos métodos de identificación. Estas opciones ofrecen la flexibilidad necesaria para cumplir con los requisitos de seguridad de la empresa. Una autenticación con éxito permite al usuario acceder al dispositivo.

Para obtener información más detalles acerca de la autenticación de Endpoint Encryption, consulte *Funciones y autenticación de cuentas en la página 1-12*.

Autenticación en KeyArmor por primera vez

Procedimiento

1. Inserte el dispositivo KeyArmor en un puerto USB para iniciar el software.
   - Si KeyArmor se inicia automáticamente, se muestra la barra de estado y el icono de KeyArmor se agrega a la bandeja.
   - Si KeyArmor no se inicia automáticamente, vaya a Mi dispositivo y abra la unidad KeyArmor.
2. Especifique el nombre de usuario y la contraseña.
3. Especifique el PolicyServer en el campo **Nombre de host** o **Dirección IP**.
4. Especifique el nombre de empresa en el campo **Nombre de empresa**.
5. Haga clic en **Iniciar sesión**.

Cambiar métodos de autenticación

Nota

- Sólo es válido un método de autenticación en un momento del tiempo para cada usuario.
- El usuario sólo puede cambiar su método de autenticación despues de iniciar sesión con éxito en un dispositivo KeyArmor.

Procedimiento

1. Haga clic con el botón derecho en el icono de KeyArmor de la bandeja y seleccione **Cambiar la contraseña**.

   Aparece la ventana **Cargando** seguida de la pantalla **Cambiar la contraseña** según el método de autenticación actual del usuario.

2. Haga clic en **Autenticación**.
3. Seleccione un nuevo método de autenticación.
4. Proporcione la contraseña actual.
5. Haga clic en **Cambiar** para mostrar las pantallas del nuevo método de autenticación.

   Aparece la pantalla **Cambio de método de autenticación finalizado**.

Contraseña fija

Las contraseñas fijas son el método de autenticación más común de un usuario. El usuario elige la contraseña. Para configurar políticas de restricción sobre contraseñas, vaya a **KeyArmor** > **Inicio de sesión** en el nivel de grupo o de empresa.

Nota

Siempre se utiliza la contraseña fija como método inicial de autenticación en KeyArmor.

Procedimiento

1. Especifique y confirme la nueva contraseña fija.
2. Realice una de las operaciones siguientes:
   - Para finalizar el cambio de contraseña, haga clic en **Cambiar**.
   - Para borrar todo el contenido de los campos, haga clic en **Borrar**.

   El usuario se autentica en KeyArmor y puede guardar datos en la carpeta **SECURE DATA**; el icono de KeyArmor se muestra en la bandeja del sistema.

Características de KeyArmor

Esta sección describe las características principales de KeyArmor.

Componentes de dispositivos

KeyArmor monta dos unidades al insertar el dispositivo en un puerto USB.



FIGURA 7-1. Dispositivos KeyArmor

- **KeyArmor (E:)** contiene los archivos de programa de KeyArmor.
- **SECURE DATA (F:)** es la unidad de almacenamiento para el usuario de KeyArmor. KeyArmor cifra todos los archivos almacenados en esta unidad.

Protección de archivos con KeyArmor

Para mantener la seguridad de los archivos con KeyArmor, copie o arrastre la carpeta, archivo o documento seleccionado a la unidad SECURE DATA de KeyArmor.

Los archivos guardados en KeyArmor se cifran automáticamente y son accesibles con credenciales Endpoint Encryption válidas. Los archivos permanecen cifrados mientras están almacenados en KeyArmor.



Nota

Para asegurarse de tener definiciones de antivirus actualizadas, no copie ningún archivo al dispositivo KeyArmor hasta que finalice la actualización de antivirus inicial.

Ninguna información sin controlar

Existen distintos métodos que KeyArmor utiliza para evitar dejar ninguna información en el dispositivo local:

- Al examinar archivos del dispositivo KeyArmor no se copian datos al dispositivo host.
- Abrir y editar documentos utilizando aplicaciones en el dispositivo host puede almacenar datos de archivos temporales o de recuperación en el dispositivo host.
- La mayoría de las aplicaciones de software se pueden configurar para que almacenen sus datos de archivos temporales y de recuperación en el dispositivo KeyArmor.

Actualizaciones y actividad de antivirus de KeyArmor

Tras la autenticación, se intentará actualizar las definiciones de antivirus de KeyArmor KeyArmor muestra avisos acerca de la actividad de actualización de antivirus.



¡ADVERTENCIA!

No desconecte ni retire un dispositivo KeyArmor de su cliente de punto final mientras está en curso la actualización de antivirus.

Copiar o abrir archivos desde KeyArmor es una actividad iniciada por el usuario final. Los archivos se exploran al guardarse o copiarse en KeyArmor. Si se encuentra un virus, el administrador del sistema controla la acción resultante, incluido un intento de reparar el archivo, eliminarlo o borrar completamente el dispositivo KeyArmor. Los usuarios pueden iniciar una exploración completa de su dispositivo KeyArmor una vez se han autenticado.

Notificación de comprobación de disco de KeyArmor

Retirar inadecuadamente un dispositivo KeyArmor sin una extracción segura puede causar daños en el sistema de archivos. Cierre siempre su sesión en KeyArmor antes de retirar físicamente el dispositivo. En caso de apagado del sistema, retirada no segura de la unidad u otras circunstancias imprevistas, se le podría solicitar una comprobación del disco la próxima vez que inserte el dispositivo. Es seguro ignorar y pasar esta comprobación; KeyArmor comprobará el disco automáticamente y corregirá cualquier error.

Uso de KeyArmor

Esta sección explica cómo utilizar KeyArmor.

Advertencias acerca de dispositivos sin cifrar

- Los usuarios de KeyArmor deben seguir la política de su organización relativa al transporte de datos fuera del dispositivo de trabajo asignado a un individuo.
- KeyArmor cifra todos los archivos almacenados en él.
- El software de KeyArmor se ejecuta desde el dispositivo y en ningún momento copia datos del software de KeyArmor al dispositivo host.
- Al examinar los archivos del dispositivo tampoco se copian datos al dispositivo host.

- Copiar archivos a un dispositivo host es una acción iniciada por el usuario que se puede llevar a cabo sólamente despues de la autenticación apropiada en el dispositivo.
- Algunas aplicaciones de software que se ejecutan en el host pueden almacenar datos de archivos temporales y de recuperación en el dispositivo host.
- La mayoría de las aplicaciones se pueden configurar para almacenar datos de archivos temporales y de recuperación en el dispositivo KeyArmor. Se recomienda esta acción si se va a permitir que el dispositivo viaje fuera de los límites de la red de confianza o protegida.

Barra de tareas de KeyArmor

Hay disponibles varias opciones para abrir KeyArmor desde la barra de tareas:

Tabla 7-1. Barra de tareas de KeyArmor

Elemento de menú	Función
Iniciar exploración completa	Explora el dispositivo KeyArmor en busca de amenazas.
Descargar actualizaciones de políticas	Descarga las actualizaciones de políticas más actuales. Por ejemplo, si el administrador realiza un cambio o agrega un método de autenticación y elimina los métodos de autenticación existentes, el usuario puede ser dirigido a descargar actualizaciones de políticas y comenzar inmediatemente a utilizar el nuevo método de autenticación.
Cambiar contraseña	Permite que usuarios autenticados sin dominio cambien su contraseña.
Abrir Secure Data	Abre la unidad SECURE DATA.
Acerca de KeyArmor	Muestra información de KeyArmor, incluida la versión, última hora de sincronización y usuario autenticado.
Fin de sesión	Desconecta KeyArmor.

Menú de KeyArmor

Existen varias opciones disponibles al abrir el menú de KeyArmor:

TABLA 7-2. Opciones de menú de KeyArmor

ELEMENTO DE MENÚ	DESCRIPCIÓN
Autenticación	Consulte *Autenticación en KeyArmor en la página 7-2* para obtener más información.
Descargar actualizaciones de políticas	Descargar actualizaciones de políticas habituales. Por ejemplo, si el administrador realiza un cambio o agrega un método de autenticación y elimina los métodos de autenticación existentes, el usuario puede ser dirigido a descargar actualizaciones de políticas y comenzar inmediatamente a utilizar el nuevo método de autenticación.
Ayuda	Consulte *Menú de ayuda de KeyArmor en la página 7-8* para obtener más información.

Menú de ayuda de KeyArmor

El menú de ayuda de KeyArmor tiene varias opciones de asistencia al usuario.

Si se encuentra

Cuando se pierde un dispositivo KeyArmor y lo encuentra una persona distinta al propietario del dispositivo, la opción **Si se encuentra** proporciona información de contacto que ayudará a esta persona a devolver el dispositivo a su legítimo propietario. Cualquiera puede acceder a esta opción sin introducir credenciales.

El mensaje **Si se encuentra** se crea como una política en PolicyServer.

Procedimiento

1. Para crear un mensaje **Si se encuentra**, vaya a **KeyArmor** > **Mensajes de notificación**.
2. Haga clic con el botón derecho en **Si se encuentra** y seleccione **Propiedades**.

Aparecerá la ventana **Editar valor de política**.

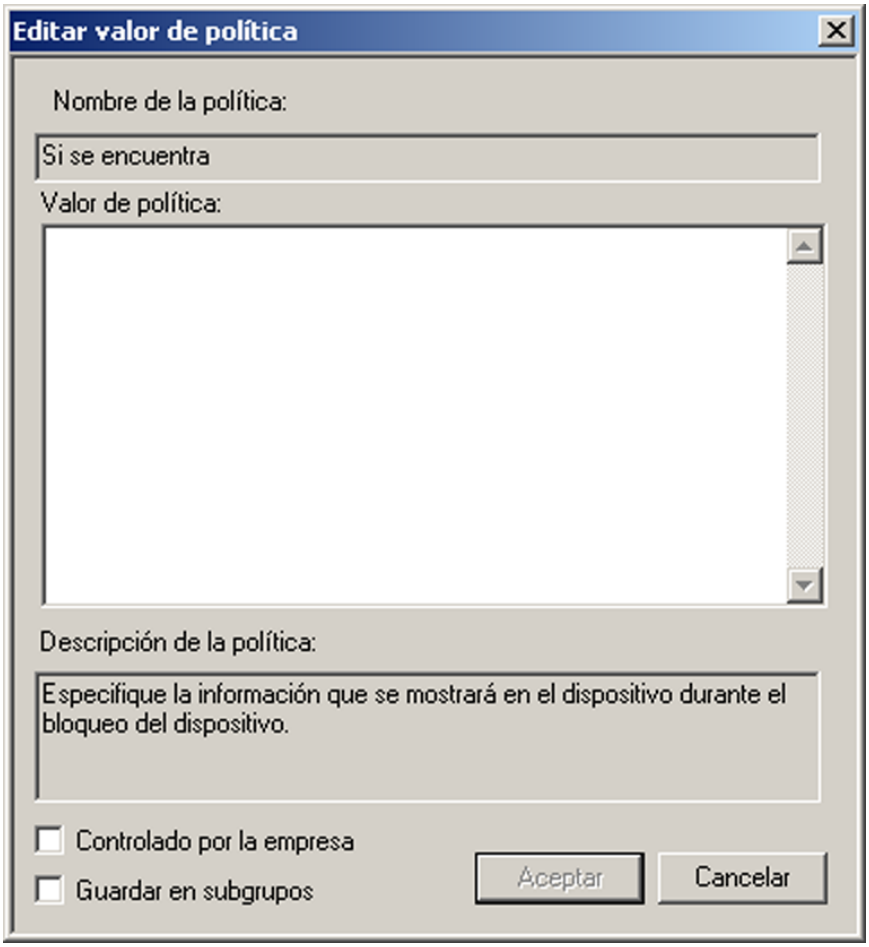


FIGURA 7-2. Editar la política Si se encuentra

3. Especifique mensaje **Si se encuentra** en el campo **Valor de política**.

4. Haga clic en **Aplicar**.

Preguntas y respuestas acerca del restablecimiento de contraseña

Autoayuda permite al usuario responder a una o varias preguntas predefinidas. Las preguntas de autoayuda se crean como políticas en PolicyServer.

Para definir las preguntas:

Procedimiento

1. Vaya a **Común** > **Autenticación** > **Inicio de sesión local** > **Autoayuda**.
2. Haga clic con el botón derecho en **Cantidad de preguntas** y seleccione **Propiedades**.
3. En el campo **Valor de política**, especifique la cantidad de preguntas que han de ser respondidas correctamente.
4. Haga clic en **Aplicar**.
5. Haga clic con el botón derecho en **Pregunta personal** y luego haga clic en **Agregar**.
6. Abra la política **Pregunta personal** que se muestra y especifique una pregunta en el campo **Valor de política**, seguidamente haga clic en **Aplicar**.



Nota

A cualquier usuario asignado al grupo en el que se crean las preguntas se le solicitará una respuesta para cada pregunta la primera vez que inicie sesión, después de la nueva configuración de la política.

Restablecimiento remoto de contraseña

Ayuda remota es un proceso que permite a un usuario que ha olvidado su contraseña hacer que ésta sea restablecida de un modo remoto. Para utilizar Ayuda remota, el usuario debe ser capaz de: (1) ponerse en contacto con el personal de asistencia técnica y (2) tener acceso a la opción Restablecimiento remoto de contraseña el menú de ayuda de KeyArmor.

Procedimiento

1. El usuario selecciona **Restablecimiento remoto de contraseña** en el menú **Ayuda**.
2. El usuario se pone en contacto con el Administrador de PolicyServer.
3. El usuario informa del **ID del dispositivo** a la persona de asistencia.
4. La persona de asistencia localiza el **ID del dispositivo** en la MMC de PolicyServer y hace clic con el botón derecho en el dispositivo para mostrar las opciones de menú y selecciona Símbolo de software.
5. El usuario lee la **Pregunta** al Administrador.
6. El Administrador introduce la pregunta en el campo **Pregunta**, hace clic en **Obtener respuesta** y lee la **Respuesta** al usuario.
7. El usuario escribe la respuesta en el campo **Respuesta** y seguidamente hace clic en **Iniciar sesión**.

   Se muestra una pantalla Cambiar la contraseña basada en el método de autenticación actual.
8. El usuario debe especificar y confirmar la nueva contraseña.

Información de asistencia

La pantalla Información de asistencia generalmente proporciona la información de contacto del servicio de asistencia técnica de la compañía.

Acerca de KeyArmor

La pantalla Acerca de KeyArmor se rellena automáticamente y proporciona la siguiente información:

- Versión de software
- Usuario
- Dirección de PolicyServer

- Empresa
- Nombre del dispositivo
- Última sincronización de políticas
- Versión de FIPS

Protección de archivos con KeyArmor

Proteger sus archivos es fácil con KeyArmor. Todo lo que tiene que hacer es copiar o arrastrar el archivo o documento seleccionado a la unidad KeyArmor Los archivos o carpetas guardadas en KeyArmor se cifran automáticamente y solo la persona que inicia sesión en el dispositivo con un nombre de usuario y contraseña válidos puede acceder a ellos.

- Todos los archivos y carpetas guardados en KeyArmor se cifran automáticamente.
- Los archivos permanecen cifrados mientras están almacenados en KeyArmor.

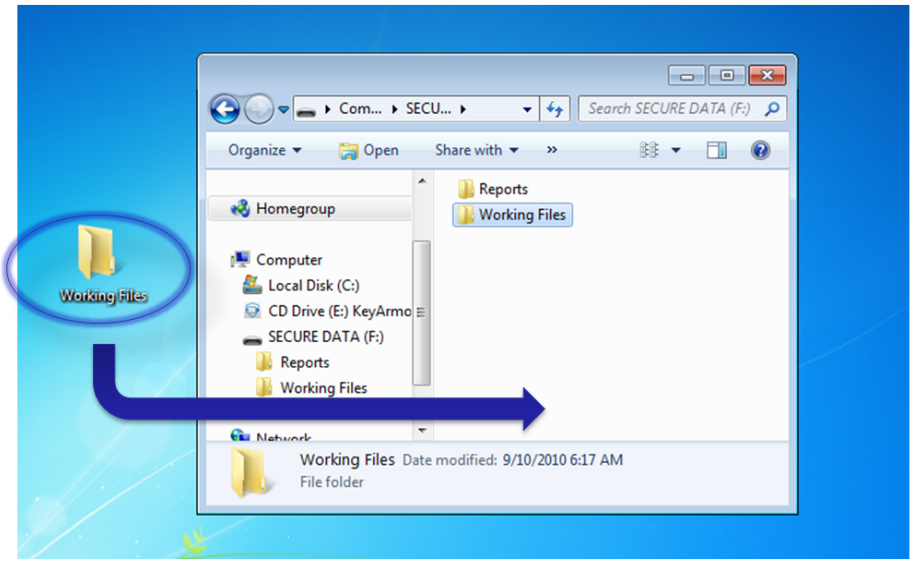


FIGURA 7-3. Copiar archivos en KeyArmor

Registro de actividad de KeyArmor

Toda la actividad de KeyArmor se registra y carga, de un modo transparente, en PolicyServer a través de la red. La MMC de PolicyServer suministra acceso a informes estándar y al registro detallado de actividad. Los administradores pueden filtrar por la actividad de un dispositivo concreto, un archivo y un usuario final. Para obtener información detallada acerca de las políticas de KeyArmor, consulte *Políticas de KeyArmor en la página 3-40*.

Extraer KeyArmor de forma segura

Al igual que con cualquier dispositivo de almacenamiento USB, realice una extracción segura del dispositivo KeyArmor antes de desconectarlo del puerto USB.

¡ADVERTENCIA!

Los datos podrían perderse o dañarse si el dispositivo KeyArmor se retira inadecuadamente de un equipo.

Seleccione una de las siguientes opciones para extraer de forma segura un dispositivo KeyArmor autenticado.

- Seleccione **Cerrar sesión** desde la interfaz de KeyArmor (en la ventana de la aplicación o haciendo clic con el botón derecho en la bandeja) para expulsar de un modo seguro el dispositivo.
- Haga clic con el botón derecho en el icono de la bandeja de KeyArmor y seleccione **Cerrar sesión**.

Después de cerrar sesión, KeyArmor ya no aparecerá en la aplicación Quitar hardware de forma segura de Windows y se puede desconectar el dispositivo del puerto USB con seguridad.

Para expulsar de un modo seguro un dispositivo KeyArmor autenticado, cierre el cuadro de diálogo de autenticación antes de enviar las credenciales.

Exploración completa de KeyArmor

Después de la autenticación, KeyArmor intenta actualizar las definiciones de antivirus. KeyArmor muestra avisos acerca de la actividad de actualización de antivirus. No desconecte ni retire un dispositivo KeyArmor de su PC host mientras está en curso la actualización de antivirus. A medida que los archivos se guardan o se copian en KeyArmor, se exploran en busca de virus.

Si se encuentra un virus, las políticas de PolicyServer controlan la acción resultante, incluido un intento de reparar el archivo, eliminarlo o borrar completamente el dispositivo KeyArmor. El cliente tiene también la posibilidad de iniciar una exploración completa de su dispositivo KeyArmor.

TABLA 7-3. Actividades antivirus de FileArmor

ACTIVIDAD	DESCRIPCIÓN
Actualizaciones de antivirus	Una vez cargadas las definiciones de antivirus, KeyArmor las actualiza tal y como se define en la política.
Actividad de exploración de archivos	Los archivos se exploran en busca de virus cuando se copian a KeyArmor. Los archivos con virus no se copian al dispositivo protegido.
Exploración completa de dispositivos	Se puede iniciar una exploración completa desde el icono de KeyArmor de la bandeja del sistema seleccionando **KeyArmor** > **Iniciar exploración completa**.

Cambiar la ubicación predeterminada de actualización de antivirus

Además de la fuente de actualización predeterminada, es posible establecer otra ubicación HTTP o FTP desde la que KeyArmor puede descargar actualizaciones para sus componentes antivirus.

Nota

- De forma predeterminada, la política de KeyArmor está configurada para obtener las actualizaciones automáticamente de la siguiente ubicación: FTP://download.trendmicro.com/products/pattern/
- Los administradores pueden optar por cambiar esta política para hacer que KeyArmor obtenga las actualizaciones de antivirus de otras ubicaciones host remotas o de una fuente local utilizando convenciones HTTP o FTP que se detallan a continuación.

Procedimiento

1. Para configurar una fuente HTTP:
   a. Desde el servidor FTP de Trend Micro, copie todos los archivos .zip que comiencen por los caracteres "LPT" y el archivo "`opr.ini`" a la ubicación host HTTP que haya seleccionado.
   b. Para hacer que los dispositivos KeyArmor descarguen las definiciones de antivirus desde su carpeta web HTTP, introduzca la URL completa de las

actualizaciones en el valor de la política **KeyArmor** > **Antivirus** > **Fuente de actualización**.

Por ejemplo, almacene estos archivos en su equipo PolicyServer colocándolos en la carpeta principal del servidor web: `c:\inetpub\wwwroot\mawebservice2\`

2. Para configurar una fuente FTP:

   a. Instale el servicio FTP de Microsoft IIS o cualquier otro software de servidor FTP y configure una carpeta FTP para que la usen los clientes de la red.

   b. Copie todos los archivos .zip que comiencen por "lpt" y el archivo `opr.ini` desde la ubicación para descargas de Trend Micro al directorio configurado en su servidor FTP (por ejemplo `c:\inetpub\ftpsvc\`).

   c. Para hacer que los dispositivos KeyArmor descarguen las definiciones de antivirus desde su carpeta web HTTP, especifique la URL completa en el valor de la política **KeyArmor** > **Antivirus** > **Fuente de actualización**.

Qué hacer a continuación

Trend Micro recomienda comprobar este cambio de configuración sincronizando las políticas en un dispositivo KeyArmor registrado y verificando que:

1. La actualización de antivirus se lleva a cabo con éxito.
2. Las definiciones de antivirus se actualizan en el dispositivo.
3. Se crean entradas en los registros de auditoría de PolicyServer mostrando la nueva URL definida en la política.

Reasignación de un dispositivo KeyArmor a otro usuario

KeyArmor se puede configurar para permitir que todos los usuarios de un grupo o un único usuario tengan acceso a un dispositivo. Para cambiar esta política, establezca **KeyArmor** > **Iniciar sesión** > **Permitir solo un usuario por dispositivo**. Cuando se establece en **Sí**, sólo un usuario podrá acceder al dispositivo en un momento determinado.

Nota

Esta política no afecta a las funciones de administrador o autenticador.

Procedimiento

1. Inicie sesión en la MMC de PolicyServer y vaya al grupo al que está asignado el dispositivo.
2. Quite el dispositivo haciendo clic en el botón derecho y seleccionando **Quitar dispositivo**.

Nota

- No elimine el ID del dispositivo KeyArmor de su empresa; si lo hace, no podrá administrar el dispositivo.
- Existen disposiciones de seguridad para prevenir que se vuelva a vincular KeyArmor a otra empresa una vez ha sido asignado a la suya.
- Esta misma lógica evita que pueda volver a añadir KeyArmor a su empresa si ha eliminado por error el ID del dispositivo de PolicyServer.

3. Inserte el dispositivo KeyArmor en un equipo y sincronice las políticas.
4. Vuelva a la consola MMC y agregue el dispositivo al grupo deseado.
5. Asegúrese de que el nuevo usuario es miembro del grupo deseado.
6. Asigne una contraseña fija al nuevo usuario.
7. Distribuya el dispositivo al nuevo usuario junto con su nombre de usuario y contraseña.
8. Ahora el dispositivo estará vinculado al nuevo individuo.



¡ADVERTENCIA!

El nuevo usuario podrá acceder a cualquier dato del usuario anterior que permanezca en el dispositivo. Los administradores deben seguir sus directrices internas para reformatear o reaprovisionar un dispositivo antes de asignar el KeyArmor a un nuevo usuario.

Añadir de nuevo un KeyArmor eliminado a la empresa

Si un dispositivo es eliminado por error, se puede volver a añadir a la empresa de dos maneras:

Procedimiento

1. **Automáticamente**. Si un usuario tiene sesión abierta en un dispositivo conectado a PolicyServer, el dispositivo se añadirá de nuevo a la empresa automáticamente en la siguiente sincronización del dispositivo.

   a. Un administrador de empresa tendrá que agregar manualmente el dispositivo al grupo adecuado para asegurar el acceso posterior del usuario al dispositivo.



Nota

- El procedimiento recomendado es bloquear o borrar un dispositivo antes de su eliminación.
- Un dispositivo eliminado de la empresa se bloqueará si las políticas requieren comunicación con PolicyServer.

2. **Manualmente**. Un administrador puede realizarlo del siguiente modo:



Nota

Se requiere conectividad al nuevo PolicyServer de empresa.

   a. Inicie sesión en el dispositivo con un ID de administrador y una contraseña válidos.

b. Haga clic con el botón derecho en el icono de KeyArmor en el menú de la bandeja y seleccione **Acerca de KeyArmor**.

c. Haga clic en **Editar** junto al nombre de la empresa.

d. Verifique que el nombre de la empresa es correcto.

e. Seleccione **Aceptar**.

f. Seleccione **Cerrar**.

g. Finalmente, el administrador de empresa tendrá que agregar de nuevo el dispositivo a un grupo para que los usuarios puedan acceder a él.

Capítulo 8

Trabajar con registros e informes

Endpoint Encryption guarda registros completos y genera informes sobre sucesos y actualizaciones. Use estos registros e informes para evaluar las políticas de su organización y para comprobar qué actualizaciones de componentes se llevaron a cabo correctamente.

En este capítulo se describen los siguientes temas:

- *Sucesos del registro en la página 8-2*
- *Informes en la página 8-6*

Sucesos del registro

PolicyServer registra los sucesos del registro usando criterios predefinidos que están integrados en el sistema como intentos de acceso, errores del sistema, modificaciones en usuarios o grupos, cambios de políticas y problemas de conformidad. Esta poderosa herramienta se puede usar para crear informes de todos los aspectos relacionados con la seguridad del servidor y los clientes. La administración de los sucesos del registro permite al administrador de un grupo o de una empresa seleccionar criterios específicos de búsqueda y, a continuación, mostrar la información en la pantalla.

Administración de sucesos del registro

De forma automática, solo se muestran los mensajes de los últimos 7 días. Use la función de filtro para ver mensajes más antiguos. Para buscar los registros, resulta útil usar el **ID del mensaje**. Por ejemplo, si busca el ID del mensaje 400008, aparecerán todos los mensajes "Cifrado del dispositivo completado". Consulte *ID de mensajes de PolicyServer en la página A-1* para obtener más información.

Procedimiento

1. Existen dos tipos de sucesos de eventos:

   - Para los registros de nivel de empresa, expanda **Sucesos del registro empresariales**.
   - Para los registros de nivel de grupo, vaya a **Nombre de grupo** > **Sucesos del registro**.

   Aparecerá la ventana del registro. De forma automática, se muestran todos los sucesos del registro de los últimos 7 días.

2. Haga doble clic en cualquier registro para ver los detalles.
3. Haga clic en **Filtrar** para buscar en el archivo de registro:

   a. Indique los criterios de búsqueda.

   b. Seleccione el intervalo de fechas.

   c. Haga clic en **Buscar**.

4. Haga clic en **Actualizar** para actualizar los datos del registro.
5. Haga clic en **Anterior** o en **Siguiente** para desplazarse por los datos del registro.

Alertas

Los administradores pueden personalizar los criterios de las alertas usando niveles de seguridad predefinidos para ayudar a clasificar las alertas. Para enviar sucesos del registro a una persona o a varios destinatarios de correo electrónico, puede definir alertas en la empresa o en el grupo.



Nota

Para obtener detalles sobre los ID de mensajes, consulte *ID de mensajes de PolicyServer en la página A-1*.

Configuración de las alertas de PolicyServer

Procedimiento

1. En MMC de PolicyServer, seleccione **Sucesos de registro empresariales (o de grupo)** de la pantalla de navegación del lado izquierdo.
2. Haga clic en **Alertas**.
3. Haga clic con el botón derecho y seleccione **Agregar**.

   Aparecerá la ventana Editar alerta.
4. Proporcione un **Nombre de alerta**.
5. Seleccione la gravedad de los registros que activan alertas.
6. Seleccione los ID de mensajes que activan alertas.
7. Proporcione una dirección de correo electrónico para recibir las alertas, una por línea.

8. Elija si desea enviar alertas en función del número de sucesos en un determinado período de tiempo.

9. Haga clic en **Finalizado**.

Activación de PolicyServer para transmitir SMS y Envío de correo electrónico

Esta función solo funciona en servidores PolicyServer que se ejecutan en Windows Server 2008 o Windows Server 2008 R2.

Procedimiento

1. Abra **Administrador del servidor**.

2. Vaya a **Características** > **Agregar características**.

3. Marque **Servidor SMTP**.

   Aparecerá la ventana **¿Desea agregar las características y los servicios de función requeridos para Servidor SMTP?**

4. Haga clic en **Agregar servicios de función requeridos**.

5. Haga clic en **Siguiente**, **Siguiente** y, a continuación, en **Instalar**.

   Se instala el servidor Web de IIS y el servidor SMTP

6. Haga clic en **Cerrar**.

7. Vaya a **Inicio** > **Herramientas administrativas** > **Administrador de Internet Information Services (IIS) 6.0**.

   Se abrirá el Administrador de IIS 6.0

8. Expanda **NombreServidor (dispositivo local)**.

9. Haga clic con el botón derecho **[Servidor virtual SMTP #1]** y haga clic en **Propiedades**.

Nota

Marque **Habilitar registro** para poder solucionar problemas en el futuro.

10. Vaya a **Acceso** > **Conexión...** y seleccione **Sólo la lista que aparece a continuación** y, a continuación haga clic en **Agregar...**.
11. Especifique `127.0.0.1` para **Dirección IP** y haga clic en **Aceptar**.

Nota

Repita estos pasos para especificar todas las direcciones IP en el servidor local

12. Haga clic en **Aceptar**.
13. Vaya a **Entrega** > **Avanzada...** y especifique el **Dominio de enmascaramiento** en el siguiente formato: **`psproxy.<suDominio>.<com/org>`**.
14. Haga clic en **Aceptar** dos veces para cerrar la ventana **Propiedades de Servidor virtual SMTP #1**.
15. Vaya a **Directivas de empresa** > **PolicyServer** > **PDA** > **Correo electrónico**.
16. Abra **Nombre del servidor SMTP**, especifique 127.0.0.1 y haga clic en **Aplicar**.

Definición de instalaciones avanzadas

Para obtener los mejores resultados, cree una entrada de DNS de marco de directivas de remitente (SPF). Para crear un registro de SPF en otros servidores DNS (BIND), consulte la documentación del proveedor.

Procedimiento

1. En un servidor DNS de Windows, abra la **Consola de administración de DNS**.
2. Haga clic con el botón derecho en la zona de búsqueda directa para el dominio y seleccione **Otros nuevos registros**.
3. Desplácese hacia abajo y seleccione **TEXTO (TXT)**.
4. Deje el **Nombre de registro** vacío y especifique:

```
v=spf1 ip4:<su IP de PolicyServer externa> -all
```

5. Haga clic en **Aceptar**.

Informes

PolicyServer registra las actividades del sistema (cambios realizados a las políticas, intentos correctos de autenticación, dispositivos bloqueados debido a demasiados intentos incorrectos de inicio de sesión) y mantiene dichos registros como sucesos de registro. Los administradores pueden generar informes de forma programada o a medida que los necesiten.

PolicyServer incluye una amplia variedad de informes que permiten comprobar el estado de cifrado de los dispositivos, la actividad de los usuarios y los dispositivos, y la integridad de PolicyServer.

Nota

Solo los administradores de empresa puede usar informes.

Opciones de informes

Los diferentes informes tienen distintas opciones. Haga clic con el botón derecho en un informe para ver las opciones que ofrece.

TABLA 8-1. Opciones para informes

OPCIÓN DEL INFORME	DESCRIPCIÓN DE LA OPCIÓN
Borrar	Borra toda la información que se muestra en la ventana de resultados; no elimina la información.
Mostrar error	Permite ver una descripción del error que impide que un informe sea válido; solo disponible para administradores.
Mostrar informe	Permite ver el informe; solo disponible para administradores.

Opción del informe	Descripción de la opción
Página siguiente	Se mueve a la siguiente página de los elementos de la búsqueda.
Página anterior	Regresa a la página anterior de los elementos de la búsqueda.
Actualizar	Actualiza el estado de un informe enviado.
Quitar informe	Elimina el informe.
Programar informe	Permite configurar un programa para que el informe se ejecute en una fecha o a una hora determinada.
Enviar informe	Genera el informe seleccionado.

Iconos de informes

Tabla 8-2. Iconos de informes

Icono	Descripción
	Los informes estándar se pueden enviar a medida que se necesiten para ver estadísticas y otras métricas de uso.
	Los informes de alertas se usan para notificar a los administradores posibles problemas de seguridad.

Tipos de informes

Los informes están diseñados para que la información que ofrecen sobre los registros sea fácilmente comprensible.

Ejecución de informes estándar

Los informes estándar se pueden enviar a medida que se necesiten. Las funciones de creación de informes solo están disponibles para los administradores de la empresa.

Procedimiento

1. Haga clic con el botón derecho en el informe que desee y seleccione **Enviar informe**.
2. Si es necesario, especifique los parámetros del informe y haga clic en **Aplicar**.
3. Para ver el informe, vaya a **Informes empresariales** > **Informes empresariales enviados**.

Informes estándar

TABLA 8-3. Lista de informes estándar

NOMBRE DEL INFORME	DESCRIPCIÓN
Estado de cifrado del dispositivo	Informa del estado de cifrado de todos los dispositivos de la empresa.
Recuento de sistemas operativos del dispositivo	Informa de todos los sistemas operativos de dispositivos y del recuento para cada uno.
Recuento de versiones del dispositivo	Informa de todas las versiones de Full Disk Encryption y del recuento para cada una.
Dispositivos por fecha de última sincronización	Informa de todos los dispositivos que se han sincronizado con PolicyServer en los últimos x días.
Los dispositivos no se están comunicando	Informa de los dispositivos que no se han comunicado en los últimos x días.
Dispositivos con el último usuario que ha iniciado sesión	Informa de todos los dispositivos y del último usuario que se ha autenticado en cada dispositivo.
Licencia de empresa disponible	Informa de los días que le quedan a la licencia, usuarios y dispositivos disponibles, y el recuento de usuarios y dispositivos usados.
Actividad del usuario empresarial	Informa de los usuarios y dispositivos totales, del recuento de usuarios de MMC y de la actividad de los dispositivos.

Nombre del informe	Descripción
Dispositivo Full Disk Encryption no cifrado al 100 %	Informa de todos los dispositivos que en los últimos x días han iniciado el cifrado pero aún no lo han completado.
Actividad del usuario por día	Informa de la actividad del usuario en un período de x días para el usuario determinado.
Usuarios agregados	Informa de todos los usuarios agregados en los últimos x días.
Usuarios que nunca han iniciado sesión en un dispositivo	Informa de todos los usuarios que nunca se han autenticado en ningún dispositivo.

Ejecución de informes de alertas

Las funciones de creación de informes solo están disponibles para los administradores de la empresa.

Para ver el informe, vaya a **Informes empresariales** > **Informes empresariales enviados**.

Procedimiento

1. Haga clic con el botón derecho en el informe de alertas que desee y seleccione **Configurar alertas**.

   Aparecerá la ventana **Configuraciones de alertas**.

2. Proporcione la **Dirección del servidor SMTP** y el **Remitente** que procesará el correo electrónico de salida.

3. Haga clic en **Aplicar**.

4. Haga clic con el botón derecho en el informe que desee y seleccione **Enviar alerta**.

Informes de alertas

TABLA 8-4. Lista de informes de alertas

NOMBRE DE LA ALERTA	DESCRIPCIÓN
Intentos consecutivos de inicio de sesión fallidos en un solo dispositivo	Cuando fallan varios intentos consecutivos de autenticación en un dispositivo individual, se envía una alerta.
Integridad del registro	Cuando hay un indicio de que se han alterado los registros de PolicyServer, se envía una alerta.
Alteración de políticas	Se envía una alerta cuando PolicyServer detecta que se han alterado las políticas.
Acción principal y secundaria aplicadas	Se envía una alerta después de que no haya conexión con PolicyServer, y se haya aplicado la acción principal o secundaria.

Mostrar informes

Las funciones de creación de informes solo están disponibles para los administradores de la empresa.

Procedimiento

1. Vaya a **Informes empresariales** > **Informes empresariales enviados**.
2. Haga clic con el botón derecho en el informe que desee y seleccione **Mostrar informe...**.

   Aparecerá el informe.

Nota

Para exportar el informe, haga clic en el icono **Guardar** y seleccione **Excel** o **Archivo PDF de Acrobat**.

Programación de informes

Estos pasos permiten ejecutar informes en una fecha y hora especificadas.

Procedimiento

1. Abra **Informes empresariales**.
2. Haga clic con el botón derecho en el informe que desee y seleccione **Programar informe**.

   Aparecerá la ventana **Parámetros de informe**.
3. Especifique los parámetros del informe y haga clic en **Aplicar**.

   Aparecerá el **Programador de informes**.
4. Especifique el intervalo, la fecha y la hora del informe, y haga clic en **Aplicar**.

   Para ver los informes programados:
5. Vaya a **Informes empresariales** > **Informes programados empresariales**.

Mostrar errores de los informes

Algunas veces un error impide que un informe se ejecute correctamente. Siga estos pasos para ver el error.

Procedimiento

1. Vaya a **Informes empresariales** > **Informes empresariales enviados**.
2. Haga clic con el botón derecho en el informe que presenta el error y seleccione **Mostrar error...**.

   Aparecerá el mensaje de error del informe.

Capítulo 9

Obtener asistencia

Según el tipo de asistencia que requiera, existen varios lugares donde obtener ayuda.

En este capítulo se describen los siguientes temas:

- *Comunidad de Trend en la página 9-2*
- *Portal de asistencia en la página 9-2*
- *Ponerse en contacto con el equipo de asistencia técnica en la página 9-3*
- *TrendLabs en la página 9-4*

Comunidad de Trend

Obtenga ayuda, comparta experiencias, formule preguntas y analice problemas de seguridad con otros colegas, entusiastas y expertos en seguridad.

http://community.trendmicro.com/

Portal de asistencia

El Portal de asistencia de Trend Micro es un recurso en línea disponible las 24 horas del día, 7 días a la semana que contiene infinidad de procedimientos de asistencia técnica sencillos y prácticos relativos a los productos y servicios de Trend Micro. Cada día se añaden nuevas soluciones.

Procedimiento

1. Vaya a http://esupport.trendmicro.com.
2. Seleccione un producto o servicio en el menú de lista desplegable correspondiente y especifique cualquier otra información relacionada, si se le pide.

   Se muestra la página de producto de Asistencia técnica.
3. Especifique los criterios de búsqueda, por ejemplo un mensaje de error y, a continuación, haga clic en el icono de búsqueda.

   Aparecerá una lista de soluciones.
4. Si no se puede encontrar la solución, envíe una incidencia y un ingeniero de asistencia de Trend Micro estudiará el problema. El tiempo de respuesta suele ser 24 horas o incluso menos.

   Envíe una incidencia de asistencia en línea a:

   http://esupport.trendmicro.com/srf/SRFMain.aspx

Ponerse en contacto con el equipo de asistencia técnica

Dispondrá del servicio de asistencia, descargas de patrones y actualizaciones de productos y servicios durante un año con todas las licencias de productos. Al cabo de un año, renueve la licencia para continuar recibiendo asistencia de Trend Micro.

Direcciones de correo y números de teléfono de todo el mundo

```
Si desea información de contacto de todo el mundo para la región Asia/Pac
http://www.trendmicro.es/acerca/contacto/index.html
```

- Obtenga una lista de las oficinas de asistencia técnica de todo el mundo en: http://www.trendmicro.com/us/about-us/contact/index.html
- Obtenga la documentación más reciente sobre Trend Micro en: http://docs.trendmicro.com/es-es/home.aspx

Resolver problemas de manera más rápida

Disponga de la siguiente información para acelerar el tiempo para solucionar un problema:

- Pasos para reproducir el problema
- Información del dispositivo o de la red
- Marca, modelo y cualquier hardware adicional del equipo conectado al punto final
- Memoria y espacio disponible en el disco duro
- Versión del sistema operativo y del Service Pack
- Versión del cliente de punto final
- Número de serie o código de activación
- Descripción detallada del entorno de instalación

- Texto exacto de cualquier mensaje de error recibido

TrendLabs

TrendLabs es una red mundial de investigación, desarrollo y centros de acción comprometida con la vigilancia de amenazas, la prevención de ataques y una entrega de soluciones oportunas y sencillas las 24 horas del día, los 7 días de la semana. Pieza fundamental en la infraestructura de servicios de Trend Micro, TrendLabs cuenta con un equipo de varios cientos de ingenieros y personal de asistencia técnica certificado que ofrecen una amplia gama de servicios de asistencia tanto técnica como de productos.

TrendLabs supervisa el panorama de amenazas en todo el mundo para ofrecer medidas de seguridad efectivas que permitan detectar, predecir y eliminar ataques. La culminación diaria de estos esfuerzos se hace llegar a los clientes por medio de constantes actualizaciones de archivos de patrones de virus y mejoras del motor de análisis.

Obtenga más información sobre TrendLabs en:

http://cloudsecurity.trendmicro.com/us/technology-innovation/experts/index.html#trendlabs

Apéndice A

ID de mensajes de PolicyServer

En este apéndice se enumeran los diferentes ID de mensajes y sus significados.

TABLA A-1. ID de mensajes de PolicyServer

CATEGORÍA	ID DEL MENSAJE	DESCRIPCIÓN	PRODUCTOS
Alertas de administrador	100002	Identificando dispositivo	Full Disk Encryption, FileArmor, DriveArmor, KeyArmor o PolicyServer
Alertas de administrador	100003	Infracción de seguridad	Full Disk Encryption, FileArmor, DriveArmor, KeyArmor o PolicyServer
Alertas de administrador	100007	Gravedad crítica	Full Disk Encryption, FileArmor, DriveArmor, KeyArmor o PolicyServer

Categoría	ID del mensaje	Descripción	Productos
Alertas de administrador	100019	La política no se ha cambiado correctamente	Full Disk Encryption, FileArmor, DriveArmor, KeyArmor o PolicyServer
Alertas de administrador	100045	Configuración no compatible	Full Disk Encryption, FileArmor, DriveArmor, KeyArmor o PolicyServer
Alertas de administrador	100046	Grupo de empresas creado	Full Disk Encryption, FileArmor, DriveArmor, KeyArmor o PolicyServer
Alertas de administrador	100047	Grupo de empresas eliminado	Full Disk Encryption, FileArmor, DriveArmor, KeyArmor o PolicyServer
Alertas de administrador	100048	Grupo de empresas modificado	Full Disk Encryption, FileArmor, DriveArmor, KeyArmor o PolicyServer
Alertas de administrador	100049	Se ha bloqueado al usuario con derechos de administrador debido a demasiados intentos de inicio de sesión incorrectos.	Full Disk Encryption, FileArmor, DriveArmor, KeyArmor o PolicyServer

Categoría	ID del mensaje	Descripción	Productos
Alertas de administrador	100052	Error en la comprobación de la integridad del valor de política	Full Disk Encryption, FileArmor, DriveArmor, KeyArmor o PolicyServer
Alertas de administrador	100053	Se ha interrumpido la solicitud de política debido a un error en la comprobación de integridad de la política.	Full Disk Encryption, FileArmor, DriveArmor, KeyArmor o PolicyServer
Alertas de administrador	100054	Se ha interrumpido la solicitud de archivo debido a un error en la comprobación de integridad de la política.	Full Disk Encryption, FileArmor, DriveArmor, KeyArmor o PolicyServer
Alertas de administrador	100055	Autenticación del administrador correcta	Full Disk Encryption, FileArmor, DriveArmor, KeyArmor o PolicyServer
Alertas de administrador	100056	Error en la autenticación del administrador	Full Disk Encryption, FileArmor, DriveArmor, KeyArmor o PolicyServer
Alertas de administrador	100062	Restablecer la contraseña del administrador	Full Disk Encryption, FileArmor, DriveArmor, KeyArmor o PolicyServer

Categoría	ID del mensaje	Descripción	Productos
Alertas de administrador	100463	No se puede eliminar el usuario. Inténtelo de nuevo.	Full Disk Encryption, FileArmor, DriveArmor, KeyArmor o PolicyServer
Alertas de administrador	100464	No se puede anular al usuario. Inténtelo de nuevo.	Full Disk Encryption, FileArmor, DriveArmor, KeyArmor o PolicyServer
Alertas de administrador	100470	No se puede cambiar la contraseña de autoayuda. La respuesta a una de las preguntas personales era incorrecta.	Full Disk Encryption, FileArmor, DriveArmor, KeyArmor o PolicyServer
Alertas de administrador	102000	Empresa agregada	Full Disk Encryption, FileArmor, DriveArmor, KeyArmor o PolicyServer
Alertas de administrador	102001	Empresa eliminada	Full Disk Encryption, FileArmor, DriveArmor, KeyArmor o PolicyServer
Alertas de administrador	102002	Empresa modificada	Full Disk Encryption, FileArmor, DriveArmor, KeyArmor o PolicyServer

Categoría	ID del mensaje	Descripción	Productos
Alertas de administrador	102003	El número de usuarios ha superado el máximo permitido por esta licencia. Reduzca el número de usuarios existentes para restaurar este dispositivo.	PolicyServer
Alertas de administrador	200000	Política actualizada por el administrador	PolicyServer
Alertas de administrador	200001	Política agregada por el administrador	PolicyServer
Alertas de administrador	200002	Política eliminada por el administrador	PolicyServer
Alertas de administrador	200003	Aplicación activada por el administrador	PolicyServer
Alertas de administrador	200004	Aplicación desactivada por el administrador	PolicyServer
Alertas de administrador	200100	Usuario agregado por el administrador	PolicyServer
Alertas de administrador	200101	Usuario eliminado por el administrador	PolicyServer
Alertas de administrador	200102	Usuario actualizado por el administrador	PolicyServer
Alertas de administrador	200103	Usuario agregado al grupo por el administrador	PolicyServer
Alertas de administrador	200104	Usuario eliminado del grupo por el administrador	PolicyServer

Categoría	ID del mensaje	Descripción	Productos
Alertas de administrador	200200	Usuario agregado	PolicyServer
Alertas de administrador	200201	Usuario eliminado	PolicyServer
Alertas de administrador	200202	Usuario agregado al grupo	PolicyServer
Alertas de administrador	200203	Usuario eliminado del grupo	PolicyServer
Alertas de administrador	200204	Usuario actualizado	PolicyServer
Alertas de administrador	200300	Dispositivo eliminado por el administrador	PolicyServer
Alertas de administrador	200301	Dispositivo agregado al grupo por el administrador	PolicyServer
Alertas de administrador	200302	Dispositivo eliminado del grupo por el administrador	PolicyServer
Alertas de administrador	200500	Grupo agregado por el administrador	PolicyServer
Alertas de administrador	200501	Grupo eliminado por el administrador	PolicyServer
Alertas de administrador	200502	Grupo actualizado por el administrador	PolicyServer
Alertas de administrador	200503	Grupo copiado y pegado por el administrador	PolicyServer
Alertas de administrador	200600	Actualización de PolicyServer aplicada.	PolicyServer

Categoría	ID del mensaje	Descripción	Productos
Alertas de administrador	200602	Usuario agregado al dispositivo	PolicyServer
Alertas de administrador	200603	Usuario eliminado del dispositivo	PolicyServer
Alertas de administrador	200700	Suceso ejecutado correctamente	PolicyServer
Alertas de administrador	200701	Error al ejecutar el suceso	PolicyServer
Alertas de administrador	200800	Suceso instalado correctamente	PolicyServer
Alertas de administrador	200801	Error al instalar el suceso	PolicyServer
Alertas de administrador	700012	El administrador ha iniciado sesión con una contraseña de un único uso	FileArmor SP6 o anterior
Alertas de administrador	700013	El administrador ha iniciado sesión con una contraseña fija	FileArmor SP6 o anterior
Alertas de administrador	700014	El administrador ha iniciado sesión con una tarjeta inteligente	FileArmor SP6 o anterior
Alertas de administrador	700017	El administrador ha iniciado sesión con autenticación remota	FileArmor SP6 o anterior
Alertas de administrador	700030	El administrador no ha podido iniciar sesión con una contraseña de un único uso	FileArmor SP6 o anterior

Categoría	ID del mensaje	Descripción	Productos
Alertas de administrador	700031	El administrador no ha podido iniciar sesión con una contraseña fija	FileArmor SP6 o anterior
Alertas de administrador	700032	El administrador no ha podido iniciar sesión con una tarjeta inteligente	FileArmor SP6 o anterior
Alertas de administrador	700035	El administrador no ha podido iniciar sesión con autenticación remota	FileArmor SP6 o anterior
Alertas de administrador	900100	El administrador ha iniciado sesión con una contraseña de un único uso.	KeyArmor
Alertas de administrador	900101	El administrador ha iniciado sesión con una contraseña fija.	KeyArmor
Alertas de administrador	900102	El administrador ha iniciado sesión con una tarjeta inteligente.	KeyArmor
Alertas de administrador	900103	El administrador ha iniciado sesión con autenticación de dominio.	KeyArmor
Alertas de administrador	900104	El administrador ha iniciado sesión con autenticación remota.	KeyArmor

Categoría	ID del mensaje	Descripción	Productos
Alertas de administrador	900105	El administrador ha iniciado sesión con autenticación por código de color.	KeyArmor
Alertas de administrador	900106	El administrador ha iniciado sesión con PIN.	KeyArmor
Alertas de administrador	900107	El administrador ha iniciado sesión con OCSP.	KeyArmor
Alertas de administrador	900250	El administrador no ha podido iniciar sesión con una contraseña de un único uso	KeyArmor
Alertas de administrador	900251	El administrador no ha podido iniciar sesión con una contraseña fija	KeyArmor
Alertas de administrador	900252	El administrador no ha podido iniciar sesión con una tarjeta inteligente	KeyArmor
Alertas de administrador	900253	El administrador no ha podido iniciar sesión con autenticación de dominio.	KeyArmor
Alertas de administrador	900254	El administrador no ha podido iniciar sesión con autenticación remota	KeyArmor

Categoría	ID del mensaje	Descripción	Productos
Alertas de administrador	900255	El administrador no ha podido iniciar sesión con autenticación por código de color.	KeyArmor
Alertas de administrador	900256	El administrador no ha podido iniciar sesión con PIN.	KeyArmor
Alertas de administrador	900257	El administrador no ha podido iniciar sesión con OCSP	KeyArmor
Alertas de administrador	900300	El administrador no ha podido iniciar sesión con autenticación remota	KeyArmor
Alertas de administrador	901000	El administrador ha cambiado el nombre de un archivo	KeyArmor
Alertas de administrador	901001	El administrador ha cambiado un archivo	KeyArmor
Alertas de administrador	901002	El administrador ha eliminado un archivo	KeyArmor
Alertas de administrador	901003	El administrador ha creado un archivo	KeyArmor
Alertas de registro de auditoría	100015	Mensaje de registro	Full Disk Encryption, FileArmor, DriveArmor, KeyArmor o PolicyServer

Categoría	ID del mensaje	Descripción	Productos
Alertas de registro de auditoría	103000	Conexión de registro de auditoría abierta	Full Disk Encryption, FileArmor, DriveArmor, KeyArmor o PolicyServer
Alertas de registro de auditoría	103001	Conexión de registro de auditoría cerrada	Full Disk Encryption, FileArmor, DriveArmor, KeyArmor o PolicyServer
Alertas de registro de auditoría	103100	Falta la entrada del registro de auditoría	Full Disk Encryption, FileArmor, DriveArmor, KeyArmor o PolicyServer
Alertas de registro de auditoría	103101	Falta la integridad de la entrada del registro de auditoría	Full Disk Encryption, FileArmor, DriveArmor, KeyArmor o PolicyServer
Alertas de registro de auditoría	103102	Integridad de la entrada del registro de auditoría comprometida	Full Disk Encryption, FileArmor, DriveArmor, KeyArmor o PolicyServer
Alertas de registro de auditoría	103103	Validación de la integridad de la entrada del registro de auditoría iniciada	Full Disk Encryption, FileArmor, DriveArmor, KeyArmor o PolicyServer
Alertas de registro de auditoría	104003	Método de autenticación definido en tarjeta inteligente.	Full Disk Encryption, FileArmor, DriveArmor, KeyArmor o PolicyServer

Categoría	ID del mensaje	Descripción	Productos
Alertas de registro de auditoría	904008	No se puede enviar alerta de registro	Full Disk Encryption, FileArmor, DriveArmor, KeyArmor o PolicyServer
Alertas de autenticador	700006	El autenticador ha iniciado sesión con una contraseña de un único uso	FileArmor SP6 o anterior
Alertas de autenticador	700007	El autenticador ha iniciado sesión con una contraseña fija	FileArmor SP6 o anterior
Alertas de autenticador	700008	El autenticador ha iniciado sesión con una tarjeta inteligente	FileArmor SP6 o anterior
Alertas de autenticador	700009	El autenticador ha iniciado sesión con credenciales de Windows	FileArmor SP6 o anterior
Alertas de autenticador	700011	El autenticador ha iniciado sesión con autenticación remota	FileArmor SP6 o anterior
Alertas de autenticador	700024	El autenticador no ha podido iniciar sesión con una contraseña de un único uso	FileArmor SP6 o anterior
Alertas de autenticador	700025	El autenticador no ha podido iniciar sesión con una contraseña fija	FileArmor SP6 o anterior

Categoría	ID del mensaje	Descripción	Productos
Alertas de autenticador	700026	El autenticador no ha podido iniciar sesión con una tarjeta inteligente	FileArmor SP6 o anterior
Alertas de autenticador	700027	El autenticador no ha podido iniciar sesión con credenciales de Windows	FileArmor SP6 o anterior
Alertas de autenticador	700029	El autenticador no ha podido iniciar sesión con autenticación remota	FileArmor SP6 o anterior
Alertas de autenticador	900050	El autenticador ha iniciado sesión con una contraseña de un único uso.	KeyArmor
Alertas de autenticador	900051	El autenticador ha iniciado sesión con una contraseña fija.	KeyArmor
Alertas de autenticador	900052	El autenticador ha iniciado sesión con una tarjeta inteligente.	KeyArmor
Alertas de autenticador	900053	El autenticador ha iniciado sesión con autenticación de dominio.	KeyArmor
Alertas de autenticador	900054	El autenticador ha iniciado sesión con autenticación remota.	KeyArmor

Categoría	ID del mensaje	Descripción	Productos
Alertas de autenticador	900055	El autenticador ha iniciado sesión con autenticación por código de color.	KeyArmor
Alertas de autenticador	900056	El autenticador ha iniciado sesión con PIN.	KeyArmor
Alertas de autenticador	900057	El autenticador ha iniciado sesión con OCSP.	KeyArmor
Alertas de autenticador	900161	El usuario no ha podido iniciar sesión con autoayuda	KeyArmor
Alertas de autenticador	900200	El autenticador no ha podido iniciar sesión con una contraseña de un único uso	KeyArmor
Alertas de autenticador	900201	El autenticador no ha podido iniciar sesión con una contraseña fija	KeyArmor
Alertas de autenticador	900202	El autenticador no ha podido iniciar sesión con una tarjeta inteligente	KeyArmor
Alertas de autenticador	900203	El autenticador no ha podido iniciar sesión con autenticación de dominio.	KeyArmor

Categoría	ID del mensaje	Descripción	Productos
Alertas de autenticador	900204	El autenticador no ha podido iniciar sesión con autenticación remota	KeyArmor
Alertas de autenticador	900205	El autenticador no ha podido iniciar sesión con autenticación por código de color.	KeyArmor
Alertas de autenticador	900206	El autenticador no ha podido iniciar sesión con PIN.	KeyArmor
Alertas de autenticador	900207	El autenticador no ha podido iniciar sesión con OCSP	KeyArmor
Alertas de autenticador	902000	El autenticador ha cambiado el nombre de un archivo	KeyArmor
Alertas de autenticador	902001	El autenticador ha cambiado un archivo	KeyArmor
Alertas de autenticador	902002	El autenticador ha eliminado un archivo	KeyArmor
Alertas de autenticador	902003	El autenticador ha creado un archivo	KeyArmor
Alertas de certificado	104008	Certificado caducado.	Full Disk Encryption, FileArmor, DriveArmor, KeyArmor o PolicyServer

Categoría	ID del mensaje	Descripción	Productos
Alertas de dispositivo	100001	La autenticación de sincronización del dispositivo PDA al escritorio no se realizó correctamente. No se encontró ningún ID de dispositivo para este dispositivo PDA.	Full Disk Encryption, FileArmor, DriveArmor, KeyArmor o PolicyServer
Alertas de dispositivo	100012	El dispositivo no se encuentra en su propio archivo de autenticación de contraseña. ¿Está dañado el archivo de autenticación de contraseña?	Full Disk Encryption, FileArmor, DriveArmor, KeyArmor o PolicyServer
Alertas de dispositivo	100044	Acción de bloqueo de dispositivo recibida	Full Disk Encryption, FileArmor, DriveArmor, KeyArmor o PolicyServer
Alertas de dispositivo	100071	Eliminación del dispositivo confirmada	KeyArmor
Alertas de dispositivo	100072	Bloqueo del dispositivo confirmado	KeyArmor
Alertas de dispositivo	100100	Instalación iniciada	Full Disk Encryption, FileArmor, DriveArmor, KeyArmor

Categoría	ID del mensaje	Descripción	Productos
Alertas de dispositivo	100101	Instalación completada	Full Disk Encryption, FileArmor, DriveArmor, KeyArmor
Alertas de dispositivo	100462	No se puede conectar a PolicyServer.	Full Disk Encryption, FileArmor, DriveArmor, KeyArmor o PolicyServer
Alertas de dispositivo	101001	La conexión de red no funciona. No se pueden obtener archivos de política de PolicyServer.	Full Disk Encryption, FileArmor, DriveArmor, KeyArmor o PolicyServer
Alertas de dispositivo	101002	Archivo de autenticación de contraseña (DAFolder.xml) dañado	Full Disk Encryption, FileArmor, DriveArmor, KeyArmor o PolicyServer
Alertas de dispositivo	105000	No se pueden sincronizar políticas con el cliente. Compruebe que haya conexión de red e inténtelo de nuevo.	Full Disk Encryption, FileArmor, DriveArmor, KeyArmor o PolicyServer
Alertas de dispositivo	200400	Dispositivo agregado	PolicyServer
Alertas de dispositivo	200401	Dispositivo eliminado	PolicyServer
Alertas de dispositivo	200402	Dispositivo agregado al grupo	PolicyServer
Alertas de dispositivo	200403	Dispositivo eliminado del grupo	PolicyServer

Categoría	ID del mensaje	Descripción	Productos
Alertas de dispositivo	200404	Dispositivo modificado	PolicyServer
Alertas de dispositivo	200405	Estado del dispositivo actualizado	PolicyServer
Alertas de dispositivo	200406	Estado del dispositivo restablecido	PolicyServer
Alertas de dispositivo	200407	Eliminación del dispositivo emitida	Full Disk Encryption, FileArmor, DriveArmor, KeyArmor o PolicyServer
Alertas de dispositivo	200408	Bloqueo del dispositivo emitido	Full Disk Encryption, FileArmor, DriveArmor, KeyArmor o PolicyServer
Alertas de dispositivo	200409	Dispositivo sincronizado	PolicyServer
Alertas de dispositivo	904012	El usuario no puede registrar el nuevo dispositivo	PolicyServer
Alertas de dispositivo	1000052	Desinstalación del producto	Full Disk Encryption, FileArmor, DriveArmor, KeyArmor
Alertas de dispositivo	1000053	Desinstalación del producto denegada por política	Full Disk Encryption, FileArmor, DriveArmor, KeyArmor

Categoría	ID del mensaje	Descripción	Productos
Alertas de error	100005	Error general	Full Disk Encryption, FileArmor, DriveArmor, KeyArmor o PolicyServer
Alertas de error	100006	Error de la aplicación	Full Disk Encryption, FileArmor, DriveArmor, KeyArmor o PolicyServer
Alertas de actividad de FileArmor	700000	El usuario ha iniciado sesión con una contraseña de un único uso	FileArmor SP6 o anterior
Alertas de actividad de FileArmor	700001	El usuario ha iniciado sesión con una contraseña fija	FileArmor SP6 o anterior
Alertas de actividad de FileArmor	700002	El usuario ha iniciado sesión con una tarjeta inteligente	FileArmor SP6 o anterior
Alertas de actividad de FileArmor	700003	El usuario ha iniciado sesión con credenciales de Windows	FileArmor SP6 o anterior
Alertas de actividad de FileArmor	700005	El usuario ha iniciado sesión con autenticación remota	FileArmor SP6 o anterior
Alertas de actividad de FileArmor	700015	El administrador ha iniciado sesión con credenciales de Windows	FileArmor SP6 o anterior

Categoría	ID del mensaje	Descripción	Productos
Alertas de actividad de FileArmor	700018	El usuario no ha podido iniciar sesión con una contraseña de un único uso	FileArmor SP6 o anterior
Alertas de actividad de FileArmor	700019	El usuario no ha podido iniciar sesión con una contraseña fija	FileArmor SP6 o anterior
Alertas de actividad de FileArmor	700020	El usuario no ha podido iniciar sesión con una tarjeta inteligente	FileArmor SP6 o anterior
Alertas de actividad de FileArmor	700021	El usuario no ha podido iniciar sesión con credenciales de Windows	FileArmor SP6 o anterior
Alertas de actividad de FileArmor	700023	El usuario no ha podido iniciar sesión con autenticación remota	FileArmor SP6 o anterior
Alertas de actividad de FileArmor	700033	El administrador no ha podido iniciar sesión con credenciales de Windows	FileArmor SP6 o anterior
Alertas de actividad de FileArmor	700036	Se ha superado el número de intentos de inicio de sesión fallidos	FileArmor SP6 o anterior
Alertas de actividad de FileArmor	701000	Archivo cifrado con clave de usuario	FileArmor SP6 o anterior
Alertas de actividad de FileArmor	701001	Archivo cifrado con clave de grupo	FileArmor SP6 o anterior

Categoría	ID del mensaje	Descripción	Productos
Alertas de actividad de FileArmor	701002	Archivo cifrado con contraseña estática	FileArmor SP6 o anterior
Alertas de actividad de FileArmor	701003	Archivo cifrado autoextraíble creado con una contraseña estática.	FileArmor SP6 o anterior
Alertas de actividad de FileArmor	701004	Archivo cifrado con certificado	FileArmor SP6 o anterior
Alertas de actividad de FileArmor	701005	Archivo cifrado autoextraíble creado con un certificado.	FileArmor SP6 o anterior
Alertas de actividad de FileArmor	701006	Archivo cifrado con grabación de CD/DVD	FileArmor SP6 o anterior
Alertas de actividad de FileArmor	701007	Directorio cifrado con clave de grupo	FileArmor SP6 o anterior
Alertas de actividad de FileArmor	701008	Directorio cifrado con contraseña estática	FileArmor SP6 o anterior
Alertas de actividad de FileArmor	701009	Directorio cifrado autoextraíble creado con una contraseña estática.	FileArmor SP6 o anterior
Alertas de actividad de FileArmor	701010	Directorio cifrado con certificado	FileArmor SP6 o anterior
Alertas de actividad de FileArmor	701011	Directorio cifrado autoextraíble creado con un certificado.	FileArmor SP6 o anterior
Alertas de actividad de FileArmor	701012	Directorio cifrado con grabación de CD/DVD	FileArmor SP6 o anterior

Categoría	ID del mensaje	Descripción	Productos
Alertas de actividad de FileArmor	701015	El soporte extraíble se ha cifrado completamente	FileArmor SP6 o anterior
Alertas de actividad de FileArmor	701016	Soporte extraíble bloqueado	FileArmor SP6 o anterior
Alertas de actividad de FileArmor	701017	El soporte extraíble ha creado y cubierto carpetas	FileArmor SP6 o anterior
Alertas de actividad de FileArmor	701018	Archivo cifrado y movido al soporte extraíble.	FileArmor SP6 o anterior
Alertas de actividad de FileArmor	701019	Archivo eliminado del soporte extraíble.	FileArmor SP6 o anterior
Alertas de actividad de FileArmor	703000	Se ha creado una carpeta cifrada de FileArmor	FileArmor SP6 o anterior
Alertas de actividad de FileArmor	703001	La carpeta se ha creado y cubierto	FileArmor SP6 o anterior
Alertas de actividad de FileArmor	703002	Se ha eliminado una carpeta cifrada de FileArmor	FileArmor SP6 o anterior
Alertas de actividad de FileArmor	703004	Se ha creado y cubierto la carpeta del soporte extraíble	FileArmor SP6 o anterior
Alertas de actividad de FileArmor	703005	El dispositivo de soporte extraíble se cifró completamente	FileArmor SP6 o anterior
Alertas de actividad de FileArmor	703006	Se creó el archivo en carpeta	FileArmor SP6 o anterior
Alertas de actividad de FileArmor	703007	Se eliminó el archivo en carpeta	FileArmor SP6 o anterior

Categoría	ID del mensaje	Descripción	Productos
Alertas de actividad de FileArmor	703008	Se cambió el archivo en carpeta	FileArmor SP6 o anterior
Alertas de actividad de FileArmor	703009	Se accedió al archivo en carpeta	FileArmor SP6 o anterior
Alertas de actividad de FileArmor	703010	Se escribió por última vez en el archivo en carpeta	FileArmor SP6 o anterior
Alertas de actividad de FileArmor	703011	Se cambió el tamaño del archivo en carpeta	FileArmor SP6 o anterior
Alertas de actividad de FileArmor	703015	Cifrado de carpeta iniciado	FileArmor SP6 o anterior
Alertas de actividad de FileArmor	703016	Descifrado de carpeta iniciado	FileArmor SP6 o anterior
Alertas de actividad de FileArmor	703017	Cifrado de carpeta completado	FileArmor SP6 o anterior
Alertas de actividad de FileArmor	703018	Descifrado de carpeta completado	FileArmor SP6 o anterior
Alertas de actividad de FileArmor	703019	Descifrado de carpeta en curso	FileArmor SP6 o anterior
Alertas de actividad de FileArmor	703020	Cifrado de carpeta en curso	FileArmor SP6 o anterior
Alertas de actividad de FileArmor	704000	Servicio de FileArmor iniciado	FileArmor SP6 o anterior
Alertas de actividad de FileArmor	704001	Cierre del servicio de FileArmor	FileArmor SP6 o anterior
Alertas de actividad de Full Disk Encryption	300700	Se ha alcanzado el límite de tamaño máximo del registro; se ha truncado el registro de sucesos.	Full Disk Encryption o MobileSentinel

Categoría	ID del mensaje	Descripción	Productos
Alertas de actividad de Full Disk Encryption	400001	El usuario ha iniciado sesión correctamente.	Full Disk Encryption o MobileSentinel
Alertas de actividad de Full Disk Encryption	400002	Error en el inicio de sesión del usuario.	Full Disk Encryption o MobileSentinel
Alertas de actividad de Full Disk Encryption	400003	Descifrado del dispositivo iniciado.	Full Disk Encryption o MobileSentinel
Alertas de actividad de Full Disk Encryption	400004	Cifrado del dispositivo iniciado.	Full Disk Encryption o MobileSentinel
Alertas de actividad de Full Disk Encryption	400005	Partición de cifrado montada.	Full Disk Encryption o MobileSentinel
Alertas de actividad de Full Disk Encryption	400006	MBR del sistema operativo nativo restaurado.	Full Disk Encryption o MobileSentinel
Alertas de actividad de Full Disk Encryption	400007	MBR de la aplicación restaurado.	Full Disk Encryption o MobileSentinel
Alertas de actividad de Full Disk Encryption	400008	Cifrado del dispositivo completado	Full Disk Encryption o MobileSentinel
Alertas de actividad de Full Disk Encryption	400009	Descifrado del dispositivo completado	Full Disk Encryption o MobileSentinel
Alertas de actividad de Full Disk Encryption	400010	Cifrado del dispositivo en curso	Full Disk Encryption o MobileSentinel
Alertas de actividad de Full Disk Encryption	400011	MBR del sistema dañado	Full Disk Encryption o MobileSentinel
Alertas de actividad de Full Disk Encryption	400012	Kernel de arranque previo del sistema eliminado	Full Disk Encryption o MobileSentinel

Categoría	ID del mensaje	Descripción	Productos
Alertas de actividad de Full Disk Encryption	401000	Se ha accedido a la consola de recuperación	Full Disk Encryption o MobileSentinel
Alertas de actividad de Full Disk Encryption	401009	Error en la consola de recuperación	Full Disk Encryption o MobileSentinel
Alertas de actividad de Full Disk Encryption	401010	Descifrado en vigor iniciado	Full Disk Encryption o MobileSentinel
Alertas de actividad de Full Disk Encryption	401011	Descifrado en vigor detenido	Full Disk Encryption o MobileSentinel
Alertas de actividad de Full Disk Encryption	401012	Descifrado en vigor completado	Full Disk Encryption o MobileSentinel
Alertas de actividad de Full Disk Encryption	401013	Descifrado del dispositivo extraíble iniciado	Full Disk Encryption o MobileSentinel
Alertas de actividad de Full Disk Encryption	401014	Descifrado del dispositivo extraíble detenido	Full Disk Encryption o MobileSentinel
Alertas de actividad de Full Disk Encryption	401015	Descifrado del dispositivo extraíble completado	Full Disk Encryption o MobileSentinel
Alertas de actividad de Full Disk Encryption	401018	Error de descifrado en vigor	Full Disk Encryption o MobileSentinel
Alertas de actividad de Full Disk Encryption	401019	Error de descifrado del dispositivo extraíble	Full Disk Encryption o MobileSentinel
Alertas de actividad de Full Disk Encryption	401020	Se ha accedido a los archivos cifrados	Full Disk Encryption o MobileSentinel
Alertas de actividad de Full Disk Encryption	401021	Se han modificado los archivos cifrados	Full Disk Encryption o MobileSentinel

Categoría	ID del mensaje	Descripción	Productos
Alertas de actividad de Full Disk Encryption	401022	Se han copiado los archivos cifrados en el dispositivo extraíble	Full Disk Encryption o MobileSentinel
Alertas de actividad de Full Disk Encryption	401029	Error de acceso a archivos cifrados	Full Disk Encryption o MobileSentinel
Alertas de actividad de Full Disk Encryption	401030	Se ha accedido a la administración de red	Full Disk Encryption o MobileSentinel
Alertas de actividad de Full Disk Encryption	401031	Se ha cambiado la dirección de PolicyServer	Full Disk Encryption o MobileSentinel
Alertas de actividad de Full Disk Encryption	401032	Se ha cambiado el número de puerto de PolicyServer	Full Disk Encryption o MobileSentinel
Alertas de actividad de Full Disk Encryption	401033	Se ha cambiado a IPv6	Full Disk Encryption o MobileSentinel
Alertas de actividad de Full Disk Encryption	401034	Se ha cambiado a IPv4	Full Disk Encryption o MobileSentinel
Alertas de actividad de Full Disk Encryption	401035	Se ha cambiado a la configuración de IP dinámica	Full Disk Encryption o MobileSentinel
Alertas de actividad de Full Disk Encryption	401036	Se ha cambiado a la configuración de IP estática	Full Disk Encryption o MobileSentinel
Alertas de actividad de Full Disk Encryption	401037	Se ha cambiado el número de puerto de DHCP	Full Disk Encryption o MobileSentinel
Alertas de actividad de Full Disk Encryption	401038	Se ha cambiado la dirección IP	Full Disk Encryption o MobileSentinel
Alertas de actividad de Full Disk Encryption	401039	Se ha cambiado la máscara de red	Full Disk Encryption o MobileSentinel

Categoría	ID del mensaje	Descripción	Productos
Alertas de actividad de Full Disk Encryption	401040	Se ha cambiado la dirección de transmisiones	Full Disk Encryption o MobileSentinel
Alertas de actividad de Full Disk Encryption	401041	Gateway cambiado	Full Disk Encryption o MobileSentinel
Alertas de actividad de Full Disk Encryption	401042	Nombre de dominio cambiado	Full Disk Encryption o MobileSentinel
Alertas de actividad de Full Disk Encryption	401043	Servidores de nombre de dominio cambiados	Full Disk Encryption o MobileSentinel
Alertas de actividad de Full Disk Encryption	401049	Error de administración de red	Full Disk Encryption o MobileSentinel
Alertas de actividad de Full Disk Encryption	401050	Se ha accedido a la administración de usuario	Full Disk Encryption o MobileSentinel
Alertas de actividad de Full Disk Encryption	401051	Usuario agregado	Full Disk Encryption o MobileSentinel
Alertas de actividad de Full Disk Encryption	401052	Usuario eliminado	Full Disk Encryption o MobileSentinel
Alertas de actividad de Full Disk Encryption	401053	Usuario modificado	Full Disk Encryption o MobileSentinel
Alertas de actividad de Full Disk Encryption	401069	Error de administración de usuario	Full Disk Encryption o MobileSentinel
Alertas de actividad de Full Disk Encryption	401070	Se ha accedido a los registros almacenados a nivel local	Full Disk Encryption o MobileSentinel

Categoría	ID del mensaje	Descripción	Productos
Alertas de actividad de Full Disk Encryption	401079	Error al acceder a los registros almacenados a nivel local	Full Disk Encryption o MobileSentinel
Alertas de actividad de Full Disk Encryption	401080	MBR original restaurado	Full Disk Encryption o MobileSentinel
Alertas de actividad de Full Disk Encryption	401089	Error de restauración del MBR original	Full Disk Encryption o MobileSentinel
Alertas de actividad de Full Disk Encryption	401090	Tema predeterminado restaurado	Full Disk Encryption o MobileSentinel
Alertas de actividad de Full Disk Encryption	401099	Error al restaurar el tema predeterminado	Full Disk Encryption o MobileSentinel
Alertas de actividad de Full Disk Encryption	402000	Inicio de aplicación	Full Disk Encryption o MobileSentinel
Alertas de actividad de Full Disk Encryption	402001	Cierre de aplicación	Full Disk Encryption o MobileSentinel
Alertas de actividad de Full Disk Encryption	600001	La actualización se realizó correctamente en el arranque previo.	Full Disk Encryption
Alertas de actividad de Full Disk Encryption	600002	Error en la actualización de arranque previo	Full Disk Encryption
Alertas de instalación	100004	Error de instalación	Full Disk Encryption, FileArmor, DriveArmor, KeyArmor o PolicyServer

Categoría	ID del mensaje	Descripción	Productos
Alertas de instalación	100020	Instalación correcta	Full Disk Encryption, FileArmor, DriveArmor, KeyArmor o PolicyServer
Alertas de instalación	700037	FileArmor se ha instalado correctamente	FileArmor SP6 o anterior
Alertas de instalación	700038	Se ha producido un error durante la instalación de FileArmor: el nombre de empresa no es válido.	FileArmor SP6 o anterior
Alertas de instalación	700039	Se ha producido un error durante la instalación de FileArmor: el nombre de usuario o la contraseña no son correctos.	FileArmor SP6 o anterior
Alertas de actividad de KeyArmor	100034	Valor de registro no válido detectado	Full Disk Encryption, FileArmor, DriveArmor, KeyArmor o PolicyServer
Alertas de actividad de KeyArmor	500000	VirusDefense	KeyArmor
Alertas de actividad de KeyArmor	500001	Objeto limpiado	KeyArmor
Alertas de actividad de KeyArmor	500002	Objeto desinfectado	KeyArmor
Alertas de actividad de KeyArmor	500003	Objeto en cuarentena	KeyArmor

Categoría	ID del mensaje	Descripción	Productos
Alertas de actividad de KeyArmor	500004	Objeto eliminado	KeyArmor
Alertas de actividad de KeyArmor	500005	Virus detectados	KeyArmor
Alertas de actividad de KeyArmor	500006	Exploración completa iniciada	KeyArmor
Alertas de actividad de KeyArmor	500007	Exploración completa completada	KeyArmor
Alertas de actividad de KeyArmor	500008	Objeto sospechoso	KeyArmor
Alertas de actividad de KeyArmor	500009	Exploración de objeto completada	KeyArmor
Alertas de actividad de KeyArmor	500010	Exploración de soportes extraíbles solicitada	KeyArmor
Alertas de actividad de KeyArmor	500011	Exploración de soportes extraíbles completada	KeyArmor
Alertas de actividad de KeyArmor	500012	Exploración de carpeta solicitada	KeyArmor
Alertas de actividad de KeyArmor	500013	Exploración de carpeta completada	KeyArmor
Alertas de actividad de KeyArmor	500014	Acceso denegado al objeto	KeyArmor
Alertas de actividad de KeyArmor	500015	Objeto dañado	KeyArmor
Alertas de actividad de KeyArmor	500016	Objeto limpio	KeyArmor

Categoría	ID del mensaje	Descripción	Productos
Alertas de actividad de KeyArmor	500017	Exploración completa cancelada	KeyArmor
Alertas de actividad de KeyArmor	500018	Exploración de objeto cancelada	KeyArmor
Alertas de actividad de KeyArmor	500019	Exploración de soportes extraíbles cancelada	KeyArmor
Alertas de actividad de KeyArmor	500020	Exploración de carpeta cancelada	KeyArmor
Alertas de actividad de KeyArmor	500021	Actualización iniciada	KeyArmor
Alertas de actividad de KeyArmor	500022	La actualización ha fallado. Inténtelo de nuevo.	KeyArmor
Alertas de actividad de KeyArmor	500023	Actualización cancelada	KeyArmor
Alertas de actividad de KeyArmor	500024	Actualización finalizada correctamente.	KeyArmor
Alertas de actividad de KeyArmor	500025	VirusDefense actualizado	KeyArmor
Alertas de actividad de KeyArmor	500026	PalmVirusDefense	KeyArmor
Alertas de actividad de KeyArmor	500027	Exploración de objeto solicitada	KeyArmor
Alertas de actividad de KeyArmor	500028	PPCVirusDefense	KeyArmor
Alertas de actividad de KeyArmor	900000	El usuario ha iniciado sesión con una contraseña de un único uso.	KeyArmor

Categoría	ID del mensaje	Descripción	Productos
Alertas de actividad de KeyArmor	900001	El usuario ha iniciado sesión con una contraseña fija.	KeyArmor
Alertas de actividad de KeyArmor	900002	El usuario ha iniciado sesión con una tarjeta inteligente.	KeyArmor
Alertas de actividad de KeyArmor	900003	El usuario ha iniciado sesión con autenticación de dominio.	KeyArmor
Alertas de actividad de KeyArmor	900004	El usuario ha iniciado sesión con autenticación remota.	KeyArmor
Alertas de actividad de KeyArmor	900005	El usuario ha iniciado sesión con autenticación por código de color.	KeyArmor
Alertas de actividad de KeyArmor	900006	El usuario ha iniciado sesión con PIN.	KeyArmor
Alertas de actividad de KeyArmor	900007	El usuario ha iniciado sesión con OCSP.	KeyArmor
Alertas de actividad de KeyArmor	900008	El usuario ha iniciado sesión con autoayuda.	KeyArmor
Alertas de actividad de KeyArmor	900009	El usuario ha iniciado sesión con RSA.	KeyArmor

Categoría	ID del mensaje	Descripción	Productos
Alertas de actividad de KeyArmor	900150	El usuario no ha podido iniciar sesión con una contraseña de un único uso	KeyArmor
Alertas de actividad de KeyArmor	900151	El usuario no ha podido iniciar sesión con una contraseña fija	KeyArmor
Alertas de actividad de KeyArmor	900152	El usuario no ha podido iniciar sesión con una tarjeta inteligente	KeyArmor
Alertas de actividad de KeyArmor	900153	El usuario no ha podido iniciar sesión con autenticación de dominio.	KeyArmor
Alertas de actividad de KeyArmor	900154	El usuario no ha podido iniciar sesión con autenticación remota	KeyArmor
Alertas de actividad de KeyArmor	900155	El usuario no ha podido iniciar sesión con autenticación por código de color.	KeyArmor
Alertas de actividad de KeyArmor	900156	El usuario no ha podido iniciar sesión con PIN.	KeyArmor
Alertas de actividad de KeyArmor	900157	El usuario no ha podido iniciar sesión con OCSP	KeyArmor
Alertas de actividad de KeyArmor	900158	Se ha bloqueado al usuario tras demasiados intentos de inicio de sesión fallidos.	KeyArmor

Categoría	ID del mensaje	Descripción	Productos
Alertas de actividad de KeyArmor	900301	Se ha superado el número de intentos de inicio de sesión fallidos	KeyArmor
Alertas de actividad de KeyArmor	900350	Clave borrada	KeyArmor
Alertas de actividad de KeyArmor	903000	El usuario ha cambiado el nombre de un archivo	KeyArmor
Alertas de actividad de KeyArmor	903001	El usuario ha cambiado un archivo	KeyArmor
Alertas de actividad de KeyArmor	903002	El usuario ha eliminado un archivo	KeyArmor
Alertas de actividad de KeyArmor	903003	El usuario ha creado un archivo	KeyArmor
Alertas de actividad de KeyArmor	903100	Se ha aplicado la acción principal porque no hay conexión con PolicyServer.	KeyArmor
Alertas de actividad de KeyArmor	903101	Se ha aplicado la acción secundaria porque no hay conexión con PolicyServer.	KeyArmor
Alertas de actividad de KeyArmor	903102	Actualizaciones de política aplicadas	KeyArmor
Alertas de actividad de KeyArmor	904000	Archivo infectado reparado	KeyArmor

Categoría	ID del mensaje	Descripción	Productos
Alertas de actividad de KeyArmor	904001	No se puede reparar el archivo infectado.	KeyArmor
Alertas de actividad de KeyArmor	904002	Omitiendo el archivo infectado; reparación no compatible	KeyArmor
Alertas de actividad de KeyArmor	904003	Archivo infectado eliminado	KeyArmor
Alertas de actividad de KeyArmor	904004	No se puede eliminar el archivo infectado.	KeyArmor
Alertas de actividad de KeyArmor	904005	Eliminando dispositivo debido a un archivo infectado	KeyArmor
Alertas de actividad de KeyArmor	904006	Error al eliminar el dispositivo debido a un archivo infectado	KeyArmor
Alertas de actividad de KeyArmor	904007	Invocando acción de reserva de archivo infectado	KeyArmor
Alertas de actividad de KeyArmor	904010	Archivos de antivirus actualizados	KeyArmor
Alertas de actividad de KeyArmor	904011	No se pueden actualizar los archivos del antivirus.	KeyArmor
Alertas de inicio y fin de sesión	100013	Error al intentar iniciar sesión	Full Disk Encryption, FileArmor, DriveArmor, KeyArmor o PolicyServer

Categoría	ID del mensaje	Descripción	Productos
Alertas de inicio y fin de sesión	100014	Inicio de sesión correcto	Full Disk Encryption, FileArmor, DriveArmor, KeyArmor o PolicyServer
Alertas de inicio y fin de sesión	100016	No se puede iniciar sesión. Utilice la autenticación remota para proporcionar al administrador de PolicyServer un código de pregunta.	Full Disk Encryption, FileArmor, DriveArmor, KeyArmor o PolicyServer
Alertas de inicio y fin de sesión	100021	Inicio de sesión con códigos de colores incorrecto	Full Disk Encryption, FileArmor, DriveArmor, KeyArmor o PolicyServer
Alertas de inicio y fin de sesión	100022	Inicio de sesión con contraseña fija incorrecto	Full Disk Encryption, FileArmor, DriveArmor, KeyArmor o PolicyServer
Alertas de inicio y fin de sesión	100023	Inicio de sesión con PIN incorrecto	Full Disk Encryption, FileArmor, DriveArmor, KeyArmor o PolicyServer
Alertas de inicio y fin de sesión	100024	Inicio de sesión con X99 incorrecto	Full Disk Encryption, FileArmor, DriveArmor, KeyArmor o PolicyServer

Categoría	ID del mensaje	Descripción	Productos
Alertas de inicio y fin de sesión	100028	Inicio de sesión con códigos de colores correcto	Full Disk Encryption, FileArmor, DriveArmor, KeyArmor o PolicyServer
Alertas de inicio y fin de sesión	100031	Inicio de sesión con X9.9 correcto	Full Disk Encryption, FileArmor, DriveArmor, KeyArmor o PolicyServer
Alertas de inicio y fin de sesión	100032	Inicio de sesión remoto correcto	Full Disk Encryption, FileArmor, DriveArmor, KeyArmor o PolicyServer
Alertas de inicio y fin de sesión	100035	Inicio de sesión con WebToken correcto	Full Disk Encryption, FileArmor, DriveArmor, KeyArmor o PolicyServer
Alertas de inicio y fin de sesión	100036	Inicio de sesión con WebToken incorrecto	Full Disk Encryption, FileArmor, DriveArmor, KeyArmor o PolicyServer
Alertas de inicio y fin de sesión	100050	Se ha bloqueado el inicio de sesión con contraseña fija debido al bloqueo.	Full Disk Encryption, FileArmor, DriveArmor, KeyArmor o PolicyServer
Alertas de inicio y fin de sesión	100051	El inicio de sesión del usuario se ha desbloqueado correctamente	Full Disk Encryption, FileArmor, DriveArmor, KeyArmor o PolicyServer

Categoría	ID del mensaje	Descripción	Productos
Alertas de inicio y fin de sesión	100057	Autenticación del usuario LDAP correcta	Full Disk Encryption, FileArmor, DriveArmor, KeyArmor o PolicyServer
Alertas de inicio y fin de sesión	100058	Error en la autenticación del usuario LDAP	Full Disk Encryption, FileArmor, DriveArmor, KeyArmor o PolicyServer
Alertas de inicio y fin de sesión	100059	Cambio de la contraseña del usuario LDAP correcto	Full Disk Encryption, FileArmor, DriveArmor, KeyArmor o PolicyServer
Alertas de inicio y fin de sesión	100060	Error al cambiar la contraseña del usuario LDAP	Full Disk Encryption, FileArmor, DriveArmor, KeyArmor o PolicyServer
Alertas de inicio y fin de sesión	100061	Se ha interrumpido la solicitud de acceso debido a un error en la comprobación de integridad de la política.	Full Disk Encryption, FileArmor, DriveArmor, KeyArmor o PolicyServer
Alertas de inicio y fin de sesión	100070	La sesión se ha cerrado correctamente	Full Disk Encryption, FileArmor, DriveArmor, KeyArmor o PolicyServer

Categoría	ID del mensaje	Descripción	Productos
Alertas de inicio y fin de sesión	100433	Los códigos de colores no coinciden.	Full Disk Encryption, FileArmor, DriveArmor, KeyArmor o PolicyServer
Alertas de inicio y fin de sesión	100434	No se puede cambiar el código de color. El nuevo código de color debe ser distinto al actual.	Full Disk Encryption, FileArmor, DriveArmor, KeyArmor o PolicyServer
Alertas de inicio y fin de sesión	100435	No se puede cambiar el código de color. El nuevo código de color debe cumplir los requisitos de longitud mínima definidos por PolicyServer.	Full Disk Encryption, FileArmor, DriveArmor, KeyArmor o PolicyServer
Alertas de inicio y fin de sesión	100436	No se puede cambiar el código de color. El nuevo código de color debe ser distinto a cualquier código de color que se haya utilizado anteriormente.	Full Disk Encryption, FileArmor, DriveArmor, KeyArmor o PolicyServer
Alertas de inicio y fin de sesión	100437	Error al cambiar el código de color - Error interno	Full Disk Encryption, FileArmor, DriveArmor, KeyArmor o PolicyServer

Categoría	ID del mensaje	Descripción	Productos
Alertas de inicio y fin de sesión	100459	Error al cambiar la contraseña de X9.9: no se puede conectar al host de PolicyServer	Full Disk Encryption, FileArmor, DriveArmor, KeyArmor o PolicyServer
Alertas de inicio y fin de sesión	100460	Error al cambiar la contraseña de X9.9 - Número de serie vacío	Full Disk Encryption, FileArmor, DriveArmor, KeyArmor o PolicyServer
Alertas de inicio y fin de sesión	100461	Error al cambiar la contraseña de X9.9 - Error interno	Full Disk Encryption, FileArmor, DriveArmor, KeyArmor o PolicyServer
Alertas de inicio y fin de sesión	101004	No se puede restablecer el dispositivo bloqueado.	Full Disk Encryption, FileArmor, DriveArmor, KeyArmor o PolicyServer
Alertas de inicio y fin de sesión	104000	Inicio de sesión de tarjeta inteligente correcto.	Full Disk Encryption, FileArmor, DriveArmor, KeyArmor o PolicyServer
Alertas de inicio y fin de sesión	104001	Inicio de sesión de tarjeta inteligente incorrecto. Compruebe que la tarjeta está correctamente insertada y que el PIN de la tarjeta inteligente es válido.	Full Disk Encryption, FileArmor, DriveArmor, KeyArmor o PolicyServer

Categoría	ID del mensaje	Descripción	Productos
Alerta de dispositivo móvil	100037	Falta la base de datos de políticas de Palm	Full Disk Encryption, FileArmor, DriveArmor, KeyArmor o PolicyServer
Alerta de dispositivo móvil	100038	Error de cifrado de Palm	Full Disk Encryption, FileArmor, DriveArmor, KeyArmor o PolicyServer
Alerta de dispositivo móvil	100039	El cifrado del dispositivo PPC ha cambiado	Full Disk Encryption, FileArmor, DriveArmor, KeyArmor o PolicyServer
Alerta de dispositivo móvil	100040	Error de cifrado de PPC	Full Disk Encryption, FileArmor, DriveArmor, KeyArmor o PolicyServer
Alertas de actividad de MobileFirewall	300000	MobileFirewall	MobileFirewall
Alertas de actividad de MobileFirewall	300001	DenialOfServiceAttack	MobileFirewall
Alertas de OCSP	104005	Estado del certificado OCSP correcto.	Full Disk Encryption, FileArmor, DriveArmor, KeyArmor o PolicyServer
Alertas de OCSP	104006	Estado del certificado OCSP revocado.	Full Disk Encryption, FileArmor, DriveArmor, KeyArmor o PolicyServer

Categoría	ID del mensaje	Descripción	Productos
Alertas de OCSP	104007	Estado del certificado OCSP desconocido.	Full Disk Encryption, FileArmor, DriveArmor, KeyArmor o PolicyServer
Alertas de OTA	100041	Falta el objeto OTA o está dañado.	Full Disk Encryption, FileArmor, DriveArmor, KeyArmor o PolicyServer
Alertas de OTA	100042	Sincronización de OTA correcta	Full Disk Encryption, FileArmor, DriveArmor, KeyArmor o PolicyServer
Alertas de OTA	100043	Dispositivo OTA eliminado	Full Disk Encryption, FileArmor, DriveArmor, KeyArmor o PolicyServer
Alertas de contraseña	100017	Error en el cambio de contraseña	Full Disk Encryption, FileArmor, DriveArmor, KeyArmor o PolicyServer
Alertas de contraseña	100018	Se ha superado el número de intentos de contraseña	Full Disk Encryption, FileArmor, DriveArmor, KeyArmor o PolicyServer
Alertas de contraseña	100025	Restablecer la contraseña a códigos de colores	Full Disk Encryption, FileArmor, DriveArmor, KeyArmor o PolicyServer

Categoría	ID del mensaje	Descripción	Productos
Alertas de contraseña	100026	Restablecer la contraseña a fija	Full Disk Encryption, FileArmor, DriveArmor, KeyArmor o PolicyServer
Alertas de contraseña	100027	Restablecer la contraseña a PIN	Full Disk Encryption, FileArmor, DriveArmor, KeyArmor o PolicyServer
Alertas de contraseña	100029	Inicio de sesión con contraseña fija correcto	Full Disk Encryption, FileArmor, DriveArmor, KeyArmor o PolicyServer
Alertas de contraseña	100030	Inicio de sesión con PIN correcto	Full Disk Encryption, FileArmor, DriveArmor, KeyArmor o PolicyServer
Alertas de contraseña	100033	No se puede restablecer la contraseña	Full Disk Encryption, FileArmor, DriveArmor, KeyArmor o PolicyServer
Alertas de contraseña	100432	No se puede cambiar la contraseña. La nueva contraseña debe ser distinta a la actual.	Full Disk Encryption, FileArmor, DriveArmor, KeyArmor o PolicyServer
Alertas de contraseña	100439	No se puede cambiar la contraseña. Las contraseñas no coinciden.	Full Disk Encryption, FileArmor, DriveArmor, KeyArmor o PolicyServer

Categoría	ID del mensaje	Descripción	Productos
Alertas de contraseña	100441	No se puede cambiar la contraseña. El campo de la contraseña no puede estar vacío.	Full Disk Encryption, FileArmor, DriveArmor, KeyArmor o PolicyServer
Alertas de contraseña	100442	No se puede cambiar la contraseña. La contraseña no cumple los requisitos de longitud mínima definidos por PolicyServer.	Full Disk Encryption, FileArmor, DriveArmor, KeyArmor o PolicyServer
Alertas de contraseña	100443	No se puede cambiar la contraseña. No se permiten números.	Full Disk Encryption, FileArmor, DriveArmor, KeyArmor o PolicyServer
Alertas de contraseña	100444	No se puede cambiar la contraseña. No se permiten letras.	Full Disk Encryption, FileArmor, DriveArmor, KeyArmor o PolicyServer
Alertas de contraseña	100445	No se puede cambiar la contraseña. No se permiten caracteres especiales.	Full Disk Encryption, FileArmor, DriveArmor, KeyArmor o PolicyServer
Alertas de contraseña	100446	No se puede cambiar la contraseña. La contraseña no puede contener el nombre de usuario.	Full Disk Encryption, FileArmor, DriveArmor, KeyArmor o PolicyServer

Categoría	ID del mensaje	Descripción	Productos
Alertas de contraseña	100447	No se puede cambiar la contraseña. La contraseña no contiene suficientes caracteres especiales.	Full Disk Encryption, FileArmor, DriveArmor, KeyArmor o PolicyServer
Alertas de contraseña	100448	No se puede cambiar la contraseña. La contraseña no contiene suficientes números.	Full Disk Encryption, FileArmor, DriveArmor, KeyArmor o PolicyServer
Alertas de contraseña	100449	No se puede cambiar la contraseña. La contraseña no contiene suficientes caracteres.	Full Disk Encryption, FileArmor, DriveArmor, KeyArmor o PolicyServer
Alertas de contraseña	100450	No se puede cambiar la contraseña. La contraseña contiene demasiados caracteres consecutivos.	Full Disk Encryption, FileArmor, DriveArmor, KeyArmor o PolicyServer
Alertas de contraseña	100451	No se puede cambiar la contraseña. La nueva contraseña debe ser distinta a cualquier contraseña que se haya utilizado anteriormente.	Full Disk Encryption, FileArmor, DriveArmor, KeyArmor o PolicyServer

Categoría	ID del mensaje	Descripción	Productos
Alertas de contraseña	100452	Error al cambiar la contraseña - Error interno	Full Disk Encryption, FileArmor, DriveArmor, KeyArmor o PolicyServer
Alertas de contraseña	101003	La contraseña fija se ha cambiado correctamente.	Full Disk Encryption, FileArmor, DriveArmor, KeyArmor o PolicyServer
Alertas de contraseña	700100	Se ha restablecido la contraseña a contraseña fija.	FileArmor SP6 o anterior
Alertas de contraseña	700101	Se ha restablecido la contraseña a tarjeta inteligente.	FileArmor SP6 o anterior
Alertas de contraseña	700102	Se ha restablecido la contraseña a autenticación de dominio.	FileArmor SP6 o anterior
Alertas de contraseña	900159	No se puede cambiar la contraseña.	KeyArmor
Alertas de contraseña	900160	La contraseña se ha cambiado correctamente.	KeyArmor
Alertas de contraseña	900302	Se ha restablecido la contraseña a contraseña fija.	KeyArmor
Alertas de contraseña	900303	Se ha restablecido la contraseña a tarjeta inteligente.	KeyArmor

Categoría	ID del mensaje	Descripción	Productos
Alertas de contraseña	900304	Se ha restablecido la contraseña a autenticación de dominio.	KeyArmor
Alertas de cambio de PIN	100438	No se puede cambiar el PIN. Los PIN no coinciden.	Full Disk Encryption, FileArmor, DriveArmor, KeyArmor o PolicyServer
Alertas de cambio de PIN	100440	No se puede cambiar el PIN. Uno de los campos está vacío.	Full Disk Encryption, FileArmor, DriveArmor, KeyArmor o PolicyServer
Alertas de cambio de PIN	100453	No se puede cambiar el PIN. Los PIN no coinciden.	Full Disk Encryption, FileArmor, DriveArmor, KeyArmor o PolicyServer
Alertas de cambio de PIN	100454	se puede cambiar el PIN. El nuevo PIN no puede ser el mismo que el anterior.	Full Disk Encryption, FileArmor, DriveArmor, KeyArmor o PolicyServer
Alertas de cambio de PIN	100455	No se puede cambiar el PIN. El nuevo PIN no cumple los requisitos de longitud mínima definidos por PolicyServer.	Full Disk Encryption, FileArmor, DriveArmor, KeyArmor o PolicyServer

Categoría	ID del mensaje	Descripción	Productos
Alertas de cambio de PIN	100456	No se puede cambiar el PIN. El PIN no puede contener el nombre de usuario.	Full Disk Encryption, FileArmor, DriveArmor, KeyArmor o PolicyServer
Alertas de cambio de PIN	100457	No se puede cambiar el PIN. El nuevo PIN debe ser distinto a cualquier PIN que se haya utilizado anteriormente.	Full Disk Encryption, FileArmor, DriveArmor, KeyArmor o PolicyServer
Alertas de cambio de PIN	100458	Error al cambiar el PIN - Error interno	Full Disk Encryption, FileArmor, DriveArmor, KeyArmor o PolicyServer
Alertas de tarjeta inteligente	104002	Tarjeta inteligente registrada.	Full Disk Encryption, FileArmor, DriveArmor, KeyArmor o PolicyServer
Alertas de tarjeta inteligente	104004	No se puede registrar la tarjeta inteligente. Compruebe que la tarjeta está correctamente insertada y que el PIN de la tarjeta inteligente es válido.	Full Disk Encryption, FileArmor, DriveArmor, KeyArmor o PolicyServer
Alertas de Windows Mobile	800000	Instalación de OTA iniciada	Full Disk Encryption para Windows Mobile

Categoría	ID del mensaje	Descripción	Productos
Alertas de Windows Mobile	800001	Instalación de OTA completada	Full Disk Encryption para Windows Mobile
Alertas de Windows Mobile	800100	Mensaje SMS de OTA enviado	Full Disk Encryption para Windows Mobile
Alertas de Windows Mobile	800200	Listado del directorio de OTA recibido	Full Disk Encryption para Windows Mobile
Alertas de Windows Mobile	800300	Atributos del dispositivo OTA recibidos	Full Disk Encryption para Windows Mobile
Alertas de Windows Mobile	800400	Copia de seguridad del dispositivo OTA	Full Disk Encryption para Windows Mobile
Alertas de Windows Mobile	800500	Restauración del dispositivo OTA	Full Disk Encryption para Windows Mobile

Índice

A

Accesibilidad
    teclado en pantalla, 5-4
acerca de
    arquitectura cliente-servidor, 1-2
    Endpoint Encryption, 1-2
    FileArmor, 6-1
    KeyArmor, 7-1
    PolicyServer, 2-1, 2-2
    tipos de cuenta, 1-12
    usuarios y grupos, 2-4
Active Directory, 1-16, 1-21, 4-24
    restablecer contraseña, 4-27
administración central, 1-8, 1-12
administración de claves, 1-11
administración de dispositivos, 1-8
administrar grupos, 2-4
administrar usuarios, 2-4
alertas, 8-3
arquitectura cliente-servidor, 1-2
arquitectura del sistema, 1-2
Arranque previo de Full Disk Encryption, 5-2
    autenticación, 5-5
    conectividad de red, 5-4
    diseño del teclado, 5-4
    opciones de menú, 5-3
    teclado en pantalla, 5-4
asistencia
    base de conocimientos, 9-2
    resolver problemas de manera más rápida, 9-3
    TrendLabs, 9-4
autenticación, 1-8
    acerca de, 1-12
Arranque previo de Full Disk Encryption, 5-2
autenticación de dominios, 1-15
autoayuda
    utilizar, 5-14
Autoayuda, 1-15, 1-19, 4-27, 5-13
    respuestas, 5-14
ayuda remota, 1-15, 5-10
Ayuda remota, 1-19, 5-9
cambiar contraseña, 6-6
cambiar método, 5-5, 5-7
ColorCode, 1-15, 1-17, 5-6, 6-5
comparación de aplicaciones, 1-13
contraseña fija, 1-15, 1-17, 7-3
control de acceso, 1-13
crear código de colores, 5-7
dominio, 1-16
FileArmor, 6-2
inicio de sesión único, 6-3
KeyArmor, 7-2
    primera vez, 7-2
LDAP, 1-16
métodos, 1-15
opciones, 1-14
opciones de seguridad, 1-14
PIN, 1-15, 1-17, 6-5
primer uso, 6-2
requisitos de configuración, 1-16
requisitos previos, 1-16
tarjeta inteligente, 1-18, 5-11, 6-4
tipos de cuenta, 1-12
autenticación de dominios, 1-16
    FileArmor, 6-3

Autoayuda, 1-19, 4-24, 5-13
asistencia para la contraseña, 4-27
definición de respuestas, 5-13
respuestas, 5-14
Ayuda de la línea de comandos, 5-2
Ayuda del instalador de la línea de comandos, 5-2
Ayuda remota, 1-19, 4-24, 4-28, 4-37, 5-9

C

cambiar de PolicyServer, 5-25
cambiar las contraseñas, 5-5
CD de reparación, 5-2, 5-26, 5-28
descifrado, 5-30
recuperación de datos, 5-29
Cifrado, 1-9, 3-30
archivar, 6-15
archivo y carpeta, 1-10
basado en hardware, 1-9, 1-10
basado en software, 1-9, 1-10
características, 1-8
certificado digital, 6-14
cifrado de archivos, 6-1
clave de contraseña fija, 6-13
clave local, 6-11
claves
compartidas, 6-12
disco completo, 1-10
extracción automática, 6-13
FileArmor
archivar y grabar, 6-11
FIPS, 1-11, 7-11
KeyArmor, 7-5
cifrado basado en hardware, 1-6
ColorCode, 1-17, 5-6
componentes del producto, 1-2
comunidad, 9-2
Configuración de red, 5-24
consideraciones de Windows Server 2008, 1-5
consola de recuperación
iniciar sesión, 5-18
Consola de recuperación, 5-16
acceso, 5-18
Windows, 5-18
administrar políticas, 5-24
administrar usuarios, 5-21
cambiar empresa o servidor, 5-25
cd de reparación, 5-30
configuración de red, 5-25
Configuración de red, 5-24
Descifrar disco, 5-19
funciones, 5-16
iniciar sesión, 5-18
métodos de recuperación, 5-26
Montar particiones, 5-20
Restaurar arranque, 5-21
usuarios
Agregar, 5-23
editar, 5-22
Eliminar, 5-23
ver registros, 5-24
contraseña
Autoayuda, 4-27
contraseña fija, 1-17
contraseñas, 1-12, 4-24
Ayuda remota, 4-28
restablecer, 4-25
restablecer a contraseña fija, 4-26
restablecer administrador/autenticador, 4-24
restablecer administrador/autenticador de grupo, 4-25

restablecer contraseña de Active Directory, 4-27
restablecer contraseña de autenticador de empresa, 4-24
restablecer contraseña de usuario, 4-26
control de políticas, 1-10, 6-1
criptografía, 1-2
csv, 4-12
cuentas
tipos, 1-12

D

DAAutoLogin, 5-2
definiciones de productos, xii–xiv
descifrado
Consola de recuperación, 5-19
Descifrar disco, 5-19
descripción
administración de claves, 1-11
cifrado de archivos, 1-10
Endpoint Encryption, 1-1
FIPS, 1-11
full disk encryption, 1-10
dispositivos, 4-1, 4-31
agregar a grupo, 4-31
bloquear, 4-37
comando eliminar, 4-37
eliminar de un grupo, 4-33
listado de directorio, 4-36
reiniciar, 4-38
ver atributos, 4-35
ver directorio, 4-35

E

Endpoint Encryption
acerca de, 1-2
herramientas, 5-2
en línea
comunidad, 9-2

F

FileArmor, 6-1
archivar, 6-11
archivar y grabar, 6-11, 6-15
autenticación, 6-2
dominio, 6-3
opciones, 1-14
PIN, 6-5
Ayuda remota, 6-6, 6-8
cambiar contraseña, 6-6
cambiar PolicyServer, 6-10
certificado digital, 6-14
crear, 6-15
Cifrado, 6-11
cifrado de archivos, 1-10
clave compartida, 6-12
crear, 6-13
clave de contraseña fija
crear, 6-14
clave local, 6-11, 6-12
ColorCode, 6-5
control de acceso, 1-13
demora de tiempo, 6-8
desbloquear dispositivo, 6-6
eliminación segura, 6-16
grabar archivo con certificado, 6-16
grabar archivo con contraseña fija, 6-15
icono de la bandeja
acerca de, 6-8
icono de la bandeja del sistema, 6-8
inicio de sesión único, 6-3
primer uso, 6-2
requisitos del sistema, 1-7
restablecer contraseña, 6-6, 6-8

sincronización con PolicyServer, 6-9
sincronización de archivos sin conexión, 6-10
sincronizar PolicyServer, 6-8
sistemas operativos compatibles, 1-7
tarjetas inteligentes, 6-4
FIPS, 1-2
acerca de, 1-11
FIPS 140-2, 1-2, 1-11
KeyArmor, 7-11
niveles de seguridad, 1-11
FIPS 140-2, 1-2
Full Disk Encryption, 5-1
3.1.3: mejoras, 1-21
acceso TCP/IP, 5-15
administrar políticas, 5-24
administrar usuarios, 5-21
autenticación, 1-19, 5-13
cambiar contraseña, 5-5
opciones, 1-14
Autoayuda, 5-13
ayuda remota, 5-10
cambiar empresa, 5-25
cambiar PolicyServer, 5-25
conectividad, 5-15
configuración del puerto, 5-15
Configuración de PolicyServer, 5-15
configuración de red, 5-24, 5-25
Consola de recuperación, 5-18
Windows, 5-18
control de acceso, 1-13
Descifrar disco, 5-19
desinstalar, 5-26
eliminar dispositivo, 4-34
herramientas, 5-2
instalación no administrada
usuarios, 5-21
limpiar archivos, 5-31
métodos de recuperación, 5-26
opciones de menú, 5-3
requisitos del sistema, 1-6
sincronizar políticas, 5-16
sistemas operativos compatibles, 1-6
tarjetas inteligentes, 1-18, 5-11
funciones clave, 1-8

G

grabar discos, 6-15
grupos, 4-1
crear grupos sin conexión, 4-6
eliminar, 4-5
eliminar dispositivo, 4-33, 4-34
grupos sin conexión, 4-5
instalar en un grupo, 4-21
modificar, 4-5
subgrupos, 4-2
tipos, 4-2
grupo superior, 2-5, 4-2

H

herramientas
CD de reparación, 5-28

I

icono de la bandeja del sistema, 6-8
idiomas admitidos, 1-20
importación de usuarios, 4-12, 4-13
informes, 1-2, 1-8
Informes, 8-1, 8-6
alerta, 8-9, 8-10
estándar, 8-8, 8-9
iconos de, 8-7
mostrar errores, 8-11

mostrar informes, 8-10
opciones, 8-6
programar informes, 8-11
tipos de, 8-7
Infraestructura virtual de VMware, 1-5

K

KeyArmor, 7-1
acerca de, 7-7
actualizaciones de antivirus, 7-5
actualizaciones de políticas, 7-7
administración de claves, 1-11
advertencia, 7-6
antivirus, 7-14
cambiar ubicación de actualización, 7-15
archivos almacenados en caché, 7-6
autenticación, 7-2
contraseña fija, 7-3
métodos, 7-3
opciones, 1-14
primera vez, 7-2
ayuda
Autoayuda, 7-10
Información de asistencia, 7-11
Restablecimiento remoto de contraseña, 7-10
si se encuentra, 7-8
barra de tareas, 7-7
cambiar contraseña, 7-7
Cifrado, 7-5
componentes de dispositivos, 7-4
comprobación de disco, 7-6
control de acceso, 1-13
desconectar, 7-7
dispositivo eliminado, 7-18
dispositivos sin cifrar, 7-6
exploración completa, 7-14
extracción segura, 7-6, 7-13
FIPS, 7-11
menú, 7-8
menú de ayuda, 7-8
ninguna información sin controlar, 7-5
PolicyServer, 7-13
protección de archivos, 7-12
proteger datos, 7-7
reasignar, 7-16
registro de actividad, 7-13
requisitos del sistema, 1-8
SECURE DRIVE, 7-4
temporal, 7-6
utilizar, 7-6

L

LDAP, 1-16

M

MBR
sustitución, 5-21
mensajes de error
autenticación, 1-14
métodos de recuperación, 5-26
Montar particiones, 5-20

N

Número de identificación personal (PIN), 1-17

O

OPAL, 1-6

P

PolicyServer
3.1.3: mejoras, 1-21
activar aplicaciones, 2-17

agregar grupo superior, 2-5, 4-2
agregar usuario empresarial, 2-9, 4-10
archivo de licencia, 2-2
autenticación, 2-2
    opciones, 1-14
Ayuda remota, 4-28
cambiar, 5-25
campos y botones, 2-14
configurar alertas de registro, 8-3
control de acceso, 1-13
dispositivos, 4-31
grupos, 2-4
    agregar usuarios, 2-7, 4-16
grupos sin conexión, 4-5
    actualizar, 4-9
    crear, 4-6
Información de asistencia, 4-30
Informes, 8-1, 8-6
instalaciones avanzadas, 8-5
interfaz, 2-3
introducción, 2-1, 2-2
Jerarquía de la MMC, 2-4
mejoras, 1-20
modificación de políticas, 2-15
políticas, 2-13, 3-1, 3-2
    Común, 3-52
    DriveArmor, 3-46
    editar, 3-3
        cadena de texto, 3-10
        políticas con intervalos, 3-3
        selección múltiple, 3-7
        varias opciones, 3-11
        Verdadero/Falso, Sí/No, 3-5
    FileArmor, 3-30
    Full Disk Encryption, 3-20
    Información de asistencia, 4-30
    KeyArmor, 3-40
    MobileSentinel, 3-36
    políticas de PolicyServer, 3-13
primer uso, 2-2
registros, 8-1
requisitos
    SQL, 1-5
requisitos del sistema
    hardware, 1-5
requisitos de software, 1-5
Requisitos de SQL, 1-5
servicio Web, 1-2
servicio Web del cliente, 1-2
subgrupos, 4-4
sucesos del registro, 8-2
transmitir SMS/envío de correo electrónico, 8-4
usuarios, 2-4, 4-10
    agregar a grupo, 2-7, 2-11, 4-16, 4-18
    agregar usuario empresarial, 2-7, 4-16
usuarios y grupos, 2-5
Ventana de MMC, 3-2
PolicyServer MMC, 1-2
políticas, 1-12
    común, 3-52
        agente, 3-52
        autenticación, 3-52
    DriveArmor, 3-46
        autenticación, 3-46
        comunicaciones, 3-49
        dispositivo, 3-51
    FileArmor
        Cifrado, 3-30
        contraseña, 3-35
        equipo, 3-30

Full Disk Encryption, 3-20
común, 3-21
PC, 3-23
PPC, 3-27
Información de asistencia, 4-30
KeyArmor, 3-40
antivirus, 3-41
conexión de PolicyServer, 3-45
iniciar sesión, 3-42
mensaje de notificación, 3-44
seguridad, 3-41
MobileSentinel, 3-36
común, 3-36
PPC, 3-38
permitir recuperación de usuario, 5-18
PolicyServer, 3-13
Administrador, 3-14
alertas de registro, 3-17
Autenticador, 3-16, 3-17
consola de administración, 3-13
descarga de Service Pack, 3-19
mensaje de bienvenida, 3-20
PDA, 3-18
Sincronización, 1-10
sincronización de clientes, 5-16
políticas de asistencia técnica, 4-30
políticas de sincronización, 5-16
protección de datos, 1-2
Proxy LDAP, 1-21, 4-10

R

recuperación
limpiar archivos, 5-31
recuperación de datos, 5-29
registros, 5-24, 8-1
administrar sucesos, 8-2
alertas, 8-3
configurar alertas, 8-3
requisitos de base de datos, 1-5
requisitos del sistema
FileArmor, 1-7
Full Disk Encryption, 1-6
KeyArmor, 1-8
PolicyServer, 1-5
Restaurar arranque, 5-21

S

seguridad
acción de bloqueo de cuenta, 1-19, 5-9
bloqueo de cuenta, 1-19, 5-9
bloqueo de dispositivo, 1-19, 5-9
borrar dispositivo, 1-14
demora de tiempo, 1-14
intentos de inicio de sesión fallidos permitidos, 1-19, 5-9
período de bloqueo de cuenta, 1-19, 5-9
protección antimalware y antivirus, 1-2
requiere autenticación remota, 1-14
símbolos, 5-12
Sincronización
FileArmor, 6-9
software, 1-5
sucesos del registro, 8-2

T

tarjeta inteligente, 1-18, 5-11
teclado en pantalla, 5-4
terminología, xii–xiv
TrendLabs, 9-4

U

Unidades DriveTrust de Seagate, 1-6
usuarios, 4-1, 4-10
agregar, 4-10

agregar nuevo usuario empresarial, 2-9, 4-10
agregar un nuevo usuario a un grupo, 2-7, 4-16
agregar un usuario existente a un grupo, 2-11, 4-18
cambiar el grupo predeterminado, 4-20
cambios de grupo y de empresa, 4-15
contraseñas, 4-24
contraseñas de Active Directory, 4-27
eliminar de un grupo, 4-22
encontrar, 4-14
explorador de directorio externo, 4-13
importación con CSV, 4-12
importación de usuarios de AD, 4-13
instalar en un grupo, 4-21
modificar, 4-15
pertenencia a grupo, 4-15
usuarios y grupos, 2-5

W

Windows 8, 1-6

Z

zona desmilitarizada, 5-15



TREND MICRO INCORPORATED

10101 North De Anza Blvd. Cupertino, CA., 95014, USA

Tel:+1(408)257-1500/1-800 228-5651 Fax:+1(408)257-2003 info@trendmicro.com

www.trendmicro.com

Item Code: APSM35733/121016