TREND MICRO™

3.1

TREND MICRO™ Endpoint Encryption

Guía de instalación

Cifrado completo de punto final para datos inactivos

Endpoint Security

Nº de documento: APSM35736/121016

Fecha de publicación: Dec 2012

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

Capítulo 1: Introducción a Trend Micro Endpoint Encryption

Capítulo 2: Consideraciones sobre la implementación

Capítulo 3: Instalación de PolicyServer

Capítulo 4: Instalación del cliente de cifrado de punto final

Capítulo 5: Actualizaciones, migraciones y desinstalaciones

Prefacio

Prefacio

Bienvenido a la Guía de instalación de Endpoint Encryption de Trend Micro™. En esta guía se recomienda a los administradores que se "familiaricen" en el menor tiempo posible mediante la descripción de las funciones y la arquitectura de seguridad de Endpoint Encryption. En los temas se incluyen los requisitos del sistema, cómo preparar la implementación, cómo instalar el software cliente y PolicyServer, y se señala lo que deberían explicar a los usuarios finales y cómo actualizar o migrar un servidor y las aplicaciones cliente.

En este prefacio se describen los temas siguientes:

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

Capítulo 1

Introducción a Trend Micro Endpoint Encryption

Al evaluar el valor de cualquier proyecto de Endpoint Encryption, es esencial una planificación cuidadosa.

En este capítulo se presentan los siguientes temas:

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.

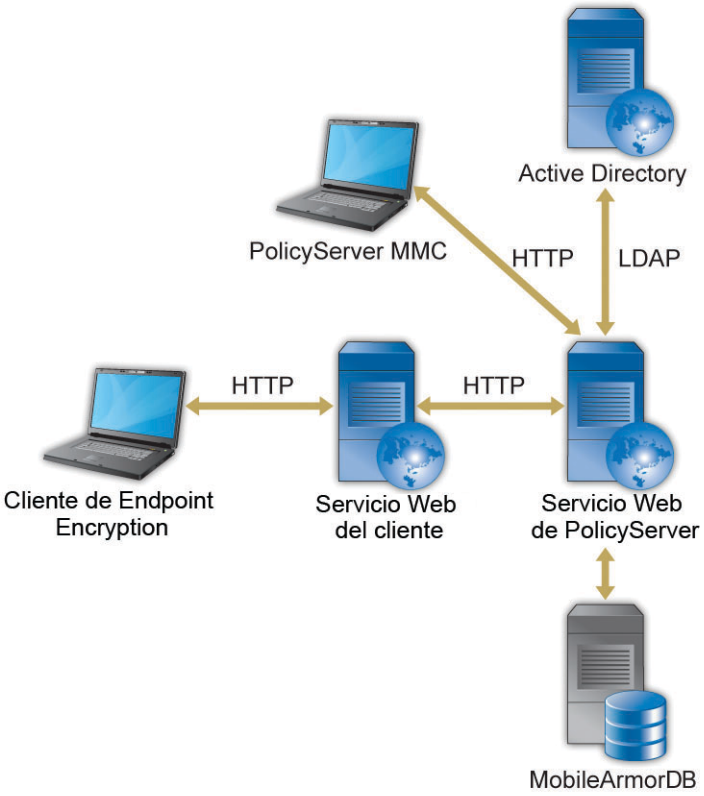


FIGURA 1-1. Arquitectura cliente-servidor de Endpoint Encryption

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)
Otro software	Requisitos adicionales para Windows 8: • Microsoft .NET Framework 3.5 está activado • Para dispositivos con UEFI, consulte *Preparación del dispositivo en la página 4-5* para cambiar la prioridad de arranque. Requisitos adicionales para Windows XP: • Microsoft .NET Framework 2.0 SP1 o versión posterior • Microsoft Windows Installer 3.1

EVENTO	REQUISITO
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
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 *Preparación del dispositivo en la página 4-5* para 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.

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

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.

Capítulo 2

Consideraciones sobre la implementación

Al tratar cualquier proyecto de cifrado, es importante identificar los objetivos de implementación. Las organizaciones que necesiten satisfacer los requisitos de cumplimiento explícito a menudo requieren soluciones de cifrado más amplias con un gran énfasis en la generación de informes, mientras que las organizaciones que buscan mejorar la seguridad de los datos pueden tener como objetivo necesidades más concretas para proteger activos de datos específicos.

No hay un plan único que se adapte a cada uno de los escenarios de casos de uso y la comprensión de lo que se requiere de una solución de cifrado reducirá considerablemente los tiempos de implementación, minimizará o eliminará la falta de rendimiento y garantizará el éxito del proyecto. Es necesaria una planificación cuidadosa para comprender los requisitos de implementación y las limitaciones al cambiar la escala de una solución de Endpoint Encryption a través de una gran empresa. La planificación es especialmente importante al introducir este cambio en miles de puntos finales, lo que afectará a todos los usuarios finales.

En este capítulo se describen los siguientes temas:

Plataformas admitidas y lista de comprobación previa a la implementación

Las tablas siguientes explican los sistemas operativos compatibles para cada cliente de Trend Micro Endpoint Encryption y los requisitos previos a la implementación.

TABLA 2-1. POLICYSERVER 3.1.3

PLATAFORMAS DE COMPATIBILIDAD	LISTA DE COMPROBACIÓN PREVIA A LA IMPLEMENTACIÓN
Windows Server 2003 (32/64 bits)	• Comprobar que Microsoft .NET 2.0 Service Pack 2 o posterior está instalado en el equipo host • Utilizar una cuenta de administrador para instalar MMC PolicyServer • Se requiere conectividad con PolicyServer para autenticarse en la consola MMC
Windows Server 2008/2008 R2 (64 bits)	

TABLA 2-2. FULL DISK ENCRYPTION

PLATAFORMAS DE COMPATIBILIDAD	LISTA DE COMPROBACIÓN PREVIA A LA IMPLEMENTACIÓN
Windows 8™ (32 o 64 bits)	• En los dispositivos compatibles con UEFI se debe establecer la prioridad de arranque BIOS en Primero heredado en lugar de Primero UEFI. • Compruebe que Microsoft .Net 3.5 esté activado • Ejecutar scandisk y defrag antes de la instalación • Confirmar el sector de inicio estándar MBR • 20% de espacio libre en disco • Hacer copia de seguridad de los datos de usuario **Nota** Full Disk Encryption para Windows 8 no es compatible con las unidades RAID, SCSI, eDrive y OPAL 2.

PLATAFORMAS DE COMPATIBILIDAD	LISTA DE COMPROBACIÓN PREVIA A LA IMPLEMENTACIÓN
Windows 7™ (32 o 64 bits) Windows Vista™ con SP1 (32 o 64 bits) Windows XP™ con SP3 (32 bits)	• Compruebe que está instalado Microsoft .NET 2.0 SP1 o una versión posterior • Windows Installer versión 3.1 • Si está administrado, conectar con PolicyServer • Ejecutar scandisk y defrag antes de la instalación • Confirmar el sector de inicio estándar MBR • 20% de espacio libre en disco • Hacer copia de seguridad de los datos de usuario **Nota** Full Disk Encryption no admite unidades RAID o SCSI.

TABLA 2-3. FileArmor 3.1.3

PLATAFORMAS DE COMPATIBILIDAD	LISTA DE COMPROBACIÓN PREVIA A LA IMPLEMENTACIÓN
Windows 8™ (32 o 64 bits)	• En los dispositivos compatibles con UEFI se debe establecer la prioridad de arranque BIOS en Primero heredado en lugar de Primero UEFI. • Compruebe que Microsoft .Net 3.5 esté activado
Windows 7™ (32 o 64 bits) Windows Vista™ con SP1 (32 o 64 bits) Windows XP™ con SP3 (32 bits)	• Compruebe que está instalado Microsoft.NET 2.0 SP1 o una versión posterior

TABLA 2-4. KeyArmor

PLATAFORMAS DE COMPATIBILIDAD	LISTA DE COMPROBACIÓN PREVIA A LA IMPLEMENTACIÓN
Windows 8™ (32 o 64 bits)	• Windows 8 no es compatible.
Windows 7™ (32 o 64 bits)	• Puerto USB disponible
Windows Vista™ con SP1 (32 o 64 bits)	
Windows XP™ con SP3 (32 bits)	

Preguntas iniciales para la implementación

Este cuestionario le ayudará a definir el equipo del proyecto, documentar su entorno operativo, evaluar los requisitos de arquitectura, facilitar la revisión del hardware de escritorio y los perfiles de software y definir las cuestiones de seguridad y los procesos de soporte técnico y administrativo.

Usuarios finales:

1. ¿Cuál es el número total de usuarios que se va a implementar?
2. De esta cifra, ¿cuántos son:
    - Administradores de empresa
    - Administradores de grupos
    - Autenticadores (personal de asistencia técnica)
    - Usuarios finales

Dispositivos de punto final:

1. ¿Hay un número estándar de particiones de hardware?
2. ¿Tienen los dispositivos varios discos duros físicos?
3. ¿Tienen los dispositivos administradores de inicio dual?

4. ¿Qué software estándar está instalado? Compruebe los siguientes aspectos:

    a. Antivirus

    b. Aplicaciones de seguridad que bloquean las instalaciones de software

    c. Productos de cifrado anteriores

Bases de datos y redes empresariales:

1. ¿Cuántos PolicyServers serán necesarios para dar soporte a la base de usuarios?

    a. Calcule el número máximo de usuarios en tres años.

    b. Si utiliza la autenticación de dominio, se requiere un PolicyServer para cada dominio de Active Directory.

2. ¿Se requiere el equilibrio de carga en los servidores?

    a. El equilibrio de carga se recomienda para instalaciones que requieren alta disponibilidad y redundancia para PolicyServers.

    b. La organización por clústeres puede utilizarse para proporcionar redundancia y alta disponibilidad para los servidores de base de datos.

3. ¿Cuál es el tamaño estimado de la base de datos?

    a. Calcule el número máximo de usuarios en tres años.

    b. El espacio necesario es de aproximadamente 1GB al año por cada 1.000 usuarios finales.

4. ¿Los clientes de punto final deben comunicarse con PolicyServer a través de Internet?

    a. Consulte con el equipo interno de seguridad o redes para comprender los requisitos y disponer de un servidor web en Internet.

    b. Las siguientes funciones son totalmente compatibles con un PolicyServer externo:

    - La autenticación de dominio/con inicio de sesión único se puede utilizar a través de Internet
    - Actualizaciones de políticas a través de Internet

- Auditoría de dispositivos a través de Internet
- Restablecimiento de contraseñas en línea

Asignación de un equipo de proyecto

Una implementación correcta de cualquier producto incluye mantener la continuidad, así como lograr involucrar a usuarios internos. Estructurar el equipo para incluir uno o más miembros estratégicos de los departamentos afectados por la implementación de software puede ayudar a lograr involucrarlos y obtener resultados en el liderazgo de equipos de proyectos más sólidos. Como mínimo, se recomienda que el equipo del proyecto incluya a uno o varios miembros de cada uno de los siguientes grupos:

- Administración ejecutiva
- Servidores de aplicaciones de empresa
- Administradores de base de datos de empresa
- Seguridad de datos
- Soporte técnico de escritorio
- Recuperación de desastres

Lista de comprobación de infraestructura de seguridad

Revise la infraestructura de seguridad existente antes de implementar un nuevo servicio IT en el entorno de producción. Trend Micro proporciona una lista de comprobación de la infraestructura de seguridad que contiene los elementos que se deben revisar para las siguientes áreas:

- Usuario final
- Respuesta a incidentes
- Evaluación de riesgos

- Recursos humanos
- Conformidad

Consulte *Lista de comprobación de infraestructura de seguridad en la página B-1* para obtener información adicional.

Establecimiento de políticas y perfiles de seguridad

Trend Micro Endpoint Encryption establece políticas de seguridad de un modo predeterminado que deberán ser revisadas en función de la implementación y los objetivos de seguridad. Hay políticas predeterminadas para el nombre de usuario, la complejidad de las contraseñas y los requisitos de cambios, el control de dispositivos, la sincronización de políticas y el bloqueo y borrado de dispositivos, entre otras opciones de políticas predeterminadas. Las políticas predeterminadas se pueden cambiar fácilmente dependiendo de los objetivos de seguridad y los mandatos reguladores para la protección de datos.

Cuando se utiliza Endpoint Encryption para controlar el uso de medios extraíbles y USB, deben tomarse decisiones avanzadas sobre qué medios USB se permiten, cuándo y dónde se pueden utilizar (en la red, fuera de la red o ambos) para garantizar que los usuarios cumplen con los objetivos y las políticas de seguridad.

Consulte el Manual del administrador para obtener una descripción completa de las políticas, valores predeterminados y opciones configurables.

Nota

Al utilizar Endpoint Encryption para administrar políticas y medios extraíbles:

- Pruebe y valide las plantillas de políticas antes de la distribución.
- Decida qué dispositivos USB están permitidos en las unidades USB y medios extraíbles, así como cuándo y dónde pueden utilizarse (en la red, fuera de la red o ambas), a fin de asegurarse de que los usuarios cumplen con las políticas.

Importancia de un programa piloto

Trend Micro recomienda ejecutar un programa piloto o realizar una implementación de prueba en un grupo reducido de usuarios antes de implementar en un público más amplio. Un programa piloto permite que una organización finalice la metodología de implementación que se utilizará al instalar Endpoint Encryption. Los programas piloto más eficaces requieren la participación de departamentos, usuarios de destino y dispositivos distintos. Por ejemplo, si la organización admite diez fabricantes de equipos portátiles diferentes, entonces, cada uno de estos dispositivos deberá incluirse en la prueba piloto. De forma similar, si ciertos grupos de alto perfil son de especial preocupación, uno o dos miembros del grupo se deberían inscribir para participar en la prueba piloto.

Consulte *Lista de comprobación piloto de Endpoint Encryption en la página A-1* para obtener más información.

Consideraciones sobre la administración de cambios

PolicyServer y las bases de datos relacionadas son servicios fundamentales. Las consideraciones sobre la administración de cambios son importantes para garantizar la disponibilidad para los usuarios finales que intentan autenticarse en la red en todo momento. Cuando son necesarios los cambios:

- Supervisar activamente el uso de la CPU y establecer un umbral para cuando se deba reiniciar el Servicio de Windows de PolicyServer.
- Reinicie el servicio con regularidad siguiendo una programación que se adapte a las ventanas de mantenimiento establecidas de la organización (diariamente, semanalmente, mensualmente).
- Reinicie el servicio PolicyServer de Windows siempre que se realice el mantenimiento en el servidor, la base de datos, las comunicaciones relacionadas o el entorno de Active Directory.
- Haga copias de seguridad regularmente de las bases de datos de PolicyServer, similares a las bases de datos empresariales críticas.

- Se recomienda hacer copias de segurida nocturnas de las bases de datos de registro y principales con almacenamiento fuera del sitio.

¡ADVERTENCIA!

Cualquier cambio en Active Directory o entornos de la base de datos pueden afectar a la conectividad con PolicyServer.

Comunicaciones de usuario final

Se debe avisar de antemano a los usuarios finales y proporcionarles un plan de comunicación inteligente para limitar el impacto y facilitar la transición. Asimismo, la comunicación posterior a la implementación juegan un papel importante para facilitar el ajuste de la utilización de Trend Micro Endpoint Encryption.

Preguntas para responder

Un obstáculo habitual en la adaptación en la empresa es la falta de comunicación. La necesidad de disponer de una comunicación de usuario final clara que aborde estas cuestiones es esencial para una implementación correcta:

1. ¿Por qué necesitamos Endpoint Encryption?
2. ¿Cómo ayuda Endpoint Encryption al usuario y a la organización?
3. ¿Qué cambiará?

Implementación de una estrategia de desarrollo por fases

Si su programa piloto se realizó correctamente, empiece a distribuir el programa por lotes de 25-50 clientes de punto final para comenzar la distribución de producción de la solución. Asegúrese de que los ingenieros de implementación se encuentran in situ con el primer grupo de implementación el día después de que se haya instalado la nueva solución, con el objeto de poder ofrecer ayuda instantánea. Siguiendo el éxito del lote inicial de clientes de punto final, implemente de 100 a 200 en una noche. A medida que la metodología de implementación se haya validado en el entorno de producción y los

equipos de TI interna y asistencia se hayan puesto de acuerdo, se podrán implementar de forma simultánea miles de dispositivos.

Permita a los usuarios saber qué, cuándo y por qué

Trend Micro recomienda que el patrocinador ejecutivo del proyecto de protección de datos envíe un mensaje a los usuarios finales para comunicar la importancia del proyecto a la empresa y los beneficios a los usuarios. Nuestra base de conocimiento tiene una serie de plantillas de comunicaciones de usuario final que se pueden aprovechar y personalizar para satisfacer las necesidades de comunicaciones antes de distribuir Endpoint Encryption.

Presentación de los cambios

1. Un mes antes de la implementación, haga que el patrocinador ejecutivo explique por qué se va a introducir un nuevo cifrado de software/hardware y cómo se beneficiarán tanto el usuario final como la empresa al aplicar los nuevos procesos.
2. Proporcione a los usuarios una cronología para la programación de la implementación, qué resultados esperar tras el primer día y confirme la forma en que los usuarios finales pueden obtener ayuda con el nuevo software.

Comunicarse una semana antes de la implementación

1. Reitere los cambios que se producirán y lo que puede esperar el día en el que sean necesarios nuevos procedimientos de autenticación para sus equipos, dispositivos móviles o medios extraíbles.
2. Incluya las capturas de pantalla e instrucciones detalladas sobre el nombre de usuario, las convenciones de la contraseña y otros servicios de asistencia internos.

Comunicación el día antes de la implementación

1. Vuelva a confirmar los intervalos de programación de la implementación, los posibles resultados y dónde obtener ayuda.

2. Distribuya hojas de referencia rápida, información de asistencia técnica y proporcione la información de contacto para el punto a domicilio que estará disponible para ayudar a los usuarios al día siguiente.

Comunicación tras la implementación

1. Reitere la información de asistencia técnica y proporcione la información de contacto para el punto a domicilio que estará disponible para ayudar a los usuarios al día siguiente.

2. Proporcione las herramientas de ayuda para solucionar el problema.

Escala: Requisitos de bases de datos de SQL y PolicyServer

A continuación se indican recomendaciones para cambiar la escala de una implementación de sitio único que ofrece una gama de opciones de hardware a tener en cuenta para la redundancia del sistema y el punto cero de error.

TABLA 2-5. Escala sin redundancia

DISPOSITIVOS	REQUISITOS MÍNIMOS	
	FRONT-END DE POLICYSERVER	BASE DE DATOS SQL DE POLICYSERVER
1,500	• El servidor desempeña varias funciones de base de datos y PolicyServer • Procesadores Intel™ Xeon™ Quad Core Core2 de 2 GHz • 8GB RAM • Espacio en disco duro RAID 5 de 120 GB	• Instalado en el host front-end de PolicyServer

Dispositivos	Requisitos mínimos	
	front-end de PolicyServer	Base de datos SQL de PolicyServer
3.000	• 1 host front-end de PolicyServer • Procesadores duales Intel™ Xeon™ Quad Core Core2 de 2 GHz • 4GB RAM • Espacio en disco duro RAID 1 de 40GB	• 1 host de base de datos SQL de PolicyServer • Procesadores Intel™ Xeon™ Quad Core Core2 de 2 GHz • 8GB RAM • Espacio en disco duro RAID 5 de 100GB

Tabla 2-6. Escala con alta disponibilidad y redundancia

Dispositivos	Requisitos mínimos	
	front-end de PolicyServer	Base de datos SQL de PolicyServer
10.000	• 2 host front-end de PolicyServer • Procesadores duales Intel™ Xeon™ Quad Core Core2 de 2 GHz • 4GB RAM • Espacio en disco duro RAID 1 de 40GB	• 1 host de base de datos SQL de PolicyServer • Procesadores Intel™ Xeon™ Quad Core Core2 de 2 GHz • 8GB RAM • Espacio en disco duro RAID 5 de 120 GB
20.000	• 4 host front-end de PolicyServer • Procesadores duales Quad Core2 Intel™ Xeon™ de 2 GHz • 4GB RAM • Espacio en disco duro RAID 1 de 40GB	• 1 host de base de datos SQL de PolicyServer • Procesadores Intel™ Xeon™ Quad Core2 de 2 GHz • 16GB RAM • Espacio en disco duro RAID 5 de 160GB

Dispositivos	Requisitos mínimos	
	front-end de PolicyServer	Base de datos SQL de PolicyServer
40.000	• 8 host front-end de PolicyServer • Procesadores duales Intel™ Xeon™ Quad Core Core2 de 2 GHz • 4GB RAM • Espacio en disco duro RAID 1 de 40GB	• 2 host de clústeres de base de datos SQL de PolicyServer • Procesadores Intel™ Xeon™ Quad Core Core2 de 2 GHz • 16GB RAM • Espacio en disco duro RAID 5 de 320GB

Tabla 2-7. Escala con un único punto de error cero

Dispositivos	Requisitos mínimos	
	front-end de PolicyServer	Base de datos SQL de PolicyServer
10.000	• 2 host front-end de PolicyServer • Procesadores Intel™ Xeon™ Quad Core Core2 de 2 GHz • 4GB RAM • Espacio en disco duro RAID 1 de 40GB **Nota** El hardware virtualizado es compatible con la infraestructura virtual de VMware.	• 2 host de base de datos SQL de PolicyServer • Procesadores duales Intel™ Xeon™ Quad Core Core2 de 2 GHz • 8GB RAM • Espacio en disco duro RAID 5 de 60GB • RAID 5 de 130 GB compartido con espacio de disco duro de SAN **Nota** Microsoft o VMware en hardware virtualizado no admite el servicio de clústeres de Microsoft.

Dispositivos	Requisitos mínimos	
	front-end de PolicyServer	Base de datos SQL de PolicyServer
20.000	• 4 host front-end de PolicyServer • Procesadores duales Intel™ Xeon™ Quad Core Core2 de 2 GHz • 4GB RAM • Espacio en disco duro RAID 1 de 40GB **Nota** El hardware virtualizado es compatible con la infraestructura virtual de VMware.	• 2 host de base de datos SQL de PolicyServer • Procesadores duales Intel™ Xeon™ Quad Core Core2 de 2 GHz • 8GB RAM • Espacio en disco duro RAID 5 de 60GB • RAID 5 de 180GB compartido con espacio de disco duro de SAN **Nota** Microsoft o VMware en hardware virtualizado no admite el servicio de clústeres de Microsoft.

Dispositivos	Requisitos mínimos	
	front-end de PolicyServer	Base de datos SQL de PolicyServer
40.000	• 8 host front-end de PolicyServer • Procesadores duales Intel™ Xeon™ Quad Core Core2 de 2 GHz • 4GB RAM • Espacio en disco duro RAID 1 de 40GB **Nota** El hardware virtualizado es compatible con la infraestructura virtual de VMware.	• 4 host de base de datos SQL de PolicyServer • Procesadores duales Intel™ Xeon™ Quad Core Core2 de 2 GHz • 16GB RAM • Espacio en disco duro RAID 5 de 60GB • RAID 5 de 350GB compartido con espacio de disco duro de SAN **Nota** Microsoft o VMware en hardware virtualizado no admite el servicio de clústeres de Microsoft.

Ejemplo de escala

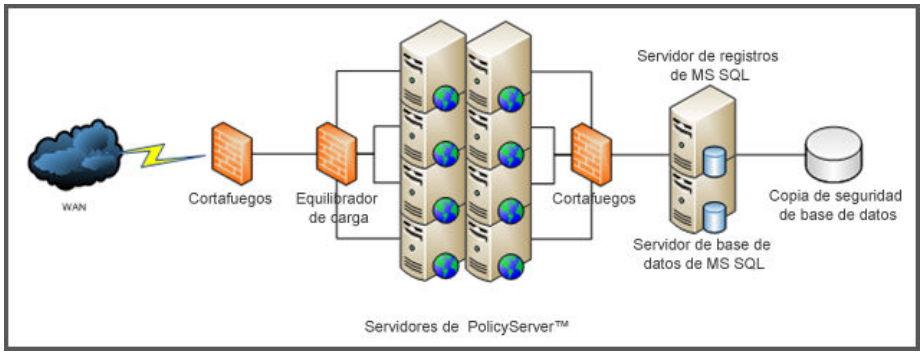


FIGURA 2-1. PolicyServer se ha ampliado para admitir 40.000 usuarios

Capítulo 3

Instalación de PolicyServer

En este capítulo se proporciona una visión general de los archivos y carpetas necesarios para instalar PolicyServer y el proceso de instalación.

Este capítulo describe los siguientes temas:

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.

Contenido de la carpeta de instalación

La carpeta de instalación de Trend Micro PolicyServer contiene los siguientes archivos de instalación para la empresa:

- `PolicyServerMMCSnapinSetup.msi`
- `PolicyServerInstaller.exe`
- `LDAProxyInstaller.exe`
- Herramientas

También se necesita el siguiente archivo:

- El archivo de texto de licencia y el código de desbloqueo (contraseña) recibido de Trend Micro. Use el archivo de licencia y el código de desbloqueo para iniciar sesión en MMC de PolicyServer por primera vez.

Nota

PolicyServer 3.1.3 incluye una licencia de prueba de 30 días. Para obtener más información sobre la licencia de prueba, consulte *Instalación de los servicios Web y de la base de datos de PolicyServer en la página 3-7*.

Requisitos de PolicyServer

En esta sección se describen los requisitos para PolicyServer, incluidos los requisitos de software y hardware, los archivos necesarios para ejecutar las instalaciones y también las cuentas necesarias para configurar la base de datos y los entornos de servidor de Windows.

Requisitos de hardware

Al instalar PolicyServer, se recomienda tener al menos dos servidores dedicados:

1. Un servidor para la base de datos dedicado, o agregar la base de datos a un clúster de SQL existente.
2. Un servidor dedicado para el servicio Web o el servicio de PolicyServer.

Nota

El hardware virtualizado es compatible con la infraestructura virtual de VMware.

TABLA 3-1. 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

Requisitos de software

TABLA 3-2. 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.

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 3-3. Consideraciones de software para Windows Server 2008 y 2008 R2

Server OS	2008	2008 R2

Funciones	• Instalar el rol del servidor de aplicaciones • Agregar compatibilidad IIS • Instalar el rol de servidor web	• Instalar el rol del servidor de aplicaciones • Agregar compatibilidad IIS • Instalar el rol de servidor web
Características	• Agregar SMTP	• Agregar SMTP
Otros requisitos previos	• .NET 3.5 SP1	• Debe instalarse SQL 2008 SP1 para ejecutar SQL 2008 • No se requiere la actualización de .NET

Archivos de instalación necesarios

TABLA 3-4. Archivos necesarios para instalar PolicyServer

ARCHIVO	OBJETIVO
`PolicyServerInstaller.exe`	Instale los servicios y bases de datos de PolicyServer
`PolicyServerMMCSnapinSetup.msi`	Instale la consola de administración de PolicyServer como un complemento de MMC
Licencia	Proporcionado por Trend Micro. Necesario para la autenticación de MMC de PolicyServer por primera vez

Importante

Copie todos los archivos de instalación en la unidad local antes de la instalación.

Cuentas necesarias

Para instalar PolicyServer, deben estar disponibles ciertas cuentas. La tabla siguiente explica la cuenta, el servicio al que está asociado y cómo utiliza PolicyServer la cuenta.

TABLA 3-5. Cuentas necesarias para instalar PolicyServer

CUENTA	SERVICIO	OBJETIVO
SA de SQL	Programa instalador de PolicyServer	Cuenta utilizada SOLO cuando se crean las bases de datos de PolicyServer.
MADB de SQL	Servicio de Windows de PolicyServer	Cuenta creada durante la instalación para autenticar las bases de datos de PolicyServer.
Cuenta de servicio	Servicio de Windows de PolicyServer y IIS	Cuenta utilizada para ejecutar el grupo de aplicaciones Servicio Web y Servicio de Windows de PolicyServer.
Administrador de empresa de PolicyServer	PolicyServer MMC	Cuenta proporcionada por Trend Micro (desde el archivo de licencia) que se requiere para autenticarse en MMC de PolicyServer por primera vez.

Proceso de instalación de PolicyServer

Instale Microsoft SQL Server™ antes de ejecutar ningún archivo de instalación de PolicyServer. Los instaladores para cada aplicación de PolicyServer están configurados para que la instalación sea sencilla y simple.

Este proceso de instalación:

1. Instale la base de datos de Microsoft SQL.

Nota

Este documento no explica cómo instalar Microsoft SQL.

2. Instale los servicios y la base de datos de PolicyServer.
3. Instale MMC de PolicyServer.

Instalación de los servicios Web y de la base de datos de PolicyServer

Antes de empezar

Microsoft SQL Server debe estar configurado.

El programa instalador de PolicyServer configura las opciones de base de datos e instala los servicios de Windows. En PolicyServer 3.1.3, ahora puede especificar un número de puerto para el servicio Web de PolicyServer. Ahora es necesario también un segundo puerto para el servicio Web del cliente. Si no existe un segundo puerto, se creará un nuevo puerto durante el proceso de instalación. Para obtener más información sobre la nueva arquitectura, consulte *Componentes de Endpoint Encryption en la página 1-2*.

Para poder utilizar Endpoint Encryption durante un período de prueba limitado, el nombre de la empresa y la cuenta de administrador de empresa se pueden configurar durante el proceso de instalación. PolicyServer funciona normalmente con todas las aplicaciones cliente, con un número ilimitado de dispositivos y con hasta 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 y dispositivos podrán seguir iniciando sesión una vez finalizado el período de prueba.

Procedimiento

1. Ejecute `PolicyServerInstaller.exe`.
2. Lea detenidamente el Contrato de licencia para usuario final. Si está de acuerdo, haga clic en **Aceptar**.
3. En la pantalla de **PolicyServer Services**, compruebe la versión de PolicyServer y, a continuación, haga clic en **Instalar**.
4. En la pantalla de **Inicio de sesión del servicio de Windows**, la configuración predeterminada es la adecuada para la mayoría de la instalaciones. Haga clic en **Continuar**.

5. En la pantalla de **Inicio de sesión del administrador de la base de datos**, introduzca la dirección IP o el nombre de host de Microsoft SQL Server, así como las credenciales de una cuenta con la función sysadmin para la instancia de SQL especificada.

   Nota

   Para entornos con varias instancias de SQL Server, añada la instancia de SQL al final del nombre de host de PolicyServer o de la dirección IP utilizada. Utilice la sintaxis siguiente para especificar una instancia:

   ```
   <nombre de host o dirección IP>\<instancia de la base de datos>
   ```

   El instalador verifica la conexión de la base de datos.

6. En la pantalla de **Inicio de sesión de Crear base de datos**, introduzca las credenciales de una cuenta para que el servicio de Windows de PolicyServer utilice en todas las transacciones de datos. Si es la primera vez que se instala PolicyServer, se creará la cuenta especificada.

7. En la pantalla **Ubicación de instalación del servicio Web**, especifique el sitio de IIS que PolicyServer MMC y el servicio Web del cliente utilizan para comunicarse con PolicyServer. El número de puerto predeterminado es 8080. Si el puerto 8080 está en uso, entonces se asignará el siguiente puerto disponible.

   a. Seleccione un sitio desde el menú desplegable **Sitio de destino**.

   b. Revise el puerto asignado actualmente y, si fuera necesario, especifique un número de puerto diferente en el campo **Nuevo puerto**.

      Nota

      Trend Micro recomienda reservar el puerto 80 para el servicio Web del cliente.

   c. Haga clic en **Continuar**.

8. El siguiente paso se ha diseñado para configurar el servicio Web del cliente, que es el sitio de IIS que todos los clientes de Endpoint Encryption utilizan para comunicarse con PolicyServer. En función de si está disponible una segunda ubicación de IIS, se mostrará una de las siguientes pantallas:

- Si está disponible una segunda ubicación de IIS, se mostrará la pantalla **Ubicación del servicio Web cliente**.

  a. Seleccione un sitio desde el menú desplegable **Sitio de destino**.

  b. Revise la asignación del puerto predeterminado para el servicio Web del cliente.

  > **Nota**
  >
  > Trend Micro recomienda mantener el número de puerto 80. Sin embargo, si fuera necesario, especifique un número de puerto diferente en el campo **Nuevo puerto**. El número de puerto debe ser un número entero positivo entre 1 y 65535.

  c. Haga clic en **Continuar**.

- Si no está disponible un segundo sitio de IIS, se mostrará la pantalla **Crear ubicación del servicio Web cliente**, desde la que podrá configurar una nueva ubicación de IIS.

  a. Especifique un nombre para la ubicación de IIS en el campo **Nombre del sitio**.

  b. Desplácese hasta la ubicación del sitio. Si no existe ninguna carpeta, cree una nueva.

  c. Especifique la dirección IP y el número de puerto para la nueva ubicación de IIS.

  > **Nota**
  >
  > Trend Micro recomienda mantener el número de puerto 80. Sin embargo, si fuera necesario, especifique un número de puerto diferente. El número de puerto debe ser un número entero positivo entre 1 y 65535.

  d. Haga clic en **Continuar**.

9. En la pantalla **Ubicación de instalación del servicio Web móvil**, revise la configuración y, a continuación, haga clic en **Continuar**.

10. En la pantalla **Crear cuentas de inicio de sesión de nombre y administrador de empresa**, especifique el nuevo nombre de empresa y las credenciales para una

cuenta de administrador de empresa utilizados para administrar PolicyServer durante el período de prueba inicial.

11. Haga clic en **Continuar**.

    Se inicia el proceso de instalación.

12. En el mensaje **Instalación de PolicyServer**, haga clic en **Aceptar**.

13. Haga clic en **Finalizado**.

14. En la ventana del programa instalador de PolicyServer, haga clic en **Salir**.

15. Reinicie el servidor.

PolicyServer MMC

Microsoft Management Console (MMC) de PolicyServer es la interfaz que utilizan los administradores para PolicyServer. MMC de PolicyServer combina una estructura jerárquica con roles de administrador y autenticador independientes que permiten a las organizaciones distribuir la responsabilidad administrativa al tiempo que mantienen un control centralizado.

MMC de PolicyServer administra:

- Todas las aplicaciones de Trend Micro Endpoint Encryption
- Usuarios y grupos de PolicyServer (incluidos los grupos sin conexión)
- Dispositivos de cliente, incluidos los equipos portátiles, ordenadores de sobremesa, dispositivos PDA, smartphones y de almacenamiento USB
- Todas las políticas, incluyendo el cifrado, la complejidad de contraseñas y la autenticación
- Registros de sucesos para ver los sucesos de autenticación, eventos de administración, el estado de cifrado del dispositivo y las violaciones de seguridad
- Proceso de restablecimiento de contraseña de ayuda remota
- Funcionalidad de bloqueo/eliminación de dispositivo

Además, PolicyServer ofrece beneficios medibles a través de las opciones de auditoría y creación de informes, que permiten a los ejecutivos de la empresa y otros cargos medir el éxito.

Para obtener una descripción detallada de la funcionalidad de MMC de PolicyServer, consulte el Manual del administrador de Endpoint Encryption.

Instalación de MMC de PolicyServer

Procedimiento

1. Ejecute `PolicyServerMMCSnapinSetup.msi`.

   Comienza la instalación.

2. Haga clic en **Siguiente** para abrir el cuadro de diálogo de bienvenida del asistente de instalación de MMC de PolicyServer.

3. Lea detenidamente el contrato de licencia, seleccione **Acepto** si acepta los términos y, a continuación, haga clic en **Siguiente**.

4. Seleccione la carpeta de instalación o deje la ubicación predeterminada y haga clic en **Siguiente**.

5. Haga clic en **Siguiente** para confirmar la instalación.

   Se inicia el proceso de instalación. Se crea un nuevo acceso directo de MMC de PolicyServer en el escritorio.

6. Haga clic en **Cerrar** para finalizar la instalación.

7. Haga clic en **Sí** para reiniciar el servidor.

8. Tras iniciar sesión en el servidor, abra MMC de PolicyServer desde el acceso directo del escritorio.

9. Cuando se abra la interfaz MMC de PolicyServer, realice una de las acciones siguientes:

   - Iniciar sesión con el nombre de empresa y la cuenta de administrador de empresa creada durante la instalación de los servicios y las bases de datos de

PolicyServer. El período de prueba de 30 días permite un número ilimitado de dispositivos y hasta 100 usuarios.

- Importar un archivo de licencia:

Nota

Para obtener el archivo de licencia, póngase en contacto con el servicio de asistencia de Trend Micro.

a. Vaya a **Archivo** > **Importar licencia**.

b. Especifique el código de desbloqueo, busque el archivo de licencia y, a continuación, haga clic en **Actualizar**.

c. Haga clic en **Aceptar** cuando aparezca la ventana **La licencia se ha actualizado correctamente**.

Ha finalizado la instalación de PolicyServer. Autentique MMC de PolicyServer con las credenciales de administrador de empresa enviadas por Trend Micro.

Qué hacer a continuación

1. Cree una cuenta de administrador de empresa de copia de seguridad y cambie la contraseña predeterminada.
2. Habilite las aplicaciones que se utilizarán en la empresa antes de la creación de los grupos de implementación de producción o prueba.
3. Consulte el Manual del administrador de Endpoint Encryption para las tareas adicionales posteriores a la instalación como la creación de dispositivos y usuarios y la configuración de políticas.

Sincronización de AD de PolicyServer

PolicyServer admite la sincronización de Active Directory (AD) para un grupo de PolicyServer configurado. La sincronización agregará y eliminará automáticamente los usuarios de AD de los grupos de PolicyServer configurados.

Información general sobre Active Directory

Para habilitar la sincronización de AD de PolicyServer se necesitan tres componentes:

1. Un dominio de AD configurado.
2. Un grupo de PolicyServer configurado para señalar a una unidad organizativa (OU) de AD válida.
3. Credenciales de acceso al dominio de AD correspondientes que coincidan con el nombre distintivo del grupo de PolicyServer.

Cuando está configurada correctamente, la sincronización crea automáticamente nuevos usuarios de PolicyServer y los mueve a los grupos emparejados correspondientes de PolicyServer. Durante la sincronización, PolicyServer se actualiza para reflejar los usuarios actuales y las asignaciones de grupo para grupos emparejados.

Si se agrega un nuevo usuario al dominio y se coloca en la unidad organizativa, se marcará para que durante la siguiente sincronización, AD lo cree en PolicyServer y, a continuación, lo mueva a los grupos emparejados correspondientes de PolicyServer.

Si se elimina un usuario de AD, este se eliminará automáticamente del grupo emparejado de PolicyServer y de la empresa.

Los administradores de PolicyServer pueden crear sus propios usuarios para agregarlos a los grupos emparejados de PolicyServer sin que el sistema de sincronización los modifique. Esto permite a los administradores agregar usuarios que no sean del dominio a grupos que se sincronizan con él.

Si un administrador de PolicyServer elimina manualmente un usuario de dominio de un grupo emparejado en PolicyServer, el sistema de sincronización no lo volverá a agregar automáticamente. Esto impide que se reemplace la acción del administrador para ese usuario. Si un administrador mueve manualmente un usuario del dominio sincronizado de nuevo a un grupo emparejado, el sistema de sincronización comenzará nuevamente a mantener al usuario en el grupo automáticamente.

Configuración de Active Directory

Esta tarea presupone que el controlador de dominio está configurado en Windows Server 2003 y que AD está instalado.

Procedimiento

1. Vaya a **Inicio** > **Programas** > **Herramientas administrativas** > **Usuarios y equipos de Active Directory** para abrir la configuración de AD.

   Se abre Usuarios y equipos de Active Directory.

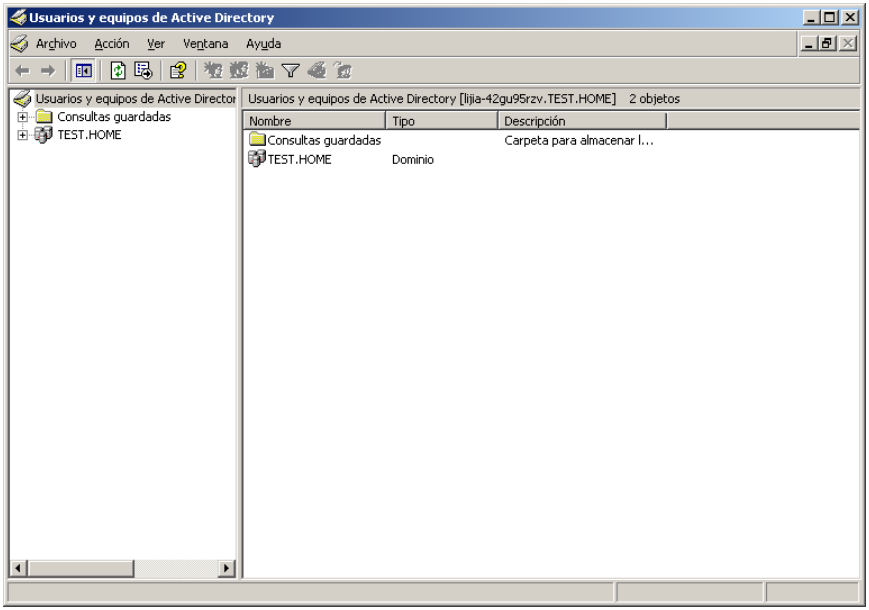


FIGURA 3-1. Usuarios y equipos de Active Directory

2. Haga clic con el botón derecho en el nuevo dominio que se creó al instalar AD y seleccione **Nuevo**

3. Seleccione **Unidad organizativa**.

4. Haga clic en **Siguiente**.

5. En la pantalla **Nuevo objeto - Unidad organizativa**, especifique el nuevo nombre y haga clic en **Aceptar**.

   El nuevo grupo aparece en la navegación izquierda bajo el dominio.

El nuevo grupo se utilizará para sincronizar con un grupo de PolicyServer, pero primero se deben agregar los usuarios al grupo.

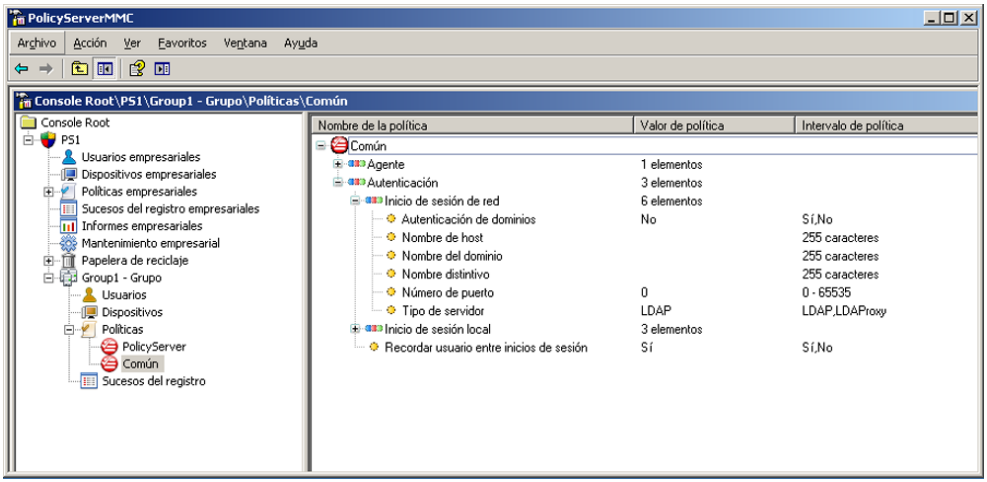
6. Haga clic en el nuevo grupo y seleccione **Nuevo usuario**.
7. En la pantalla **Nuevo objeto - Usuario**, especifique la información de cuenta del nuevo usuario y haga clic en **Siguiente**.
8. Especifique y confirme la contraseña de dominio del nuevo usuario y haga clic en **Siguiente** para continuar

Nota

Desactive la opción **El usuario debe cambiar la contraseña en el siguiente inicio de sesión** y seleccione la opción **La contraseña nunca caduca** para simplificar otras pruebas posteriormente.

9. Cuando se le pregunte si desea finalizar, haga clic en **Finalizar**.

   El controlador de dominio está configurado con una nueva unidad organizativa y un usuario en ese grupo. Para sincronizar ese grupo con PolicyServer, instálelo y cree un grupo para la sincronización. En esta sección se presupone que PolicyServer ya está instalado.
10. Inicie sesión en la MMC de PolicyServer.
11. Haga clic con el botón derecho en la empresa y seleccione **Crear grupo de nivel superior**.
12. Especifique el nombre y descripción del grupo y, a continuación, haga clic en **Aplicar**.
13. Para configurar la directiva de sincronización, abra el grupo y vaya a **Común** > **Autenticación** > **Inicio de sesión de red**.



14. Abra **Nombre distintivo** y especifique el nombre distintivo de la organización de AD configurada para sincronizarse con este grupo y haga clic en **Aceptar**.

Nota

El formato para el nombre distintivo de una unidad organizativa denominada Ingeniería del dominio denominado test.home es:
`OU=Engineering,DC=TEST,DC=HOME`

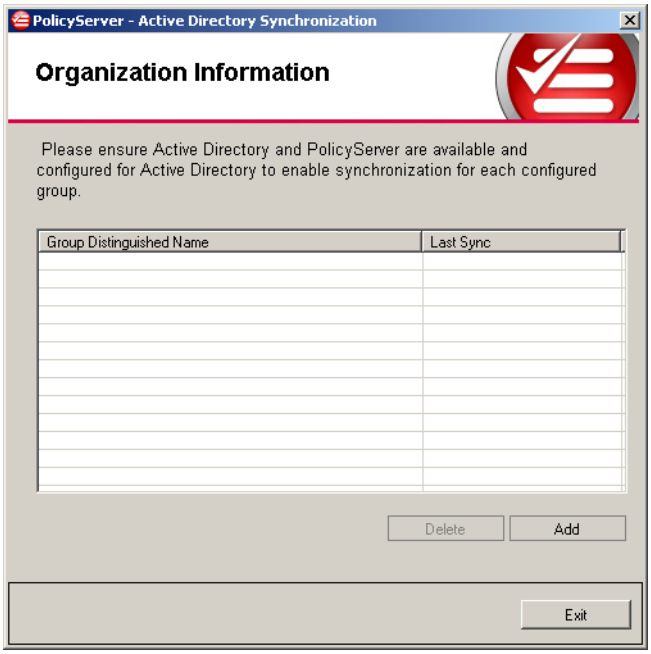
---

15. Abra **Nombre de dominio** y especifique el nombre de dominio NetBIOS que se usó para configurar el servidor de AD.

Una vez configurada la política de PolicyServer, la configuración final necesaria es crear la configuración de sincronización a través de la herramienta de configuración de sincronización de AD. Esta herramienta permite a los administradores crear credenciales independientes de AD para cada unidad organizativa y cada controlador de dominio sincronizados.

16. Para acceder a la herramienta **Configuración de sincronización de AD**, vaya a la carpeta de instalación del Servidor de políticas y abra **ADSyncConfiguration.exe**.

Se abre la herramienta de sincronización de AD de PolicyServer



17. Haga clic en **Agregar** para especificar las credenciales para la unidad organizativa de AD.

Nota

Para los servidores que requieren credenciales adicionales, los usuarios pueden introducir el nombre de usuario administrativo apropiado y la contraseña correspondientes para conectarse al controlador de dominio a través de esta herramienta.

18. Salga de la herramienta **ADSyncConfiguration**.

La sincronización entre AD y PolicyServer ha finalizado. La sincronización se llevará a cabo automáticamente cada 45 minutos (este es el intervalo de sincronización predeterminado que utilizan los controladores de dominio de Microsoft). Puede forzar la sincronización deteniendo y reiniciando el servicio de Windows de PolicyServer; la

sincronización del dominio se ejecutará poco después del inicio del servicio de Windows de PolicyServer y, a continuación, se ejecutará cada 45 minutos después de esta acción.

Proxy LDAP opcional

El proxy LDAP opcional permite la autenticación de dominio/el inicio de sesión único (SSO) a través de un servidor proxy externo ubicado en el cliente DMZ.

Nota

- La instalación del proxy LDAP se necesita para entornos alojados que usen autenticación de dominio/SSO.
- Ya no se admiten las versiones del proxy LDAP anteriores a 3.1.
- Los clientes existentes que utilicen el proxy LDAP deben actualizarse a la versión 3.1.

Requisitos de LDAP

TABLA 3-6. Especificaciones de software y de hardware de LDAP

EVENTO	REQUISITO
Procesador	Intel™ Core™ 2 o procesador compatible.
Memoria	• Mínimo: 2GB
Espacio en disco	• Mínimo: 30GB • Necesario: 20% de espacio libre en disco

Evento	Requisito
Conectividad de red	• El servidor debe estar en el dominio con acceso a Active Directory • El servidor debe tener una dirección que sea accesible a través de Internet • Se debe permitir el proxy entrante • PolicyServer debe tener acceso al servidor IIS de este servidor
Sistemas operativos	• Windows Server 2003 de 32/64 bits • Windows Server 2008 o 2008 R2 de 32/64 bits

Aplicaciones y configuración	• Rol de servidor de aplicaciones
	  • IIS
	  • Permitir las páginas Active Server
	  • Permitir ASP.NET
	• .Net Framework 2.0 SP2

Lista de comprobación de hardware del servidor proxy LDAP

Tabla 3-7. Lista de comprobación de hardware del servidor proxy LDAP

Servidor proxy LDAP		Comentarios
Información de Windows Server	Versión del SO	
	Nivel de Service Pack	
Información de hardware	Crear	
	RAM	
	Modelo	
	CPU	

SERVIDOR PROXY LDAP		COMENTARIOS
Software de servidor instalado	IIS	
	Microsoft .NET SP 2.0 Sp1 o posterior	
Información de la red	Dirección IP	
	Máscara de subred	
	Nombre de host	
	Nombre del dominio	
	Credenciales de dominio disponibles (solo para SSO)	

Capítulo 4

Instalación del cliente de cifrado de punto final

Todas las aplicaciones de Endpoint Encryption tienen unos requisitos únicos de sistema e instalación. Para obtener explicaciones detalladas de aplicaciones de punto final sobre configuración y uso, consulte el Manual del administrador de Endpoint Encryption.

Este capítulo aborda los siguientes temas:

Consideraciones previas a la instalación

Antes de continuar, tenga en cuenta lo siguiente:

- Copie todos los archivos de instalación de cliente de punto final al dispositivo.
- Todas las aplicaciones cliente de punto final requieren Microsoft .NET Framework 2.0 SP1 o versiones posteriores.

> **Nota**
>
> Para instalar clientes de punto final en Windows 8, es necesaria la compatibilidad con Microsoft .NET Framework 3.5.

- Las instalaciones de Full Disk Encryption y FileArmor se pueden automatizar.
- Se necesitan privilegios administrativos para todas las instalaciones del producto.

Para obtener información detallada acerca de las plataformas compatibles y otras consideraciones previas a la implementación, consulte *Plataformas admitidas y lista de comprobación previa a la implementación en la página 2-3*.

Instalación de Full Disk Encryption

Full Disk Encryption está diseñado para proporcionar 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. La autenticación segura de arranque previo restringe el acceso al sistema operativo host vulnerable hasta que el usuario se valide.

Opciones previas a la implementación

Para minimizar el impacto del usuario final y simplificar la implementación masiva, deshabilite temporalmente el cifrado de la unidad. Una vez que se confirme la

compatibilidad, el cifrado se puede volver a activar como parte de la distribución del producto estándar.

TABLA 4-1. Activar o desactivar el cifrado del dispositivo

OPCIONES DE CONFIGURACIÓN	OPCIONES	RUTA DE POLICYSERVER
Cifrado del dispositivo	Sí/No	**Full Disk Encryption** > **Equipo** > **Cifrado** > **Cifrar dispositivo**

Lista de comprobación previa a la instalación

El instalador de Full Disk Encryption comprueba el sistema de destino para asegurarse de que se cumplen todos los requisitos de sistema necesarios antes de instalar la aplicación. Para obtener información adicional, consulte el archivo `PreInstallCheckReport.txt` situado en el directorio de instalación después de ejecutar el instalador.

Para obtener información detallada sobre la comprobación y los requisitos del sistema, consulte *Lista de comprobación previa a la instalación de Full Disk Encryption en la página C-1*

Requisitos del sistema de Full Disk Encryption

Esta sección describe los requisitos mínimos y recomendados del sistema necesarios para instalar Full Disk Encryption.

TABLA 4-2. 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

EVENTO	REQUISITO
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)
Otro software	Requisitos adicionales para Windows 8: • Microsoft .NET Framework 3.5 está activado • Para dispositivos con UEFI, consulte *Preparación del dispositivo en la página 4-5* para 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.

Preparación de la unidad de disco duro

Full Disk Encryption cifra todos los sectores de la unidad física. Dado que muchas aplicaciones, incluido el sistema operativo, no utilizan el espacio de disco duro físico completo, los sectores pueden estar dañados o la unidad puede estar muy fragmentada.

Nota

Trend Micro recomienda hacer a una pequeña prueba piloto de instalaciones y actualizaciones nuevas antes de implementar la última compilación de Full Disk Encryption. Si tiene preguntas o necesita asistencia técnica, póngase en contacto con Asistencia de Trend Micro.

Preparación del dispositivo

Procedimiento

1. Desconecte todos los dispositivos de almacenamiento USB. Puede volver a conectarlos después de la instalación.
2. Asegúrese de que la unidad con el sistema operativo ya no está cifrada y de que se ha desactivado el cifrado de Bitlocker.
3. Para dispositivos de Windows 8 compatibles con BIOS UEFI, cambie la prioridad de arranque a **Primero heredado**.
   a. Desde Windows 8, mantenga pulsada la tecla MAYÚS y reinicie el dispositivo.

      El dispositivo se reinicia y se carga la BIOS UEFI.
   b. Haga clic en el panel **Solucionar problemas**.

      Aparecerá la pantalla **Opciones avanzadas**.
   c. Haga clic en el mosaico **Configuración del firmware UEFI**.

      Si no existe el mosaico **Configuración del firmware UEFI**, el dispositivo no utiliza UEFI y no es necesario realizar ningún cambio.
   d. Establezca **UEFI/Prioridad de arranque heredado** en **Primero heredado**.
   e. Reinicie el dispositivo.

Preparación de la unidad

Procedimiento

1. Ejecute la utilidad de desfragmentación de Windows en la unidad del sistema.
2. Compruebe que la unidad del sistema tiene al menos 256MB de espacio libre contiguo.
3. Ejecute la utilidad de integridad de disco de Windows (requiere reinicio).
   a. Mediante una secuencia de comandos o el símbolo del sistema, ejecute `chkdsk /f /r` y programe la comprobación de disco después del siguiente reinicio del sistema.
   b. Arranque el dispositivo.
   c. Sustituya la unidad si chkdsk informa de varios sectores defectuosos.
4. Compruebe el disco para realizar un registro de arranque maestro (MBR) normal y confirme que hay un sector de inicio normal en la partición de inicio. Por ejemplo, un equipo de inicio dual tiene un sector de inicio modificado.

   Nota
   GPT no se admite actualmente.

5. Copie el software de instalación de Full Disk Encryption en la unidad del sistema de Windows.

Notas importantes para DataArmor SP7 y versiones anteriores

- Service Pack 6 y versiones anteriores:
  - En la BIOS, compruebe que el controlador de disco está establecido en el modo AHCI o ATA.
  - Para equipos portátiles acoplados, instale el software mientras se desacopla de varias plataformas.

- Intel™Rapid Recovery Technology (IRRT):
  - Algunos sistemas más recientes son compatibles con IRRT de la BIOS.
  - Si la controladora de disco de la BIOS está configurada en el modo IRRT, se deberá cambiar al modo AHCI antes de la instalación de Full Disk Encryption.
  - El SO debe ser compatible con IRRT.
- Software Intel™Matrix Manager:
  - De forma predeterminada, Windows XP no tiene instalado el software Intel Matrix Manager. Debe realizar la configuración en la BIOS sin una reconstrucción del sistema operativo.
  - Windows Vista tiene el software Intel Matrix Manager de forma predeterminada.

Nota

Si se cambia la configuración de funcionamiento de SATA en Windows VISTA y está instalado Full Disk Encryption, Windows no se iniciará. Vuelva a cambiar a IRRT y Vista se cargará normalmente.

Instalación de Full Disk Encryption

En esta sección se describe cómo instalar Full Disk Encryption en Windows.

Tipos de instalación

El tipo de instalación de Full Disk Encryption puede ser administrada o no administrada, según las necesidades particulares de la empresa.

Tipo	Detalles
Administrado	• PolicyServer administra las políticas de autenticación y cifrado. • Tipo de instalación más común para los dispositivos conectados normalmente a PolicyServer.
No administrado	• Las políticas de autenticación y cifrado se administran directamente con Full Disk Encryption y la consola de recuperación. • Adecuado para los dispositivos que no se administran centralmente mediante PolicyServer.

Opciones de instalación

Instale Full Disk Encryption manualmente o compile secuencias de comandos para automatizar las tareas de instalación.

Tabla 4-3. Opciones de instalación de Full Disk Encryption

Opción	Detalles
Automatizada	• Requiere software de administración del sistema: Tivoli, SMS/SCCM o LANDesk y una secuencia de comandos de instalación. • Se recomienda un método para empresas con un gran número de puntos finales.
Manual	• Instalación sencilla directamente desde Windows, ya sea mediante el instalador gráfico o la línea de comandos. • Adecuado para pequeñas empresas, implementaciones de prueba o instalaciones individuales.

Instalación automatizada

La instalación de Full Disk Encryption mediante secuencias de comandos automatiza el proceso y facilita la tarea de distribuir el software en toda la empresa. Consulte *Uso de*

secuencias de comandos para automatizar las instalaciones en la página 4-20 para obtener más información.

Instalación administrada

Una instalación administrada de Full Disk Encryption es el tipo de instalación más común para los dispositivos conectados normalmente a PolicyServer. PolicyServer administra las políticas de autenticación y cifrado. Esta sección describe los pasos de instalación básicos para un cliente de punto final administrado.

Antes de continuar, asegúrese de:

- Revisar *Requisitos del sistema de Full Disk Encryption en la página 4-3*
- Consulte *Preparación de la unidad de disco duro en la página 4-4*

¡ADVERTENCIA!

Una preparación insuficiente de la unidad de disco duro y de la instalación del sistema puede dar lugar a la pérdida de datos irreversible.

Requisitos

Los siguientes requisitos son necesarios para las instalaciones administradas:

- El cliente se conecta a PolicyServer durante la instalación.
- PolicyServer se debe configurar con una empresa, un nombre de host y una dirección IP.

Nota

Trend Micro recomienda utilizar el nombre de dominio completo de PolicyServer. Si cambia el nombre de host o la dirección IP de PolicyServer, no necesitará actualizar manualmente cada cliente.

- La cuenta de usuario debe pertenecer a un grupo de PolicyServer y tener permisos para agregar dispositivos a este grupo.

¡ADVERTENCIA!

Las cuentas de autenticador o administrador de empresa de PolicyServer no pueden utilizarse para instalar Full Disk Encryption.

- La cuenta de instalación debe tener privilegios de administrador local.
- Si la autenticación de dominio/inicio de sesión único está activada, el nombre de usuario debe coincidir con Active Directory. La contraseña de Active Directory se utiliza en su lugar.

Instalación de Full Disk Encryption como cliente administrado

Revise los requisitos del sistema antes de instalar Full Disk Encryption como cliente administrado. Para conocer más detalles, consulte *Requisitos del sistema de Full Disk Encryption en la página 4-3*. Después de instalar Full Disk Encryption, el equipo se reinicia en el caso del cifrado basado en software o se apaga en el caso del cifrado basado en hardware.

Nota

El usuario responsable de la instalación no puede ser una cuenta de autenticador o administrador de empresa.

Procedimiento

1. Copie el paquete de instalación de Full Disk Encryption en el disco duro local.
2. Ejecute `TMFDEInstall.exe`.

   Nota

   Si se muestra la ventana **Control de cuentas de usuario**, haga clic en **Sí** para permitir que el instalador realice cambios en el dispositivo.

   Aparecerá la ventana de bienvenida del instalador.
3. Seleccione **Instalación administrada** y haga clic en **Siguiente**.

   Se muestra la pantalla **Instalación administrada**.

4. Especifique las credenciales, la dirección de PolicyServer y la empresa y, a continuación, haga clic en **Siguiente**.

   Comienza la instalación de Full Disk Encryption. El programa se cierra una vez finalizada la instalación, que puede tardar varios minutos.

Consejo

Si se produce un error durante la instalación administrada, utilice el ID de dispositivo situado en la esquina inferior derecha de la pantalla del instalador para comprobar si el dispositivo ya existe en PolicyServer. El ID de dispositivo solo aparece tras producirse un error en la instalación.

5. En la pantalla de confirmación, haga clic en **Sí** para reiniciar o apagar el dispositivo.

   La instalación de Full Disk Encryption se completa cuando se muestra el arranque previo. El cifrado de disco comienza después de iniciar Windows.

Qué hacer a continuación

Una vez cargado el arranque previo de Full Disk Encryption, el usuario debe iniciar sesión para obtener acceso a Windows. Si la política así lo establece, es posible que el usuario tenga que cambiar la contraseña después de iniciar sesión.

Instalación no administrada

Una instalación no administrada de Full Disk Encryption es similar a una instalación administrada, excepto en que las credenciales de usuario y las políticas son solo para el dispositivo cliente.

Instalación de Full Disk Encryption como cliente no administrado

Revise los requisitos del sistema antes de instalar Full Disk Encryption como cliente administrado. Para conocer más detalles, consulte *Requisitos del sistema de Full Disk Encryption en la página 4-3*. Después de instalar Full Disk Encryption, el equipo se reinicia en el caso del cifrado basado en software o se apaga en el caso del cifrado basado en hardware.

Procedimiento

1. Copie el paquete de instalación de Full Disk Encryption en el disco duro local.
2. Ejecute `TMFDEInstall.exe`.

   Nota

   Si se muestra la ventana **Control de cuentas de usuario**, haga clic en **Sí** para permitir que el instalador realice cambios en el dispositivo.

   Aparecerá la ventana de bienvenida del instalador.
3. Seleccione **Instalación no administrada** y haga clic en **Siguiente**.

   Se muestra la pantalla **Instalación no administrada**.
4. Especifique el nombre de usuario y la contraseña que se deberán utilizar en una nueva cuenta al iniciar sesión en el cliente no administrado. A continuación, haga clic en **Siguiente**.

   Comienza la instalación.
5. En la pantalla **Instalación finalizada**, haga clic en **Cerrar**.
6. En la pantalla de confirmación, haga clic en **Sí** para reiniciar o apagar el dispositivo.

   La instalación de Full Disk Encryption se completa cuando se muestra el arranque previo. El cifrado de disco comienza después de iniciar Windows.

Qué hacer a continuación

Una vez cargado el arranque previo de Full Disk Encryption, el usuario debe iniciar sesión para obtener acceso a Windows.

Instalación de FileArmor

Use el cifrado de FileArmor para proteger archivos y carpetas que se encuentren en prácticamente cualquier dispositivo que aparece como una unidad en el sistema operativo del host.

Esquema de implementación de FileArmor

Procedimiento

1. Active FileArmor en MMC de PolicyServer.
2. Configure las políticas de FileArmor:
   a. Clave de cifrado utilizada
   b. Carpetas para cifrar
   c. Uso de medios extraíbles
   d. Método de autenticación
3. Configure los grupos y usuarios.
4. Cree y pruebe el paquete de instalación.
5. Compruebe que la configuración se aplica tal y como se ha definido.
6. Prepare las comunicaciones del usuario final.

Configuración de políticas de FileArmor necesaria

Procedimiento

1. La decisión más importante antes de la implementación de FileArmor es seleccionar la clave de cifrado adecuada:

   - **Clave de usuario:** Solo el usuario puede acceder al archivo cifrado.
   - **Clave de grupo:** Todos los usuarios dentro del grupo pueden acceder al archivo.
   - **Clave de empresa:** Todos los usuarios de todos los grupos pueden acceder al archivo.

2. La segunda decisión está relacionada con las políticas de medios extraíbles de FileArmor. Todas las políticas están ubicadas en: **FileArmor** > **Cifrado** > **Medios extraíbles**.

   TABLA 4-4. Políticas de FileArmor para configurar

POLÍTICA	DESCRIPCIÓN
Soportes extraíbles	Permitir la protección de dispositivos de almacenamiento USB.
Dispositivos USB permitidos	Permitir que se utilice cualquier dispositivo de almacenamiento USB o que solo se utilicen los dispositivos de KeyArmor.
Cifrado completo del dispositivo	Cifrar automáticamente todos los archivos copiados al dispositivo de almacenamiento USB.
Desactivar unidad USB	Establecer en Siempre, Desconectado o Nunca.

3. Decida si usará FileArmor para cifrar automáticamente las carpetas del dispositivo host. Los archivos copiados a una carpeta segura se cifrarán automáticamente. De forma predeterminada, se crea una carpeta cifrada de FileArmor en el escritorio.

   - Utilice **Cifrado** > **Especifique carpetas que cifrar** para crear carpetas seguras en el dispositivo host.

- Utilice **Cifrado** > **Medios extraíbles** > **Carpetas que cifrar en soportes extraíbles** para crear carpetas seguras en un dispositivo de almacenamiento USB.

Instalación de FileArmor

FileArmor se puede instalar mediante alguno de los métodos siguientes:

- Mediante una herramienta de automatización como Microsoft SCCM o SMS
- Manualmente en un equipo local

Requisitos del sistema de FileArmor

TABLA 4-5. 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
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 *Preparación del dispositivo en la página 4-5* para cambiar la prioridad de arranque. Requisitos adicionales para Windows XP: • Microsoft .NET Framework 2.0 SP1 o versión posterior • Microsoft Windows Installer 3.1

Otros requisitos

- El usuario que realiza la instalación debe tener derechos de administrador en el dispositivo.
- Copie y ejecute el paquete de instalación localmente.
- Establezca una contraseña fija para todos los usuarios de PolicyServer.
- La cuenta de usuario debe pertenecer a un grupo de PolicyServer y tener permisos para agregar dispositivos a este grupo.

Nota

Las cuentas de autenticador o administrador de empresa de PolicyServer no pueden utilizarse para instalar FileArmor.

Instalación manual de FileArmor

El proceso de instalación manual implica ejecutar un instalador en el cliente y seguir las instrucciones paso a paso. Los usuarios estándar, autenticadores o administradores de grupos de PolicyServer pueden instalar FileArmor.

Procedimiento

1. Ejecute `FASetup.msi` para SO de 32 bits o `FASetup(x64).msi` para SO de 64 bits.

   Asistente para instalación de FileArmor para comenzar el proceso de instalación de FileArmor

2. Haga clic en **Siguiente**.

   Nota

   Si se le pide el Control de cuentas de usuario, haga clic en **Sí**.

3. Cuando finalice la instalación, haga clic en **Cerrar**.

4. Haga clic en **Sí** para reiniciar Windows.

   Tras reiniciar el dispositivo, se instala el software FileArmor y se muestran dos iconos de FileArmor: un acceso directo en el escritorio y un icono en la bandeja.

Instalación automática de FileArmor

La instalación de FileArmor mediante secuencias de comandos automatiza el proceso y facilita la tarea de distribuir el software en toda la empresa. Consulte *Uso de secuencias de comandos para automatizar las instalaciones en la página 4-20* para obtener más información.

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.

Requisitos del sistema de KeyArmor

La tabla siguiente explica los requisitos mínimos para utilizar los medios extraíbles USB protegidos de KeyArmor.

TABLA 4-6. 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

Componentes de dispositivos

KeyArmor monta dos unidades al insertar el dispositivo en un puerto USB.

FIGURA 4-1. 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.

Esquema de implementación de KeyArmor

Similar a Full Disk Encryption y FileArmor, el esquema de implementación de KeyArmor es el siguiente:

1. Active KeyArmor en PolicyServer.
2. Configure las políticas aplicables para KeyArmor:
    - Método de autenticación
    - Debe estar conectado al servidor
    - Un usuario por dispositivo
    - Acción de inicio de sesión incorrecta
    - Opciones de actualización de antivirus
3. Configure los usuarios y grupos.
4. Prepare las contraseñas y la autenticación de dispositivos.
5. Prepare las comunicaciones del usuario final.

Directrices para el usuario final de KeyArmor

- Si el dispositivo está conectado a un puerto USB 2.0, Windows detecta y configura el dispositivo automáticamente.
- Al recibir un nuevo dispositivo, los usuarios finales deben completar un proceso de configuración puntual.
- El uso constante solo requiere un nombre de usuario y una contraseña válidos.
- KeyArmor cifra automáticamente todos los archivos almacenados en el dispositivo de KeyArmor.
- Abrir, ver, mover o copiar archivos a un dispositivo host es una actividad iniciada por el usuario que solo puede llevarse a cabo después de la autenticación apropiada en el dispositivo de KeyArmor.

Protección de archivos de KeyArmor

- Los archivos o carpetas guardados 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.
- Los archivos permanecen cifrados mientras están almacenados en KeyArmor.
- Para asegurarse de tener las últimas definiciones de antivirus, Trend Micro recomienda no copiar ningún archivo al dispositivo KeyArmor hasta que finalice la actualización de antivirus inicial.

¡ADVERTENCIA!

Siempre siga el proceso para eliminar con seguridad los dispositivos de KeyArmor:

1. Elija **Cerrar sesión** en la aplicación de KeyArmor.
2. Haga clic con el botón derecho en el icono de la bandeja de KeyArmor y seleccione **Cerrar sesión**.

Si un dispositivo de KeyArmor se elimina de forma segura puede evitar un desgaste y pérdida de datos anticipados.

Uso de secuencias de comandos para automatizar las instalaciones

Las instalaciones con secuencias de comandos son más comunes para grandes implementaciones mediante herramientas como Microsoft SMS o Active Directory. La Ayuda del instalador de la línea de comandos (para más detalles, consulte *Ayuda del instalador de la línea de comandos en la página 4-22*) es una herramienta que sirve para crear secuencias de comandos. Los argumentos disponibles permiten instalaciones parcialmente o totalmente silenciosas.

¡ADVERTENCIA!

Una preparación insuficiente de la unidad de disco duro y de la instalación del sistema puede dar lugar a la pérdida de datos irreversible.

Requisitos

- Todas las secuencias de comandos de la instalación deben ejecutarse localmente, no desde un recurso compartido de red o una unidad USB.
- Las secuencias de comandos deben ejecutarse como administradores locales.
- Las secuencias de comandos de la instalación deben probarse en un programa piloto.

Argumentos de secuencia de comandos

La tabla siguiente explica los argumentos disponibles para la creación de secuencias de comandos para instalar automáticamente los clientes de punto final.

TABLA 4-7. Argumentos con secuencias de comandos en las instalaciones automatizadas de Full Disk Encryption

ARGUMENTO	VALOR	NOTAS
ENTERPRISE	Nombre de la empresa	Puede encontrar el nombre de la empresa en el archivo de licencia.
HOST	Nombre de host DNS o dirección IP	El nombre o la ubicación de PolicyServer.
USERNAME	• Administrador de grupo • Autenticador de grupo • Usuario de grupo (si está activada la política de instalación)	La cuenta de administrador o autenticador de nivel empresarial no se puede utilizar para instalar Full Disk Encryption.

Argumento	Valor	Notas
PASSWORD	Contraseña para el nombre de usuario especificado	La contraseña fija configurada en PolicyServer para el usuario o una contraseña de dominio.

Tabla 4-8. Argumentos con secuencias de comandos en las instalaciones automatizadas de FileArmor

Argumento	Valor	Notas
PSENTERPRISE	Nombre de la empresa	Puede encontrar el nombre de la empresa en el archivo de licencia.
PSHOST	Nombre de host DNS o dirección IP	El nombre o la ubicación de PolicyServer.
FAUSERNAME	• Administrador de grupo • Autenticador de grupo • Usuario de grupo (si está activada la política de instalación)	La cuenta de administrador o autenticador de nivel empresarial no se puede utilizar para instalar FileArmor.
FAPASSWORD	Contraseña para el nombre de usuario especificado	La contraseña fija configurada en PolicyServer para el usuario o una contraseña de dominio.

Ayuda del instalador de la línea de comandos

La Ayuda del instalador de la línea de comandos (`CommandLineInstallerHelper.exe`) puede generar secuencias de comandos utilizados para instalar Full Disk Encryption, FileArmor y PolicyServer. Opciones que permiten cifrar y ocultar la información de la cuenta de instalación y seleccionar las diversas opciones de símbolo del sistema. Los resultados de la secuencia de comandos se copian fácilmente en el portapapeles para la exportación. La herramienta tiene dos pestañas: una para los clientes y otra para PolicyServer.

Nota

La instalación de línea de comandos de PolicyServer se admite en las versiones 3.1.2 y posterior.

Cuando utilice la Ayuda del instalador de la línea de comandos:

- Ejecute únicamente secuencias de comandos en un cliente de punto final, y no desde la red.
- Ejecute las secuencias de comandos como un administrador local.
- Pruebe las secuencias de comandos de la instalación en un programa piloto primero.
- Revise todos los elementos de la lista de comprobación previa a la instalación de Full Disk Encryption y FileArmor antes de ejecutar cualquier distribución masiva de software.

Full Disk Encryption y FileArmor son compatibles con herramientas de distribución de software automatizadas, como SMS, SCCM, Tivoli, GPO y LANDesk.

Crear secuencias de comandos de instalación de PolicyServer

La información mínima necesaria para crear una secuencia de comandos:

- Credenciales de administrador y dirección de base de datos principal
- Ruta de acceso al programa de instalación de PolicyServer

Importante

La instalación mediante secuencias de comandos sólo es compatible con la versión 3.1.2 de PolicyServer o posterior.

Procedimiento

1. Proporcione toda la información requerida.
2. Proporcione información adicional si es necesario.

3. Haga clic en **Generar comando**.

   El campo de código del **comando de instalación del servidor de políticas** se rellena.

4. Haga clic en **Copiar al portapapeles**.

   La secuencia de comandos resultante se copia en el portapapeles.

Creación de secuencias de comandos de instalación del cliente

La siguiente información es necesaria para generar una secuencia de comandos de instalación silenciosa: Nombre de host o dirección IP de PolicyServer, el nombre de la empresa, el nombre de usuario, la contraseña y la ruta de acceso y el número de versión del instalador del cliente de punto final.

Procedimiento

1. Proporcione la información necesaria en los campos de texto correspondientes.
2. Seleccione las opciones que desee incluir en la secuencia de comandos.
3. Haga clic en **Generar comando**.

   Se generan las secuencias de comandos.

4. Haga clic en **Copiar comando de Full Disk Encryption** o **Copiar comando de FileArmor**.

   La secuencia de comandos resultante se copia en el portapapeles.

Ayuda de la línea de comandos

La Ayuda de la línea de comandos se utiliza para crear valores cifrados que se pueden utilizar para proteger las credenciales al crear secuencias de comandos de una instalación para la implementación o el uso de DAAutoLogin. La herramienta Ayuda de la línea de comandos se encuentra en la carpeta de herramientas de FileArmor.

Nota

La Ayuda de línea de comandos solo se puede ejecutar en sistemas donde esté instalado PolicyServer, Full Disk Encryption o FileArmor, ya que utiliza el cifrado de Mobile Armor.

El programa acepta una cadena única como único argumento y devuelve un valor cifrado para utilizarse en la secuencia de comandos de instalación. Los signos "=" iniciales y finales se incluyen como parte de la cadena cifrada completa y se deben incluir en la línea de comandos. Si el valor está cifrado y no devuelve un signo = inicial, debe agregarse un signo igual a la secuencia de comandos.

Opciones que permiten cifrar y ocultar la información de la cuenta de instalación y seleccionar las diversas opciones de símbolo del sistema. Los resultados de la secuencia de comandos se copian fácilmente en el portapapeles para la exportación.

TABLA 4-9. Argumentos para la Ayuda de la línea de comandos

FUNCIÓN	ARGUMENTOS		
	FULL DISK ENCRYPTION	FULL DISK ENCRYPTION CIFRADO	FILEARMOR
Empresa	ENTERPRISE	eENTERPRISE	PSENTERPRISE
PolicyServer	HOST	eHOST	PSHOST
Usuario	USERNAME	eUSERNAME	FAUSERNAME
Contraseña	PASSWORD	ePASSWORD	FAPASSWORD

Nota

El programa de instalación de FileArmor puede controlar automáticamente los valores cifrados.

Ejemplo de secuencias de comandos de Full Disk Encryption

Solo se puede pasar un valor a la Ayuda de la línea de comandos. No obstante, se puede ejecutar todas las veces que sea necesario para recopilar todos los valores cifrados necesarios.

```
Ubicación del software = C:\Archivos de programa\Trend Micro
\Full Disk Encryption\TMFDEInstaller.exe

ENTERPRISE = MyCompany

HOST = PolicyServer.mycompany.com

eUSERNAME = GroupAdministrator

ePASSWORD = 123456
```

Nota

En este ejemplo, se cifrarán el nombre de usuario y la contraseña.

Salida para instalar Full Disk Encryption:

```
C:\Archivos de programa\Trend Micro\DataArmor
\DataArmorInstaller.exe ENTERPRISE=MyCompany
HOST=policyserver.mycompany.com eUSERNAME==jJUJC/Lu4C/
Uj7yYwxubYhAuCrY4f7AbVFp5hKo2PR4O
ePASSWORD==5mih67uKdy7T1VaN2ISWGQQ=
```

Ejemplo de secuencia de comandos de FileArmor

Este es un ejemplo de una secuencia de comandos de instalación de FileArmor para un dispositivo con un sistema operativo de 32 bits. Para los dispositivos de 64 bits, se debe utilizar `FASetup(x64).msi`.

```
Ubicación del software = C:\Archivos de programa\Trend Micro
\FileArmor\FASetup.msi

PSEnterprise = MyCompany

PSHost = PolicyServer.mycompany.com

FAUser = GroupAdministrator

FAPassword = 123456
```

Nota

En este ejemplo, se cifrarán el nombre de usuario y la contraseña.

Salida para instalar FileArmor:

```
C:\Archivos de programa\Trend Micro\FileArmor\FASetup.msi
PSEnterprise=MyCompany PSHost= PolicyServer.mycompany.com
FAUser==jJUJC/Lu4C/Uj7yYwxubYhAuCrY4f7AbVFp5hKo2PR4O=
FAPassword==5mih67uKdy7T1VaN2ISWGQQ=
```

Capítulo 5

Actualizaciones, migraciones y desinstalaciones

En este capítulo se describen varios aspectos acerca de la actualización, administración, migración y desinstalación de todas las aplicaciones de Trend Micro Endpoint Encryption.

Este capítulo incluye los siguientes temas:

Actualización del servidor y software cliente

En esta sección se explican las actualizaciones del software de cliente de PolicyServer y Endpoint Encryption.

Actualización de PolicyServer

Antes de actualizar PolicyServer, tenga en cuenta lo siguiente:

- Todos los servicios o servidores de servicios front-end PolicyServer deben detenerse antes de finalizar la actualización de la base de datos.
- Al actualizar varios servidores de políticas conectados a la misma base de datos:
  1. Asegúrese de que solo un PolicyServer realiza la actualización de la base de datos.
  2. Detenga el servicio de Windows de PolicyServer en todos los servidores de políticas excepto en uno.
  3. Realice la actualización en el servidor activo.
  4. Una vez finalizada la actualización y la replicación de la base de datos, ejecute la actualización en los servidores restantes.
- Si se usa el proxy de LDAP de Trend Micro, actualícelo antes de actualizar a PolicyServer 3.1.3.

Nota

Trend Micro no admite entornos alojados de PolicyServer.

Actualización de las bases de datos y los servicios de PolicyServer

El programa instalador de PolicyServer configura las opciones de base de datos e instala los servicios de Windows. En PolicyServer 3.1.3, ahora puede especificar un número de puerto para el servicio Web de PolicyServer. Ahora es necesario también un segundo

puerto para el servicio Web del cliente. Si no existe un segundo puerto, se creará un nuevo puerto durante el proceso de instalación. Para obtener más información sobre la nueva arquitectura, consulte *Componentes de Endpoint Encryption en la página 1-2*.

Para poder utilizar Endpoint Encryption durante un período de prueba limitado, el nombre de la empresa y la cuenta de administrador de empresa se pueden configurar durante el proceso de instalación. PolicyServer funciona normalmente con todas las aplicaciones cliente, con un número ilimitado de dispositivos y con hasta 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 y dispositivos podrán seguir iniciando sesión una vez finalizado el período de prueba.

Procedimiento

1. Ejecute `PolicyServerInstaller.exe`
2. Lea detenidamente el Contrato de licencia para usuario final. Si está de acuerdo, haga clic en **Aceptar**.
3. Compruebe la versión de PolicyServer y, a continuación, haga clic en **Actualizar**.
4. En la pantalla de **Inicio de sesión del servicio de Windows**, la configuración predeterminada es la adecuada para la mayoría de la instalaciones. Haga clic en **Continuar**.
5. En la pantalla de **inicio de sesión del administrador de la base de datos**, introduzca la dirección IP o el nombre de host de Microsoft SQL Server (localhost), así como el nombre de usuario y la contraseña de una cuenta con la función sysadmin para la instancia de SQL especificada.

Nota

Para entornos con varias instancias de SQL Server, añada la instancia de SQL al final del nombre de host de PolicyServer o de la dirección IP utilizada. Utilice la sintaxis siguiente para especificar una instancia:

```
<nombre de host o dirección IP>\<instancia de la base de datos>
```

El instalador verifica la conexión de la base de datos.

6. En la ventana **Pregunta de PolicyServer**, haga clic en **Sí** para hacer una copia de seguridad de las bases de datos existentes o en **No** para sobrescribir los datos existentes.

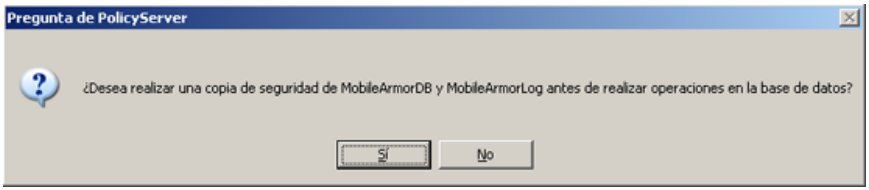


FIGURA 5-1. Mensaje de copia de seguridad de la base de datos

7. En la pantalla **Inicio de sesión de base de datos**, proporcione las credenciales de la cuenta que se utilizaba anteriormente para que PolicyServer gestionara las transacciones de datos (servicio de Windows de PolicyServer).

   Si esta cuenta no está disponible, escriba las credenciales para crear una cuenta nueva.

8. En la pantalla **Ubicación de instalación del servicio Web**, especifique el sitio de IIS que PolicyServer MMC y el servicio Web del cliente utilizan para comunicarse con PolicyServer. El número de puerto predeterminado es 8080. Si el puerto 8080 está en uso, entonces se asignará el siguiente puerto disponible.

   a. Seleccione un sitio desde el menú desplegable **Sitio de destino**.

   b. Revise el puerto asignado actualmente y, si fuera necesario, especifique un número de puerto diferente en el campo **Nuevo puerto**.

   Nota

   Trend Micro recomienda reservar el puerto 80 para el servicio Web del cliente.

   c. Haga clic en **Continuar**.

9. El siguiente paso se ha diseñado para configurar el servicio Web del cliente, que es el sitio de IIS que todos los clientes de Endpoint Encryption utilizan para comunicarse con PolicyServer. En función de si está disponible una segunda ubicación de IIS, se mostrará una de las siguientes pantallas:

- Si está disponible una segunda ubicación de IIS, se mostrará la pantalla **Ubicación del servicio Web cliente**.

  a. Seleccione un sitio desde el menú desplegable **Sitio de destino**.

  b. Revise la asignación del puerto predeterminado para el servicio Web del cliente.

  > **Nota**
  >
  > Trend Micro recomienda mantener el número de puerto 80. Sin embargo, si fuera necesario, especifique un número de puerto diferente en el campo **Nuevo puerto**. El número de puerto debe ser un número entero positivo entre 1 y 65535.

  c. Haga clic en **Continuar**.

- Si no está disponible un segundo sitio de IIS, se mostrará la pantalla **Crear ubicación del servicio Web cliente**, desde la que podrá configurar una nueva ubicación de IIS.

  a. Especifique un nombre para la ubicación de IIS en el campo **Nombre del sitio**.

  b. Desplácese hasta la ubicación del sitio. Si no existe ninguna carpeta, cree una nueva.

  c. Especifique la dirección IP y el número de puerto para la nueva ubicación de IIS.

  > **Nota**
  >
  > Trend Micro recomienda mantener el número de puerto 80. Sin embargo, si fuera necesario, especifique un número de puerto diferente. El número de puerto debe ser un número entero positivo entre 1 y 65535.

  d. Haga clic en **Continuar**.

10. En la pantalla **Ubicación de instalación del servicio Web móvil**, revise la configuración y, a continuación, haga clic en **Continuar**.

11. En la pantalla **Crear cuentas de inicio de sesión de nombre y administrador de empresa**, especifique el nuevo nombre de empresa y las credenciales para una

cuenta de administrador de empresa utilizados para administrar PolicyServer durante el período de prueba inicial.

12. Haga clic en **Continuar**.

    Se inicia el proceso de instalación.

13. En el mensaje **Instalación de PolicyServer**, haga clic en **Aceptar**.

14. Haga clic en **Finalizado**.

15. En la ventana del programa instalador de PolicyServer, haga clic en **Salir**.

16. Reinicie el servidor.

Actualización de MMC de PolicyServer

MMC de PolicyServer se debe eliminar con la característica de Windows Agregar o quitar programas antes de instalar una nueva versión.

Procedimiento

1. Vaya a **Inicio** > **Panel de control** > **Agregar o quitar programas**.

2. Seleccione Complemento de MMC de PolicyServer en la lista y haga clic en **Quitar**.

3. Haga clic en **Sí** para eliminar MMC de PolicyServer.

4. Ejecute `PolicyServerMMCSnapinSetup.msi`.

5. Haga clic en **Siguiente** para abrir el cuadro de diálogo de bienvenida del asistente de instalación de MMC de PolicyServer.

6. Lea detenidamente el contrato de licencia, seleccione **Acepto** si acepta los términos y, a continuación, haga clic en **Siguiente**.

7. Seleccione la carpeta de instalación o deje la ubicación predeterminada y haga clic en **Siguiente**.

8. Haga clic en **Siguiente** para confirmar la instalación.

   Comienza el proceso de actualización.

9. Haga clic en **Cerrar** para finalizar la instalación.

10. Haga clic en **Sí** para reiniciar el dispositivo (opcional).

11. Tras iniciar sesión en el servidor, abra MMC de PolicyServer desde el acceso directo del escritorio.

    La actualización de MMC de PolicyServer ha finalizado. Autentique MMC de PolicyServer con las credenciales de administrador de empresa.

Nota

Consulte el Manual del administrador de Endpoint Encryption para las tareas posteriores a la instalación como habilitar las aplicaciones, la creación de dispositivos y usuarios y la configuración de políticas.

Actualización de Full Disk Encryption

El programa instalador de Full Disk Encryption (`TMFDEUpgrade.exe`) es compatible con DataArmor SP7g (3.0.12.861) y con DataArmor 3.1.2. Para actualizar desde DataArmor SP7g, el dispositivo debe estar conectado a PolicyServer. Para versiones anteriores de DataArmor y DriveArmor, desinstale la aplicación y reinicie el dispositivo antes de instalar Full Disk Encryption.

Nota

Los sistemas operativos que no están en inglés y que ejecutan una versión más antigua de Full Disk Encryption (DataArmor 3.0.12 o 3.1.2) continuarán utilizándose en inglés a partir del momento de la actualización. Para actualizar a un idioma compatible, primero debe desinstalar la aplicación anterior y, a continuación, instalar Full Disk Encryption 3.1.3. Para obtener información sobre la desinstalación de Full Disk Encryption, consulte *Desinstalación de Full Disk Encryption en la página 5-17*.

Procedimiento

1. Copie el paquete de instalación de Full Disk Encryption en el disco duro local.

2. Ejecute `TMFDEUpgrade.exe`.

Nota

Si se abre el Control de cuentas de usuario de Windows, haga clic en **Sí** para continuar.

3. Una vez finalizada la actualización y que aparezca la notificación, reinicie el dispositivo.

Actualización de FileArmor

Use `FA_313_Upgrade.exe` para actualizar un dispositivo de FileArmor 3.0.13 o FileArmor 3.0.14. `FA_313_Upgrade.exe`se encuentra en la carpeta de herramientas en el directorio de instalación de FileArmor.

Nota

`FA_313_Upgrade.exe` omite la política Permitir al usuario desinstalar y realiza la actualización independientemente de que la política esté establecida en **Sí** o **No**.

Procedimiento

1. Ejecute `FA_313_Upgrade.exe`.

   El instalador de Windows desinstala la versión anterior de FileArmor y después instala FileArmor 3.1.3. Una vez finalizada, Windows se reinicia.

2. Una vez reiniciado Windows, inicie sesión y compruebe la nueva carpeta de FileArmor. Los archivos y las carpetas cifrados se mantienen.

Actualización a Windows 8

Endpoint Encryption no es compatible con la actualización a Windows 8. Si es necesario realizar una actualización, Trend Micro recomienda seguir este procedimiento para evitar la pérdida de datos cuando Full Disk Encryption o FileArmor están instalados en el cliente de punto final. KeyArmor no es compatible con el entorno de Windows 8.

Procedimiento

1. Siga las instrucciones de la Guía del administrador de Endpoint Encryption para descifrar el dispositivo.
2. Desinstale las aplicaciones cliente de punto final:
   - Para obtener información sobre la desinstalación de Full Disk Encryption, consulte *Desinstalación de Full Disk Encryption en la página 5-17*.
   - Para obtener detalles sobre la desinstalación de FileArmor, consulte *Desinstalación de FileArmor en la página 5-18*.
3. Actualice o instale el sistema operativo de Windows 8.

Nota

Este documento no explica cómo instalar el entorno de Windows 8. Para obtener instrucciones, consulte la documentación de usuario asociada de Microsoft.

4. Compruebe que el entorno de Windows 8 es estable y que la actualización se ha realizado correctamente.
5. Vuelva a instalar las aplicaciones cliente de punto final:
   - Para obtener información sobre la instalación de Full Disk Encryption, consulte *Instalación de Full Disk Encryption en la página 4-2*.
   - Para obtener detalles sobre la instalación de FileArmor, consulte *Instalación de FileArmor en la página 4-13*.

Administración de revisiones con Full Disk Encryption

Use la **Ayuda de la línea de comandos** y **DAAutoLogin** juntos para ejecutar la administración de revisiones de Windows en dispositivos con Full Disk Encryption instalado. La Ayuda de la línea de comandos crea valores cifrados para secuencias de

comandos y DAAutoLogin concede una omisión temporal del arranque previo de Full Disk Encryption.

DAAutoLogin se puede utilizar en diversas combinaciones para satisfacer distintas necesidades. Después de forzar las revisiones se puede ejecutar una secuencia de comandos mediante DAAutoLogin para enviar un comando de reinicio al dispositivo para mostrar Windows GINA y confirmar que la revisión se ha instalado correctamente o para forzar otra ronda de revisiones.

DAAugoLogin acepta los siguientes modificadores:

```
DAAutoLogin <nombre de usuario de arranque previo> <contraseña
de arranque previo> [<nombre de dominio> <nombre de usuario de
dominio> <contraseña de dominio>]
```

Cada valor requerido se puede pasar y separar por espacios. Agregar los modificadores de dominio permite la autenticación de Windows.

Nota

- Ejecute ambas herramientas en un dispositivo con Full Disk Encryption instalado.
- Ambas herramientas están disponibles en la carpeta de herramientas del archivo zip descargado desde Trend Micro. Para obtener ayuda, póngase en contacto con Asistencia de Trend Micro.

Uso de la Ayuda de la línea de comandos

La Ayuda de la línea de comandos y DAAutoLogin se pueden utilizar juntos para la administración de revisiones de Full Disk Encryption. La Ayuda de la línea de comandos permite pasar valores cifrados a través de la secuencia de comandos al arranque previo de Full Disk Encryption. DAAutoLogin concede una omisión temporal del arranque previo de Full Disk Encryption.

Procedimiento

1. Copie `CommandLineHelper.exe` localmente al dispositivo de Full Disk Encryption. (En este ejemplo, `CommandLineHelper.exe` se copia a `C:\`).

2. Abra el símbolo del sistema y escriba `C:\CommandLineHelper.exe`, y especifique el nombre de usuario o la contraseña que se utilizarán. Si el nombre de usuario es SMSUser, el comando es `C:\CommandLineHelper.exe SMSUser`.

3. Haga clic en **Volver** para mostrar el valor cifrado.

4. Vuelva a ejecutar la Ayuda de la línea de comandos para el segundo valor cifrado. Si la primera vez era el nombre de usuario, ejecútelo de nuevo para cifrar la contraseña.

Proceso de revisiones para Full Disk Encryption

Procedimiento

1. Fuerce las revisiones en los dispositivos de destino.

2. Realice un seguimiento con una secuencia de comandos mediante DAAutoLogin.

3. Envíe un comando de reinicio para que el dispositivo cargue Windows GINA para confirmar la instalación correcta de las revisiones o para forzar otra ronda de revisiones.

Sustitución de un producto de cifrado instalado previamente

Full Disk Encryption se puede instalar en un dispositivo que previamente se haya cifrado con un producto de cifrado de disco completo distinto. Como la mayoría del software de cifrado modifica todos los sectores de un disco duro, es fundamental probar el proceso de preparación del disco y la estrategia de implementación. En función del tiempo necesario para descifrar un dispositivo y cifrarlo con Full Disk Encryption, quizás sea más sencillo realizar una copia de seguridad de los datos del usuario y volver a crear una imagen del equipo antes de instalar Full Disk Encryption.

Opción 1: Eliminar el producto de cifrado anterior

Procedimiento

1. Descifre el disco mediante el método definido que ha proporcionado el proveedor de software.
2. Desinstale el software del proveedor previamente instalado (o compruebe que la opción de BitLocker está deshabilitada).
3. Arranque el dispositivo.
4. Ejecute `chkdsk` y desfragmente la unidad.
5. Compruebe que se realiza un registro de arranque maestro (MBR) normal en cada dispositivo y confirme que hay un sector de arranque normal en la partición de arranque.

   Nota

   El dispositivo no puede ser un equipo con arranque dual.

6. Realice una copia de seguridad de los archivos de usuario.
7. Instale Full Disk Encryption. Para conocer más detalles, consulte *Instalación de Full Disk Encryption en la página 4-2*.

Opción 2: Hacer copia de seguridad y volver a crear imagen del dispositivo

Procedimiento

1. Realice una copia de seguridad de los archivos de usuario.
2. Vuelva a crear una imagen del dispositivo:
   a. En el símbolo del sistema, ejecute `DiskPart Clean All`.
   b. Cree una partición.

c. Formatee la unidad.

d. Cree una imagen de la unidad.

3. Instale Full Disk Encryption y cifre el dispositivo.

4. Restaure los archivos de usuario.

Migración de clientes de punto final a un nuevo PolicyServer

Esta sección explica cómo cambiar el PolicyServer que controla las políticas del cliente de punto final. Esto es útil cuando se cambia de un usuario final a un departamento o unidad de negocio administrados por una instancia diferente de PolicyServer.

Cambio de PolicyServer de Full Disk Encryption

Las opciones de PolicyServer de Full Disk Encryption se pueden configurar en la consola de recuperación; ábrala desde el arranque previo de Full Disk Encryption o ejecutando `C:\Archivos de programa\Trend Micro\Full Disk Encryption\RecoveryConsole.exe`.

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.

Traslado de Full Disk Encryption a una nueva empresa

¡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.

Procedimiento

1. Abra la consola de recuperación. Hay dos maneras de abrir la consola de recuperación:

   - Desde el arranque previo de Full Disk Encryption:

     a. Seleccione la casilla de verificación **Consola de recuperación**.

     b. Especifique las credenciales y haga clic en **Iniciar sesión**.

- Desde Windows:

  a. Vaya a `C:\Archivos de programa\Trend Micro\Full Disk Encryption\`.

  b. Ejecute `RecoveryConsole.exe`.

  c. Especifique las credenciales y haga clic en **Iniciar sesión**.

2. Haga clic en **Configuración de red**.
3. Seleccione la pestaña **PolicyServer**.
4. Haga clic en **Cambiar empresa**.

   Se mostrará la ventana **Cambiar empresa**.

FIGURA 5-2. Cambio de empresa en la consola de recuperación

5. Especifique el nuevo nombre de usuario, la contraseña, la dirección IP de PolicyServer (o el nombre de host) y la empresa.
6. Haga clic en **Guardar**.

Full Disk Encryption valida el servidor y muestra un mensaje de confirmación.

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

Cambio de PolicyServer de FileArmor

Procedimiento

1. Haga clic con el botón derecho en el icono de la bandeja de FileArmor y seleccione **Acerca de FileArmor**.
2. Haga clic en **Editar PolicyServer**.
3. Especifique la dirección IP o el nombre de host nuevos de PolicyServer y haga clic en **Aceptar**.

Mover KeyArmor a una empresa nueva

Procedimiento

1. Inicie sesión en el dispositivo con las credenciales de administrador de Endpoint Encryption.
2. Haga clic con el botón derecho en el icono de KeyArmor en el menú de la bandeja y seleccione **Acerca de KeyArmor**.
3. Haga clic en el enlace **editar** que aparece junto a la casilla **Dirección del servidor** y escriba la nueva dirección del servidor.
4. Haga clic en **Aceptar**.
5. Cierre sesión en KeyArmor.
6. Vuelva a montar el dispositivo y a iniciar sesión con las credenciales de administrador.
7. Haga clic con el botón derecho en el icono de KeyArmor en el menú de la bandeja y seleccione **Acerca de KeyArmor**.

8. Haga clic en el enlace **editar** que aparece junto a la casilla **Empresa** y escriba el nuevo nombre de la empresa.
9. Haga clic en **Aceptar**.
10. Haga clic en **Cerrar**.
11. Cierre sesión en KeyArmor.
12. Inicie sesión en el dispositivo de KeyArmor con un nombre de usuario y una contraseña de administrador de grupo de la nueva empresa de destino.
13. Compruebe el registro de sucesos del grupo de empresa nuevo que el dispositivo agregó al grupo correcto.

Desinstalación de aplicaciones cliente

En esta sección se explica cómo desinstalar las aplicaciones cliente de Endpoint Encryption.

Desinstalación de Full Disk Encryption

Para desinstalar Full Disk Encryption, el usuario debe disponer de derechos para desinstalar dentro de su grupo y tener derechos de administrador local de Windows.

Consejo

Cualquier autenticador de usuario o grupo puede ejecutar el programa de desinstalación de Windows si la política **Full Disk Encryption** > **Común** > **Cliente** > **Permitir al usuario desinstalar** = **Sí**.

Procedimiento

1. Inicie sesión en Full Disk Encryption y, después, en Windows.
2. En Windows, vaya a `C:\Archivos de programa\Trend Micro\Full Disk Encryption` y ejecute `TMFDEUninstall.exe`.

Nota

Si se le pide el **Control de cuentas de usuario**, haga clic en **Sí**.

Se abre la pantalla de desinstalación de Full Disk Encryption.

3. Haga clic en **Siguiente**.

   Full Disk Encryption comienza a desinstalarse.

4. Haga clic en **Aceptar** para confirmar el descifrado de la unidad.

Nota

Para ver el estado de descifrado, abra Full Disk Encryption desde la bandeja del sistema.

5. Cuando finalice el descifrado, haga clic en **Aceptar**.
6. Ejecute `TMFDEUninstall.exe` de nuevo para finalizar la desinstalación.
7. Arranque el dispositivo.

Nota

El registro del dispositivo no se eliminará automáticamente y tendrá que quitarse manualmente de PolicyServer.

Desinstalación de FileArmor

Utilice la característica Agregar o quitar programas de Windows para desinstalar FileArmor.

Nota

- Establezca **Políticas** > **FileArmor** > **Equipo** > **Permitir al usuario desinstalar** en **Sí** para permitir que cualquier autenticador de grupo o usuario ejecute el programa de desinstalación de Windows.
- Descifre manualmente todos los archivos cifrados antes de desinstalar FileArmor. De lo contrario, quedarán ilegibles.
- Guarde y cierre todos los documentos antes de iniciar el proceso de desinstalación. Es necesario reiniciar cuando finalice el programa de desinstalación.

Procedimiento

1. Inicie sesión en FileArmor con una cuenta que tenga permiso para desinstalar FileArmor.
2. Abra el **Menú Inicio de Windows** y vaya a **Panel de control** > **Programas** > **Desinstalar un programa**.
3. Seleccione FileArmor en la lista y haga clic en **Desinstalar**.

Capítulo 6

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

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

Lista de comprobación piloto de Endpoint Encryption

Lista de comprobación del programa piloto	Fecha y hora	Notas
PolicyServer configurado según sea necesario • Políticas definidas • Grupos creados • Usuarios creados/importados		
Software cliente instalado (Full Disk Encryption o FileArmor) • El software se ha copiado localmente en el equipo y se ejecuta correctamente		

Lista de comprobación del programa piloto	Fecha y hora	Notas
Los administradores, autenticadores y usuarios finales pueden acceder a dispositivos basados en la configuración de políticas • Contraseña fija • Inicio de sesión único • Tarjeta inteligente		
Todos los equipos compatibles con el nuevo software • Autenticación de arranque previo o conectividad confirmadas • El cifrado se ha finalizado • El equipo funciona con normalidad • Archivos/carpetas cifrados por política • Puerto USB controlado como define la política • Las alertas, los registros de eventos y los informes de PolicyServer confirman la actividad del usuario final y administrador		

Lista de comprobación del programa piloto	Fecha y hora	Notas
Los usuarios finales pueden realizar su actividad habitualmente • Acceda a las ventanas a través del nombre de usuario y la contraseña existentes o el inicio de sesión único (Single Sign-SSO) del arranque previo • El equipo funciona normalmente tanto dentro como fuera de la red • El usuario tiene acceso a todos los datos, aplicaciones y recursos de red de usuario		

LISTA DE COMPROBACIÓN DEL PROGRAMA PILOTO	FECHA Y HORA	NOTAS
Las pruebas de los administradores del sistema son compatibles con los procesos • Crear administradores de copia de seguridad • Informes de prueba y alertas • Utilice la consola de recuperación de Full Disk Encryption para realizar copias de seguridad y recuperar archivos • Utilice el CD de recuperación de Full Disk Encryption para descifrar el dispositivo y eliminar el arranque previo • Proceso de autenticación de ayuda remota de prueba • Borrado y bloqueo del dispositivo de prueba  **¡ADVERTENCIA!** No borre un dispositivo KeyArmor. El dispositivo no se puede restaurar.		

Apéndice B

Lista de comprobación de infraestructura de seguridad

Tabla B-1. Lista de comprobación de infraestructura de seguridad

Comprobar	Preguntas
Usuario final	1. ¿La formación para el usuario final incluye la nueva funcionalidad que proporciona Endpoint Encryption? 2. ¿Se ha actualizado la política de uso aceptable (AUP) para incluir servicios de cifrado, especialmente las posibles sanciones por no utilizar u omitir el cifrado? 3. ¿Se notifica a los usuarios cuando inician sesión en la máquina que cumple la AUP? 4. ¿Se ha formado a los usuarios perfectamente para que informen en el caso de un dispositivo perdido o robado? 5. ¿Se ha formado a los usuarios acerca de los procedimientos relacionados con los intentos fallidos de conexión y la recuperación de contraseña? 6. ¿Hay una política sobre el cifrado de documentos confidenciales que se envían fuera de la organización? 7. ¿Se han agregado las nuevas políticas de contraseña a la AUP?

COMPROBAR	PREGUNTAS
Respuesta a incidentes	1. ¿Se ha actualizado la política de respuesta a incidentes (IR) para incluir las acciones realizadas cuando se produce la pérdida o el robo de un dispositivo? 2. ¿Se ha establecido algún programa de revisión de registros de auditoría para los registros de PolicyServer? 3. ¿Se han agregado las alertas de correo electrónico a la política IR, incluidos los destinatarios y la respuesta esperada al recibir una alerta? 4. ¿Se han desarrollado criterios específicos para permitir que un dispositivo se elimine o borre, incluida cualquier documentación de la pista de auditoría una vez finalizada la acción?
Evaluación de riesgos	1. ¿Se ha realizado una nueva evaluación de riesgos para mostrar el cambio en el perfil de riesgo que Endpoint Encryption ha proporcionado? 2. ¿Se han actualizado los procedimientos de evaluación de riesgos para incluir los datos de auditoría que proporciona PolicyServer?
Recuperación de desastres	1. ¿Se ha agregado PolicyServer a la lista de servicios críticos? 2. ¿Se ha actualizado el plan DR/BC para incluir la restauración del servicio PolicyServer? 3. ¿Se ha desarrollado un proceso para permitir que los datos del usuario se recuperen de un dispositivo?
Recursos humanos	1. ¿Se ha actualizado la lista de comprobación del nuevo empleado para incluir cualquier nuevo proceso de Endpoint Encryption? 2. ¿Se han actualizado los procesos de terminación para incluir cualquier nuevo proceso de Endpoint Encryption, especialmente la eliminación y el borrado del dispositivo?

Comprobar	Preguntas
Conformidad	1. ¿Se ha actualizado el perfil de compatibilidad para incluir las ventajas que ofrece Endpoint Encryption? 2. ¿Se ha realizado una revisión de cumplimiento de las normas en todos los aspectos de la instalación e implementación de Endpoint Encryption?

Apéndice C

Lista de comprobación previa a la instalación de Full Disk Encryption

Antes de instalar Full Disk Encryption, el instalador de Full Disk Encryption inicia el dispositivo de destino para comprobar que se cumplen todos los requisitos del sistema necesarios. Si no se cumplen, el instalador se cierra.

Use la lista de comprobación para determinar si faltan requisitos. Compruebe el archivo `PreInstallCheckReport.txt` para obtener más información. `PreInstallCheckReport.txt` se encuentra en la misma carpeta que los archivos de instalación de Full Disk Encryption.

TABLA C-1. Condiciones que comprueba el instalador

COMPROBACIÓN DEL SISTEMA	REQUISITO	NOTAS
Medios fijos	Unidad de disco duro interno	Full Disk Encryption no se puede instalar en las unidades extraíbles que ejecutan Windows. Para el cifrado de archivos y carpetas en medios extraíbles, utilice FileArmor.
Espacio libre	256 MB como mínimo	
Memoria	1GB como mínimo	

Comprobación del sistema	Requisito	Notas
Número de partición	Menos de 25 particiones	Las particiones con los MBR extendidos no están disponibles.
Tipo de partición	Solo se admite MBR	Actualmente no se admite GPT (necesario para los discos superiores a 2 TB).
La unidad física se puede arrancar	Es necesario una partición que se pueda arrancar.	Full Disk Encryption debe instalarse en una tabla de arranque.
Disco SCSI	El controlador de unidad ATA, AHCI o IRRT. No se admite SCSI.	• La comprobación solo proporciona una advertencia; Windows puede informar de una unidad SATA como SCSI. • Si el disco no es un verdadero SCSI, Full Disk Encryption se puede instalar. Si no está seguro, compruebe físicamente la unidad.
.Net Framework	.Net 2.0 SP1 o superior necesario para Windows XP y versiones posteriores.	Se omite para Windows Vista o sistemas operativos posteriores.
Compatibilidad con hardware SED	El cifrado de hardware está activado si existe.	Full Disk Encryption admite unidades Seagate™ DriveTrust™, OPAL y OPAL 2.
BitLocker no está instalado.	BitLocker no puede estar instalado en el dispositivo.	Si BitLocker está instalado, se deberá quitar antes de instalar Full Disk Encryption.

Nota

Si se produce un error en la comprobación previa a la instalación por cualquiera de estos motivos, póngase en contacto con Asistencia de Trend Micro para obtener más ayuda.

Índice

D

E

F

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: APSM35736/121016