Manual de producto de GFI

GFI EndPointSecurity™

Guía de introducción

Versión del documento: 1.1.1

Última actualización (mes/día/año): 3/20/2014

Tabla de contenido

Lista de figuras

Lista de tablas

1 Introducción

La proliferación de dispositivos de consumo, como iPods, dispositivos USB y teléfonos inteligentes ha aumentado drásticamente el riesgo de filtraciones de datos y otras actividades malintencionadas deliberadas o no intencionales. Para un empleado, es muy simple copiar grandes cantidades de datos confidenciales en un iPod o un dispositivo USB, o ingresar software ilegal y malintencionado en la red a través de estos dispositivos. GFI EndPointSecurity lo ayuda rápida y fácilmente a combatir estas amenazas críticas sin necesidad de bloquear todos los puertos y alterar sus operaciones diarias.

Temas de este capítulo

1.1 Acerca de GFI EndPointSecurity

GFI EndPointSecurity les permite a los administradores gestionar el acceso de usuario y registrar la actividad de manera activa sobre lo siguiente:

- Reproductores de medios, como iPods, Creative Zen y otros
- Unidades USB, CompactFlash, tarjetas de memoria, CD, disquetes y otros dispositivos de almacenamiento portátiles
- Dispositivos portátiles iPhone, BlackBerry y Android, teléfonos móviles, teléfonos inteligentes y dispositivos de comunicación similares
- Tarjetas de red, equipos portátiles y otras conexiones de red.

Cómo funciona GFI EndPointSecurity: Implementación y supervisión

Las operaciones de implementación y supervisión de directivas de protección de GFI EndPointSecurity pueden dividirse en las cuatro etapas lógicas que se describen a continuación:

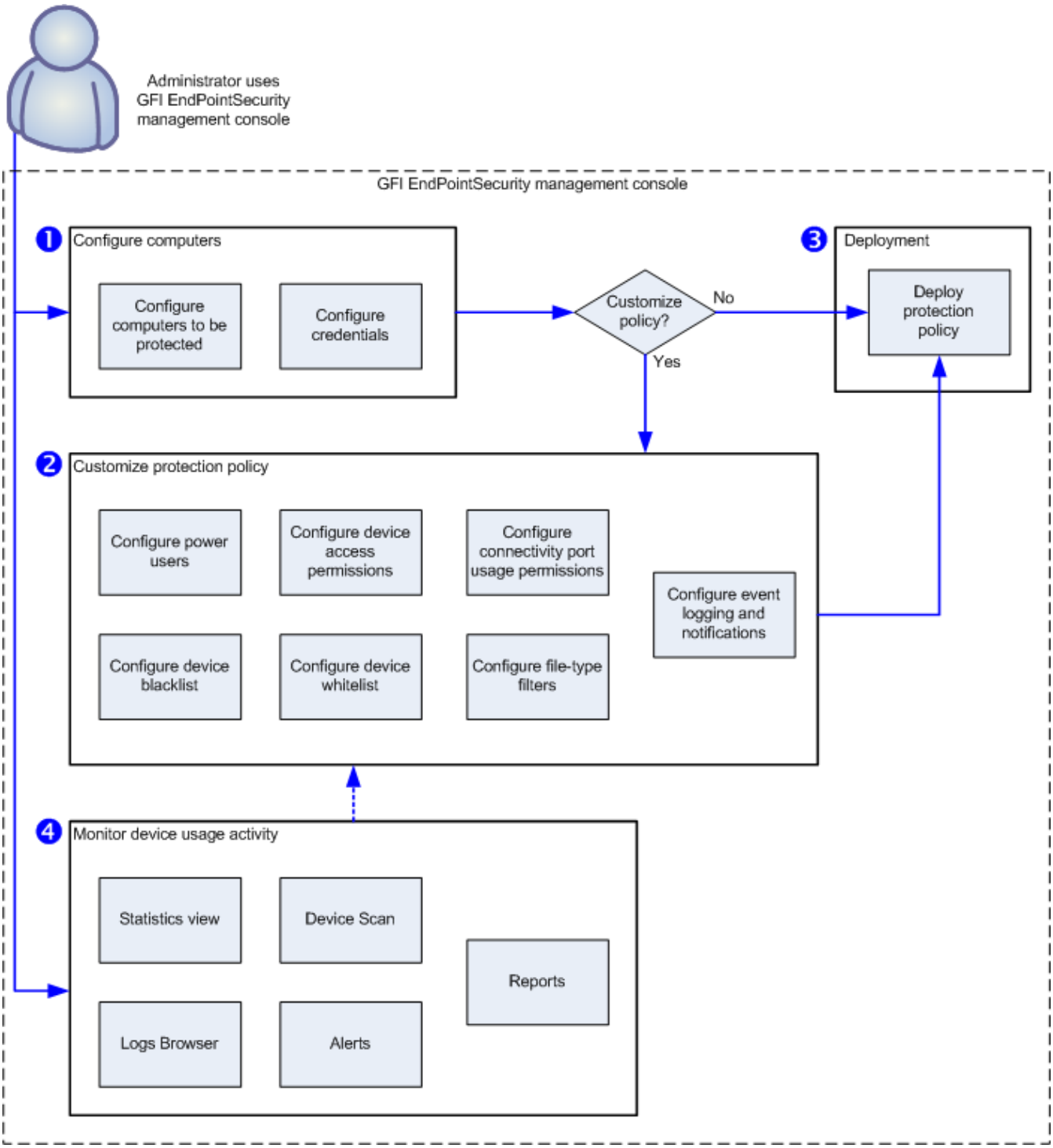


Figura 1: Directiva de protección: Implementación y supervisión

En la siguiente tabla, se describen las etapas detalladas más arriba:

Tabla 1: Implementación y supervisión de la directiva de protección

Etapa	Descripción
Etapa 1: Configurar equipos	El administrador especifica qué directiva de protección se asigna a cada equipo y las credenciales de inicio de sesión que usará GFI EndPointSecurity para acceder a los equipos de destino e implementar los agentes.
Etapa 2: Personalizar la directiva de protección	El administrador puede personalizar una directiva de protección antes o después de implementarla. Las opciones de personalización incluyen la creación de usuarios avanzados, la incorporación de dispositivos de lista negra/lista blanca y los permisos de acceso para dispositivos.

Etapa	Descripción
Etapa 3: Implementar la directiva de protección	El administrador implementa la directiva de protección. En la primera implementación de una directiva de protección, se instala automáticamente un agente de GFI EndPointSecurity en el equipo de destino de red remoto. En las siguientes implementaciones de la misma directiva de protección, el agente se actualizará y no se volverá a instalar.
Etapa 4: Supervisar el acceso a dispositivos	Cuando se hayan implementado los agentes, el administrador puede supervisar todos los intentos de acceso a dispositivos a través de la Consola de administración; recibir alertas y generar informes a través de GFI EndPointSecurity GFI ReportPack.

Cómo funciona GFI EndPointSecurity: Acceso a dispositivos

Las operaciones de acceso a dispositivos de GFI EndPointSecurity pueden dividirse en tres etapas lógicas:

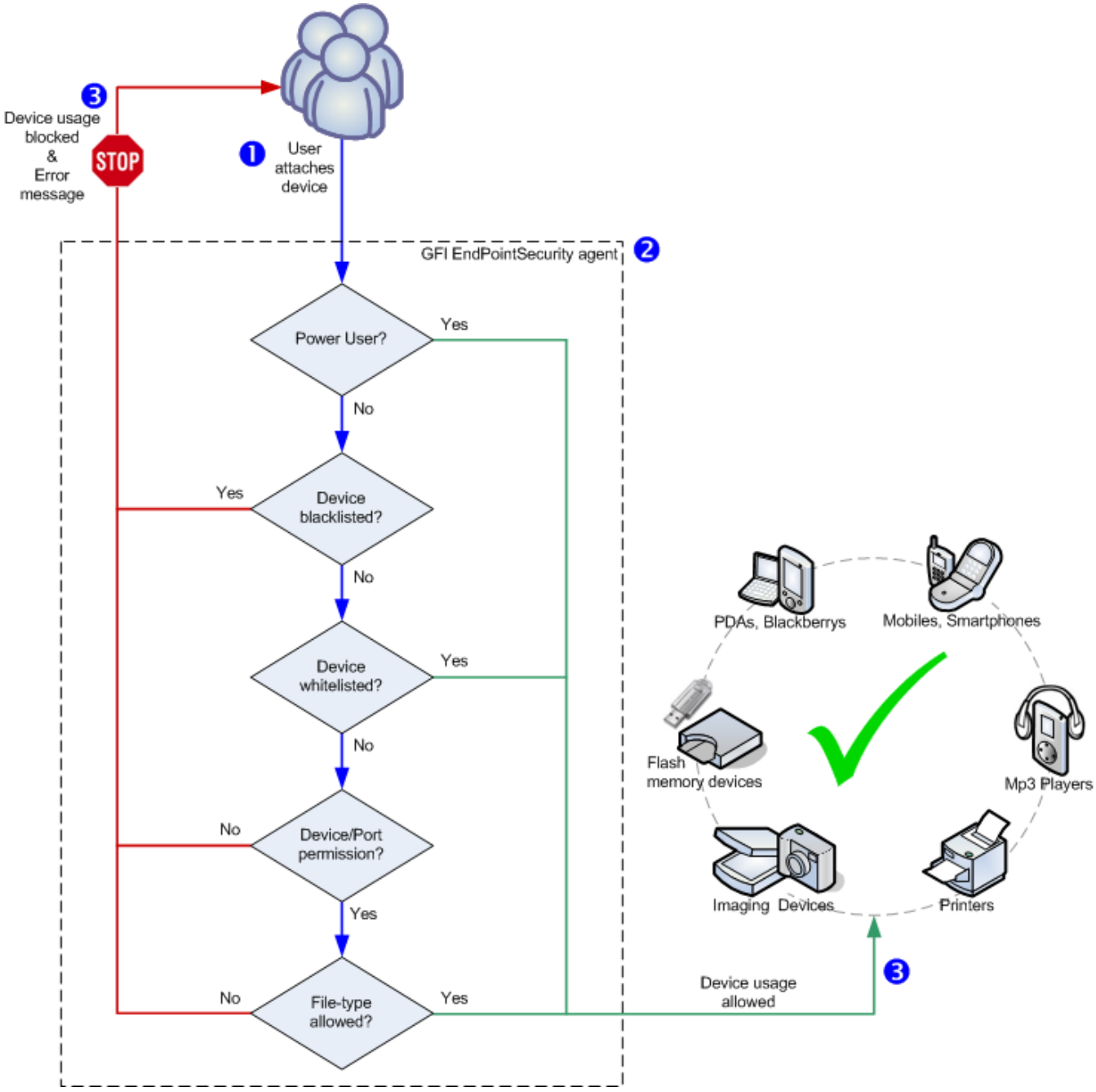


Figura 2: Acceso a dispositivos

En la siguiente tabla, se describen las etapas detalladas más arriba:

Tabla 2: Implementación y supervisión de la directiva de protección

Etapa	Descripción
Etapa 1: Dispositivo conectado a equipo	El usuario conecta un dispositivo a un equipo de destino protegido por GFI EndPointSecurity.
Etapa 2: Aplicación de directiva de protección	El agente de GFI EndPointSecurity instalado en el equipo de destino detecta el dispositivo conectado y pasa por las reglas de la directiva de protección aplicables al equipo/usuario. Esta operación determina si se permite o bloquea el acceso al dispositivo.
Etapa 3: Uso del dispositivo permitido/bloqueado	El usuario recibe un mensaje de error que indica que se ha bloqueado el uso del dispositivo o se le permite el acceso al dispositivo.

Cómo funciona GFI EndPointSecurity: Acceso temporal

Las operaciones de acceso temporal de GFI EndPointSecurity pueden dividirse en tres etapas lógicas:

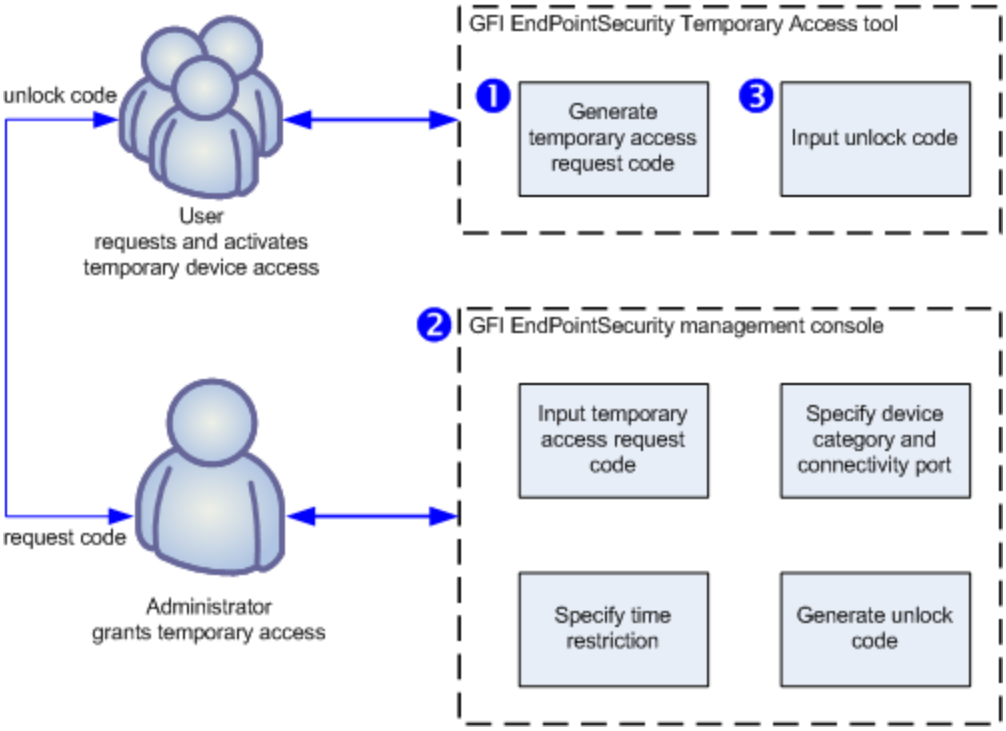


Figura 3: Solicitud/concesión de acceso temporal

En la siguiente tabla, se describen las etapas detalladas más arriba:

Tabla 3: Implementación y supervisión de la directiva de protección

Etapa	Descripción
Etapa 1: El usuario solicita acceso temporal al dispositivo	El usuario ejecuta la herramienta GFI EndPointSecurity Temporary Access desde el equipo desde el que se accederá al dispositivo. La herramienta se usa para generar un código de solicitud, que el usuario le comunica al administrador. El usuario también debe informarle al administrador sobre los tipos de dispositivos y los puertos de conexión a los que debe acceder, y durante cuánto tiempo necesita acceder a estos.
Etapa 2: El administrador otorga acceso temporal	El administrador usa la función Temporary Access dentro de la consola de administración de GFI EndPointSecurity para introducir el código de solicitud y para especificar los dispositivos/puertos y las restricciones de tiempo. Se genera un código de desbloqueo que luego el administrador le comunica al usuario.
Etapa 3: El usuario activa el acceso temporal al dispositivo	Una vez que el usuario recibe el código de desbloqueo que le envió el administrador, lo introduce en la herramienta GFI EndPointSecurity Temporary Access para activar el acceso temporal y para poder usar los dispositivos/puertos necesarios.

1.2 Componentes de GFI EndPointSecurity

Cuando instala GFI EndPointSecurity, se implementan los siguientes componentes:

- Consola de administración de GFI EndpointSecurity
- Agente de GFI EndpointSecurity

1.2.1 Consola de administración de GFI EndPointSecurity

A través de la consola de administración de GFI EndPointSecurity, puede realizar lo siguiente:

- Crear y administrar directivas de protección y especificar qué categorías de dispositivos y puertos de conectividad se deben controlar
- Implementar directivas de protección y agentes de forma remota en sus equipos de destino. Conceder acceso temporal a los equipos de destino para usar dispositivos específicos
- Ver el estado de protección de dispositivos de cada equipo supervisado
- Llevar a cabo exámenes en los equipos de destino para identificar los dispositivos conectados actual o anteriormente
- Comprobar los registros y analizar qué dispositivos han estado conectados a cada equipo de red
- Realizar un seguimiento de los equipos que tienen un agente implementado y qué agentes requieren actualizaciones.

1.2.2 Agente de GFI EndPointSecurity

El agente de GFI EndPointSecurity es un servicio del cliente responsable de la implementación de las directivas de protección en los equipos de destino. Este servicio se instala automáticamente en el equipo de destino de red remoto después de la primera implementación de la directiva de protección relevante a través de la consola de administración de GFI EndPointSecurity. En las siguientes implementaciones de la misma directiva de protección, el agente se actualizará y no se volverá a instalar.

1.3 Guía del administrador

Para obtener pautas de configuración y administración detalladas, consulte GFI EndPointSecurity - Guía del administrador, que se instala con el producto o se descarga por separado desde: http://www.gfi.com/esec/esecmanual.pdf.

La Guía del administrador complementa esta guía de inicio rápido y proporciona más información sobre el uso y la personalización de las herramientas y funciones de GFI EndPointSecurity.

1.4 Convenciones usadas en este manual

Tabla 4: Términos y convenciones que se usan en este manual

Término	Descripción
	Información adicional y referencias esenciales para la operación de GFI EndPointSecurity.
	Notificaciones y precauciones importantes sobre los problemas comunes que pueden surgir.
>	Instrucciones de navegación paso a paso para acceder a una función concreta.
Texto en negrita	Elementos que se seleccionan, como nodos, opciones de menú o botones de comando.

Término	Descripción
Texto en cursiva	Parámetros y valores que debe reemplazar por el valor aplicable, como rutas de acceso y nombres de archivo personalizados.
`Código`	Indica los valores de texto que se escriben, como comandos y direcciones.

1.5 Puertos de conectividad admitidos

GFI EndPointSecurity examina los dispositivos que están o han estado conectados en los siguientes puertos:

USB

Secure Digital (SD)

Firewire

Bluetooth

Infrarrojos

PCMCIA

Serie y paralelos

Internos (ejemplo: unidades ópticas conectadas internamente en PCI).

1.6 Categorías de dispositivos admitidas

En GFI EndPointSecurity, los dispositivos se organizan en las siguientes categorías:

Disquetes

CD/DVD

Impresoras

PDA, incluidos:

- Pocket PC
- Teléfonos inteligentes

Adaptadores de red, incluidos:

- Adaptadores Ethernet
- Adaptadores Wi-Fi
- Adaptadores extraíbles (USB, Firewire, PCMCIA)

Módems, incluidos:

- Teléfonos inteligentes
- Teléfonos móviles

Dispositivos de imágenes:

- Cámaras digitales
- Cámaras web
- Escáneres

Dispositivos de interfaz humana (HID):

- Teclados
- Mouse
- Controladores de juegos

Dispositivos de almacenamiento, incluidos:

- Pen drives USB
- Reproductores de medios digitales (por ej., reproductores de MP3/MP4)
- Lectores de tarjetas de memoria y flash
- Dispositivos USB de varias unidades (es decir, dispositivos que no se montan como una unidad única)

Otros dispositivos:

- Llaves/puertos bluetooth
- Llaves/puertos infrarrojos
- Unidades Zip
- Unidades de cinta
- Unidades magnetoópticas (internas y externas).

2 Instalación de GFI EndPointSecurity

En este capítulo, se proporciona información sobre cómo preparar su entorno de red para implementar GFI EndPointSecurity correctamente.
Temas de este capítulo

2.1 Requisitos del sistema

Requisitos de hardware

En la tabla que aparece a continuación, se muestran los requisitos de hardware para GFI EndPointSecurity y para el agente de GFI EndPointSecurity:

Tabla 5: Requisitos del sistema: Hardware

	GFI EndPointSecurity	GFI EndPointSecurityAgente
Procesador	Mínimo: 2 GHz Recomendado: 2 GHz	Mínimo: 1 GHz Recomendado: 1 GHz
RAM	Mínimo: 512 MB Recomendado: 1 GB	Mínimo: 256 MB Recomendado: 512 MB
Espacio libre	Mínimo: 100 MB Recomendado: 100 MB	Mínimo: 50 MB Recomendado: 50 MB

Sistemas operativos compatibles (x64/x86)

GFI EndPointSecurity y el agente de GFI EndPointSecurity se pueden instalar en un equipo que esté ejecutando cualquiera de los siguientes sistemas operativos:

- Microsoft Windows Server 2012
- Microsoft Windows Small Business Server 2011 (Standard Edition)
- Microsoft Windows Server 2008 R2 (Standard o Enterprise Edition)
- Microsoft Windows Server 2008 (Standard o Enterprise Edition)
- Microsoft Windows Small Business Server 2008 (Standard Edition)
- Microsoft Windows Server 2003 (Standard, Enterprise o Web Edition)
- Microsoft Windows Small Business Server 2003
- Microsoft Windows 8 (Professional o Enterprise)
- Microsoft Windows 7 (Professional, Enterprise o Ultimate Edition)
- Microsoft Windows Vista (Enterprise, Business o Ultimate Edition)
- Microsoft Windows XP Professional Service Pack 3.

Agente: Requisitos de hardware

- Procesador: Velocidad del procesador de 1 GHz o más
- RAM: 256 MB (mínimo); 512 MB (recomendado)
- Disco duro: 50 MB de espacio disponible

Agente: Requisitos de software

- Procesador: Velocidad del procesador de 1 GHz o más
- RAM: 256 MB (mínimo); 512 MB (recomendado)
- Disco duro: 50 MB de espacio disponible

Otros componentes de software

GFI EndPointSecurity requiere los siguientes componentes de software para una implementación completamente funcional:

- Microsoft Internet Explorer 5.5 o superior
- Microsoft .NET Framework 2.0 o superior
- Microsoft SQL Server 2000, 2005 o 2008 como base de datos back-end

Nota

Se requiere un back-end de base de datos para almacenar los datos de acceso a dispositivos y para los informes. GFI EndPointSecurity ofrece la opción de usar una instancia de Microsoft SQL Server disponible o descargar e instalar automáticamente Microsoft SQL Server 2005 Express en el mismo equipo donde está instalada la consola de administración de GFI EndPointSecurity.

Puertos de cortafuegos

Los agentes de GFI EndPointSecurity requieren el **puerto TCP 1116** (predeterminado) para notificarle sus estados a GFI EndPointSecurity y para enviar eventos de acceso a dispositivos. Sin este puerto abierto, el administrador debe supervisar los eventos de cada equipo de destino manual o automáticamente a través de GFI EventsManager. Para obtener más información, consulte http://www.gfi.com/eventsmanager.

2.2 Actualización de GFI EndPointSecurity

Actualización de GFI EndPointSecurity 3 o versiones posteriores

Si tiene GFI LanGuard Portable Storage Control o una versión anterior de GFI EndPointSecurity, es posible actualizar a la versión más reciente de GFI EndPointSecurity. La actualización de GFI EndPointSecurity 3 o versiones posteriores a GFI EndPointSecurity 2013 es sencilla. El proceso de actualización es parte del proceso de instalación de GFI EndPointSecurity 2013, e incluye lo siguiente:

- Desinstalación de GFI EndPointSecurity 3 o versiones posteriores
- Importación de los parámetros de configuración de GFI EndPointSecurity 3.

Al instalar GFI EndPointSecurity, se le pide que confirme si desea importar parámetros de configuración de la versión anterior. Haga clic en **Yes** para importar parámetros de configuración. A continuación, se le pide que especifique cuáles de los siguientes parámetros de configuración desea importar:

- Directivas de protección:
  - Equipo
  - Configuración de seguridad
- Opciones:
  - Opciones de inicio de sesión
  - Opciones de base de datos.

Actualización de GFI LanGuard Portable Storage Control

Si el equipo en el que está instalando GFI EndPointSecurity está protegido con un agente de GFI LanGuardPortable Storage Control, primero debe desinstalar el agente. Para ello:

1. Abra la consola de configuración de GFI LanGuard Portable Storage Control.

2. Elimine el agente del equipo donde se instalará GFI EndPointSecurity.

> **Nota**
>
> Este proceso debe realizarse únicamente para el equipo donde se instalará GFI EndPointSecurity.

3. Cierre la aplicación de la consola de configuración de GFI LanGuard Portable Storage Control y continúe con la instalación de GFI EndPointSecurity.

4. Al instalar GFI EndPointSecurity, se le pide que confirme si desea importar parámetros de configuración de la versión anterior. Haga clic en **Yes** para importar parámetros de configuración.

> **Nota**
>
> Los agentes de GFI LanGuard Portable Storage Control que estaban protegiendo los equipos se agregarán automáticamente a una directiva de protección llamada **LegacyAgents** en GFI EndPointSecurity.

2.3 Instalación de una nueva instancia de GFI EndPointSecurity

Para instalar GFI EndPointSecurity:

1. Inicie sesión en el equipo donde se instalará GFI EndPointSecurity, con privilegios administrativos.

2. Haga doble clic en el archivo ejecutable GFI EndPointSecurity.

2. Seleccione el idioma que desee instalar y haga clic en **OK**.

3. Haga clic en **Next** en la pantalla de bienvenida para comenzar la configuración.

4. Lea detenidamente el Acuerdo de licencia para el usuario final. Si está de acuerdo con los términos descritos en el acuerdo, seleccione **I accept the license agreement** y haga clic en **Next**.

Captura de pantalla 1: Instalación de GFI EndPointSecurity: Configuración de la cuenta de administrador de dominio

5. Escriba las credenciales de inicio de sesión de una cuenta con privilegios administrativos y haga clic en **Next** para continuar.

Captura de pantalla 2: Instalación de GFI EndPointSecurity: Detalles de la clave de licencia

6. Complete los campos **Full Name** y **Company**. Si tiene una clave de licencia, actualice los detalles de **License Key** y haga clic en **Next**.

> **Nota**
>
> La clave de licencia se puede completar después de la instalación o del vencimiento del periodo de evaluación de GFI EndPointSecurity. Para obtener más información, consulte Licencias del producto (página 28).

7. Escriba o seleccione una ruta de instalación alternativa, o haga clic en **Next** para usar la ruta predeterminada y continuar con la instalación.

8. Haga clic en **Back** para volver a introducir la información de instalación o haga clic en **Next** y espere que finalice la instalación.

9. Cuando se complete la instalación, habilite o deshabilite la casilla de verificación Launch GFI EndPointSecurity y haga clic en **Finish** para finalizar la instalación.

2.4 Parámetros de configuración posteriores a la instalación

En el primer inicio de la consola de administración de GFI EndPointSecurity, se abre automáticamente el asistente para inicio rápido. Esto le permite configurar parámetros importantes de GFI EndPointSecurity para el uso inicial.

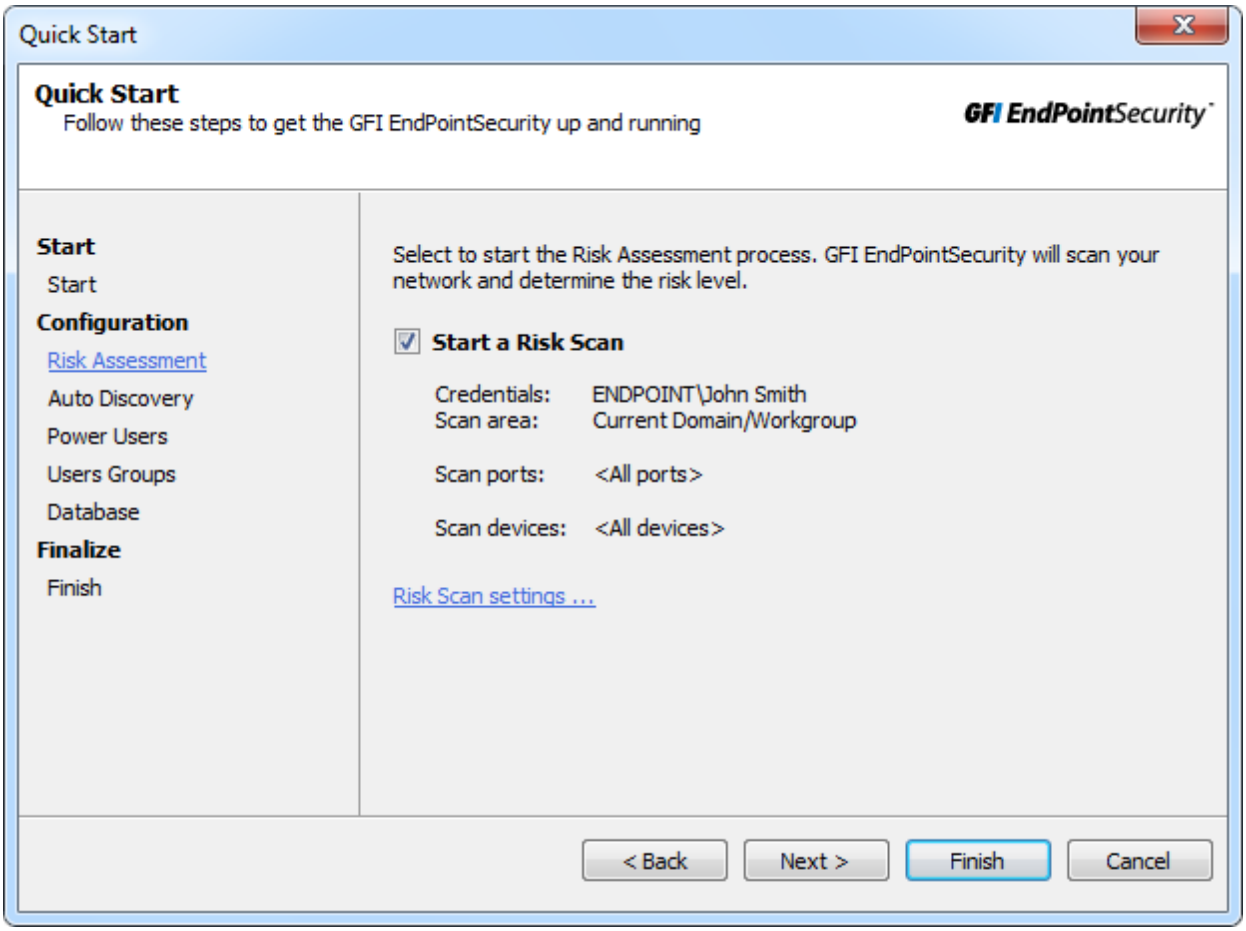
El asistente para inicio rápido consta de los siguientes pasos y guías para que configure:

- Evaluación de riesgos
- Detección automática
- Usuarios avanzados
- Grupos de usuarios
- Back-end de base de datos.

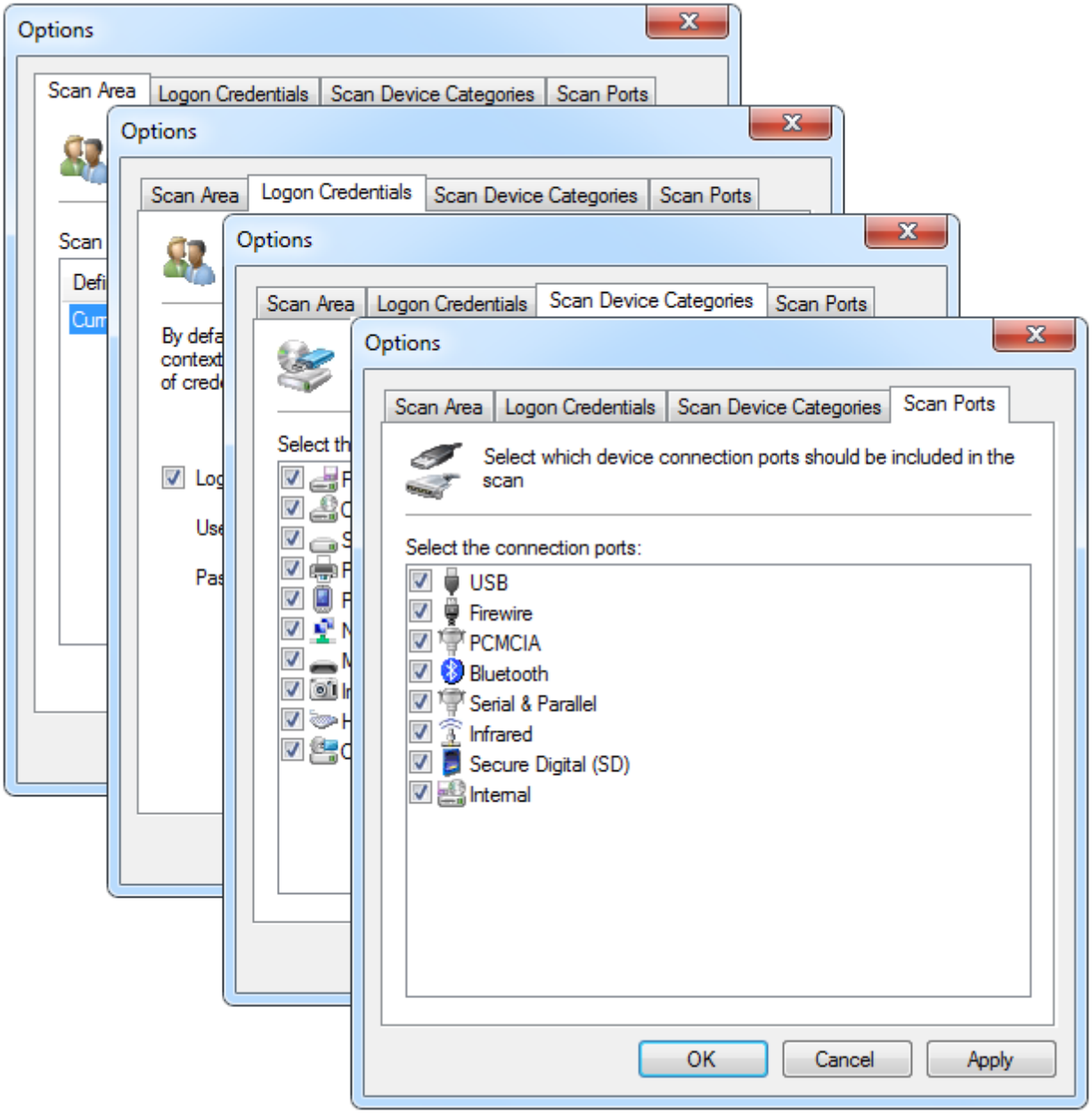
> **Nota**
>
> El asistente para inicio rápido se puede volver a iniciar desde **File > Quick Start Wizard**.

Para usar el asistente para inicio rápido:

1. Haga clic en **Next** en la pantalla de bienvenida del asistente.



2. En **Risk Assessment**, seleccione o anule la selección de **Start a Risk Scan** para habilitar o deshabilitar la función que inicia un examen de la red para determinar el nivel de riesgo.

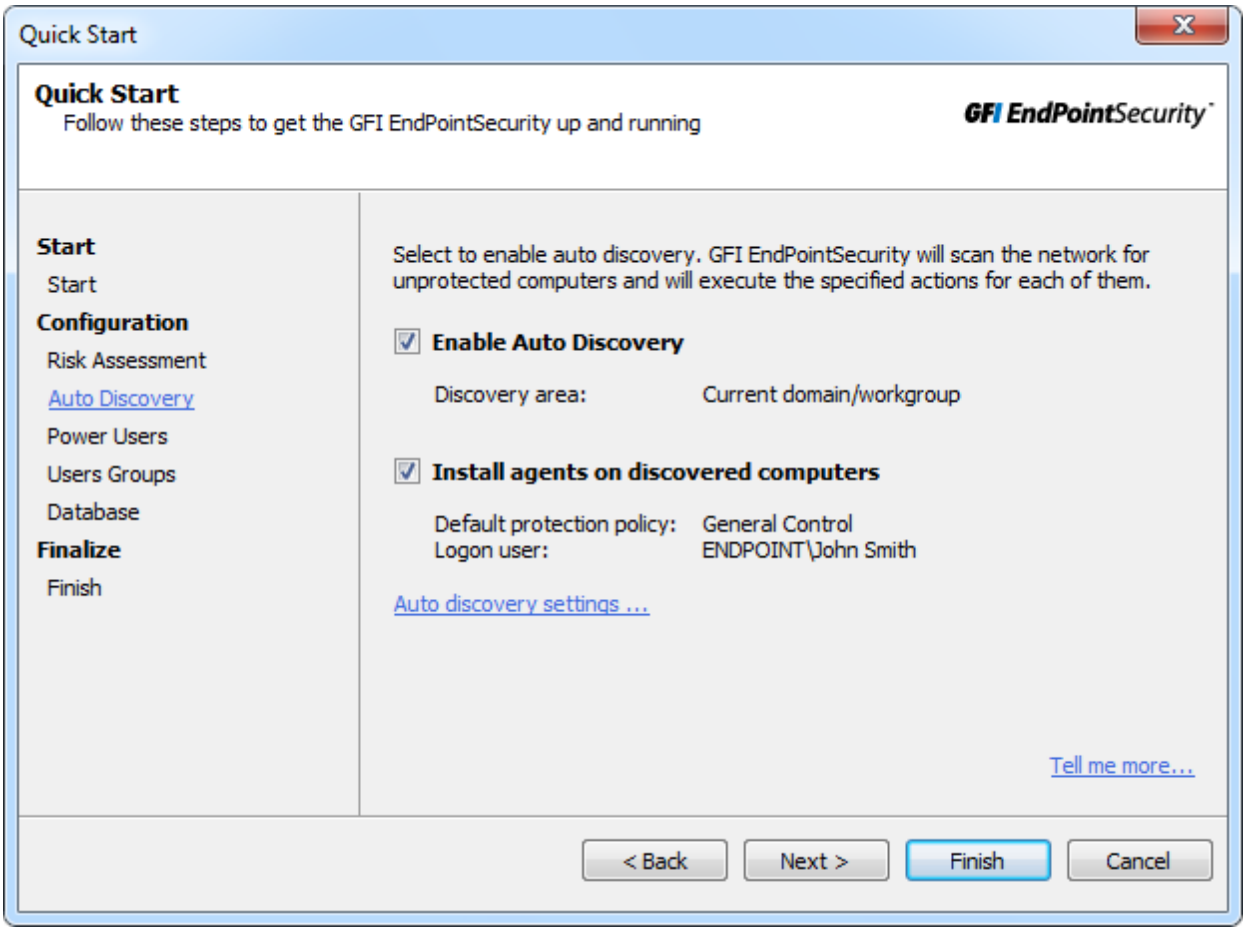


3. Opcionalmente, haga clic en **Risk scan settings...** y configure los parámetros para las fichas que se describen a continuación:

Tabla 6: Configuración de detección automática

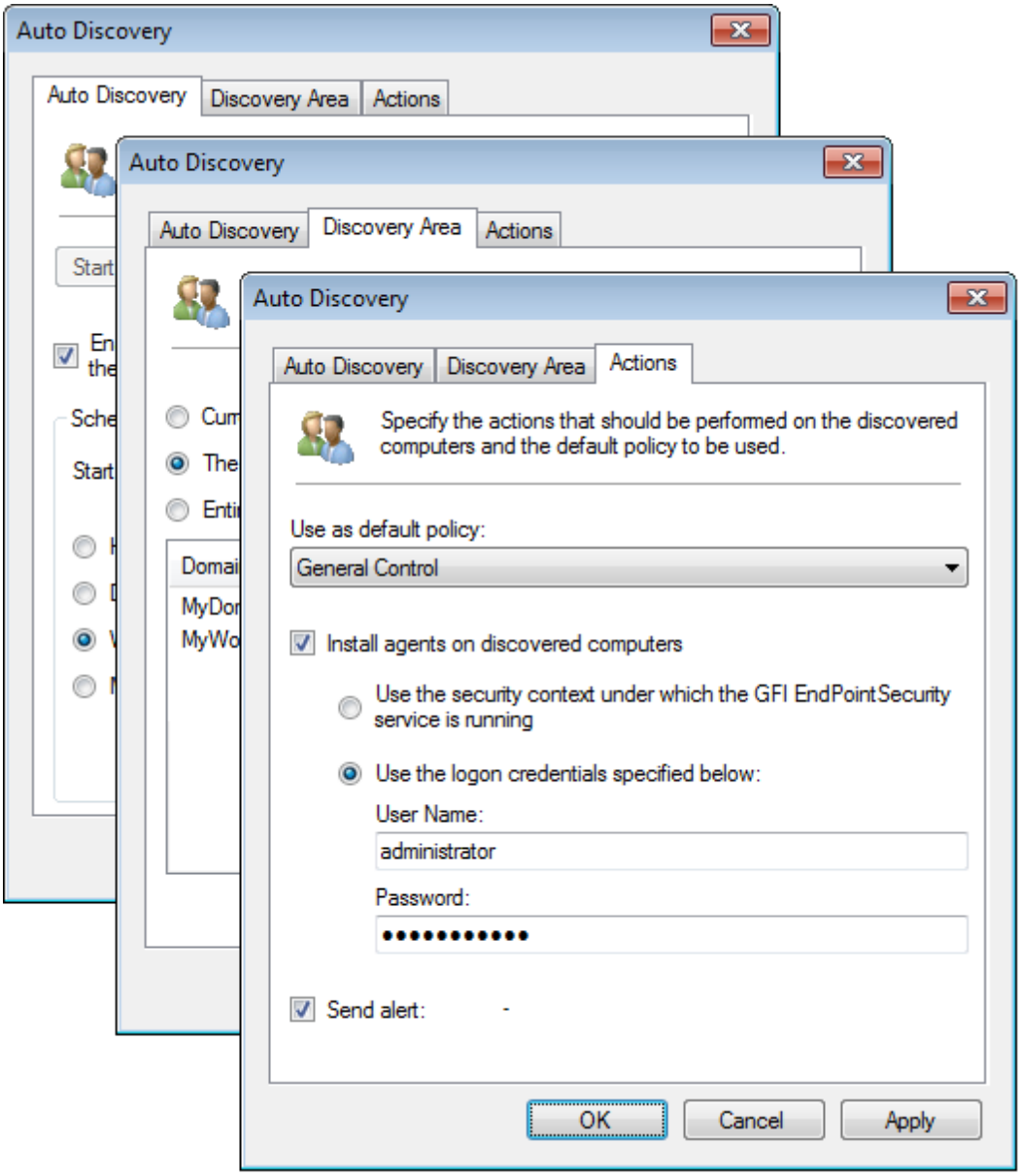
Ficha	Descripción
Scan Area	Seleccione el área de destino en el cual GFI EndPointSecurity examina los equipos en la red. » **Current domain/workgroup**: GFI EndPointSecurity busca equipos nuevos dentro del mismo dominio/grupo de trabajo donde está instalado. » **The following domains/workgroups**: Seleccione esta opción y haga clic en **Add**. Especifique los dominios donde GFI EndPointSecurity buscará equipos nuevos y haga clic en **OK**. » **Entire network except**: Seleccione esta opción y haga clic en **Add**. Especifique el dominio o grupo de trabajo que se debe ejecutar durante la detección automática y haga clic en **OK**. » **IP range**: Seleccione esta opción y haga clic en **Add**. Especifique el rango de direcciones IP que deben incluirse o ejecutarse durante la detección automática y haga clic en **OK**. » **Computer list**: Seleccione esta opción y haga clic en **Add**. Especifique el dominio o grupo de trabajo que se debe incluir o ejecutar durante la detección automática y haga clic en **OK**.
Logon Credentials	Habilite o deshabilite **Logon using credentials below** y especifique un conjunto de credenciales que GFI EndPointSecurity usará para acceder a los equipos que se examinarán.
Scan Device Categories	Seleccione las categorías de dispositivos que GFI EndPointSecurity incluirá en el examen.
Scan ports	Seleccione los puertos de conexión de dispositivos que GFI EndPointSecurity incluirá en el examen.

4. Haga clic en **Apply** y en **OK** para cerrar el cuadro de diálogo Risk Assessment y haga clic en **Next** en el asistente para inicio rápido.



5. En **Auto Discovery**, seleccione o anule la selección de **Enable Auto Discovery** para activar o desactivar la detección automática. Cuando la detección automática está habilitada, GFI EndPointSecurity examina periódicamente su red para detectar equipos nuevos.

6. Seleccione o anule la selección de **Install agents on discovered computers** para habilitar o deshabilitar la implementación automática de agentes de GFI EndPointSecurity en equipos recientemente detectados.



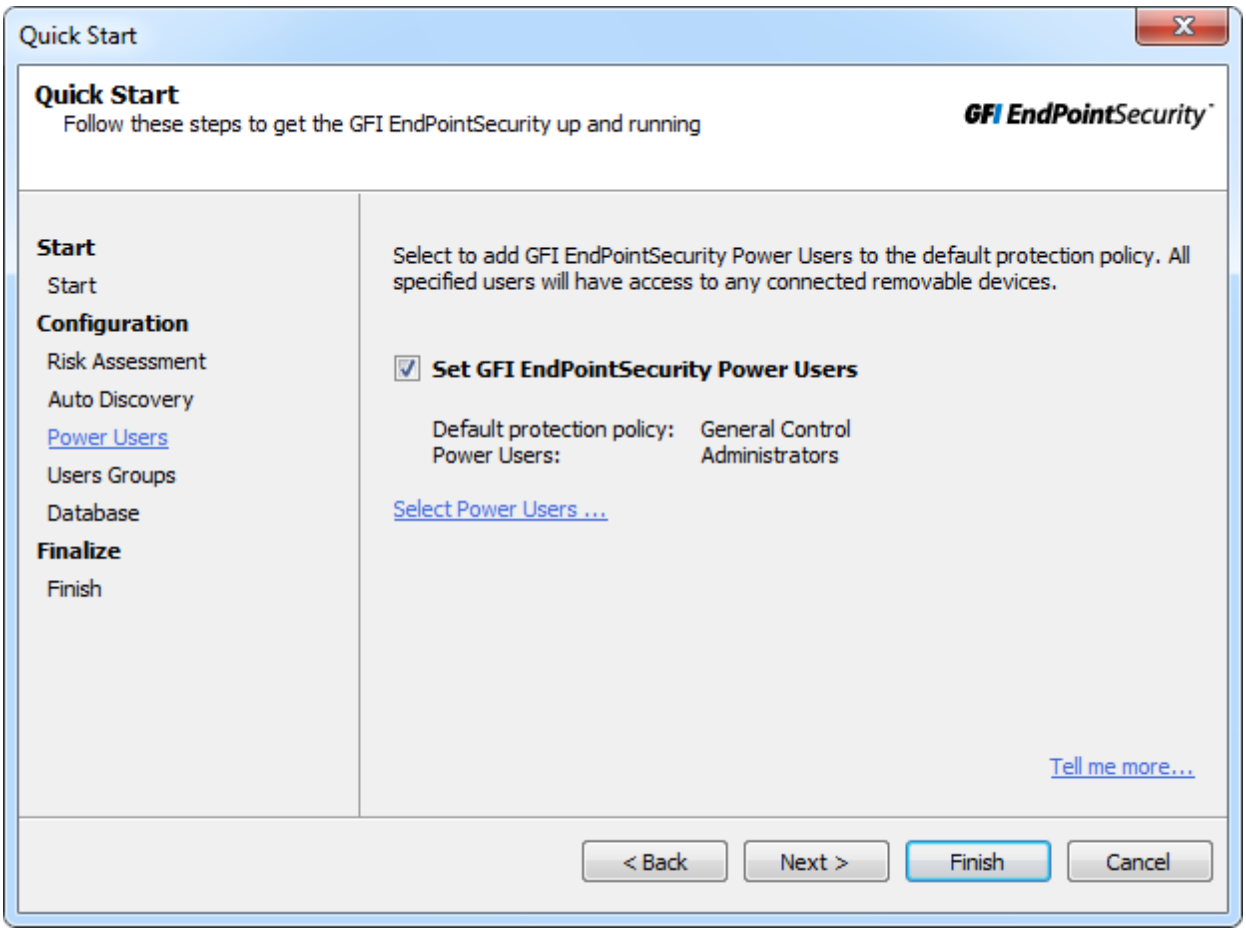
7. Opcionalmente, haga clic en **Auto discovery settings...** y configure los parámetros para las fichas que se describen a continuación:

Tabla 7: Configuración de detección automática

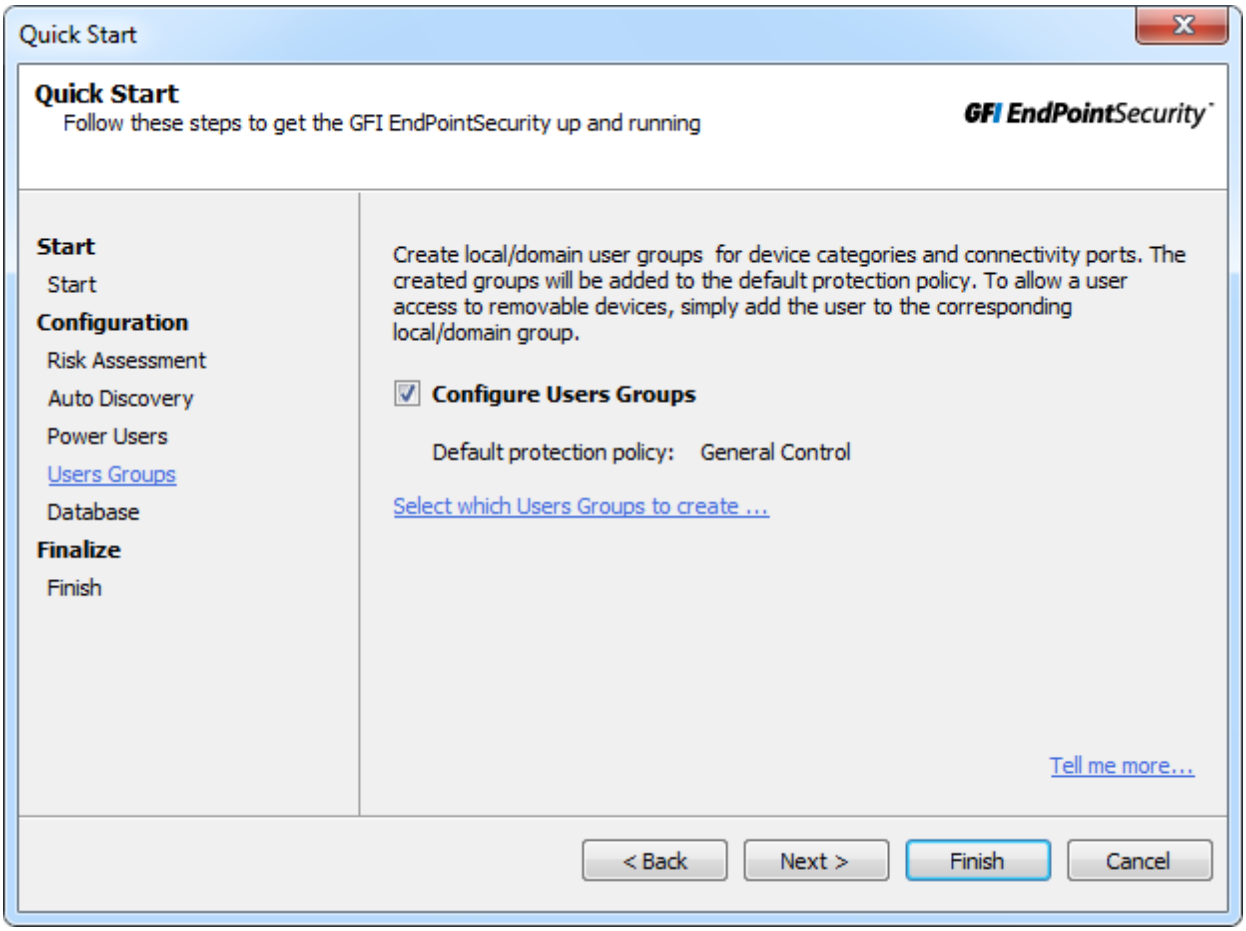
Ficha	Descripción
Auto Discovery	Habilite o deshabilite la detección automática y configure una programación para que GFI EndPointSecurity examine la red para detectar equipos nuevos.
Discovery Area	Seleccione dónde desea que GFI EndPointSecurity busque equipos nuevos. Seleccione una de las siguientes opciones: » **Current domain/workgroup**: GFI EndPointSecurity busca equipos nuevos dentro del mismo dominio/grupo de trabajo donde está instalado. » **The following domains/workgroups**: Seleccione esta opción y haga clic en **Add**. Especifique los dominios donde GFI EndPointSecurity buscará equipos nuevos y haga clic en **OK**. » **Entire network except**: Seleccione esta opción y haga clic en **Add**. Especifique el dominio o grupo de trabajo que se debe ejecutar durante la detección automática y haga clic en **OK**.

Ficha	Descripción
Actions	Configure las acciones que realiza GFI EndPointSecurity cuando se detecta un equipo nuevo. Además, seleccione la directiva a la que se aplica esta configuración.

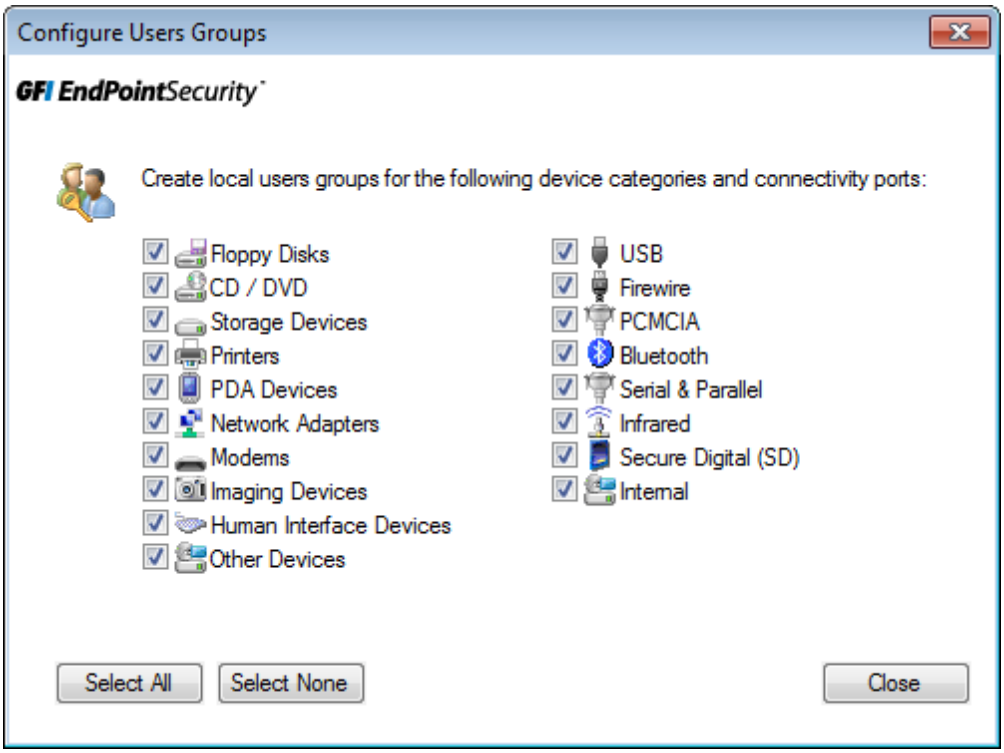
8. Haga clic en **Apply** y en **OK** para cerrar el cuadro de diálogo Auto Discovery y haga clic en **Next** en el asistente para inicio rápido.



9. En **Power Users**, seleccione o anule la selección de **Set GFI EndPointSecurity Power Users** para habilitar o deshabilitar las funciones de usuarios avanzados. Los miembros del grupo de usuarios avanzados tienen acceso a cualquier dispositivo conectado en efecto mediante esta directiva.
10. Haga clic en **Select Power Users...** y, en el cuadro de diálogo Power Users, haga clic en **Add...** para agregar usuarios a su dominio/grupo de trabajo.
11. Haga clic en **Apply** y en **OK** para cerrar el cuadro de diálogo Power Users y haga clic en **Next** en el asistente para inicio rápido.

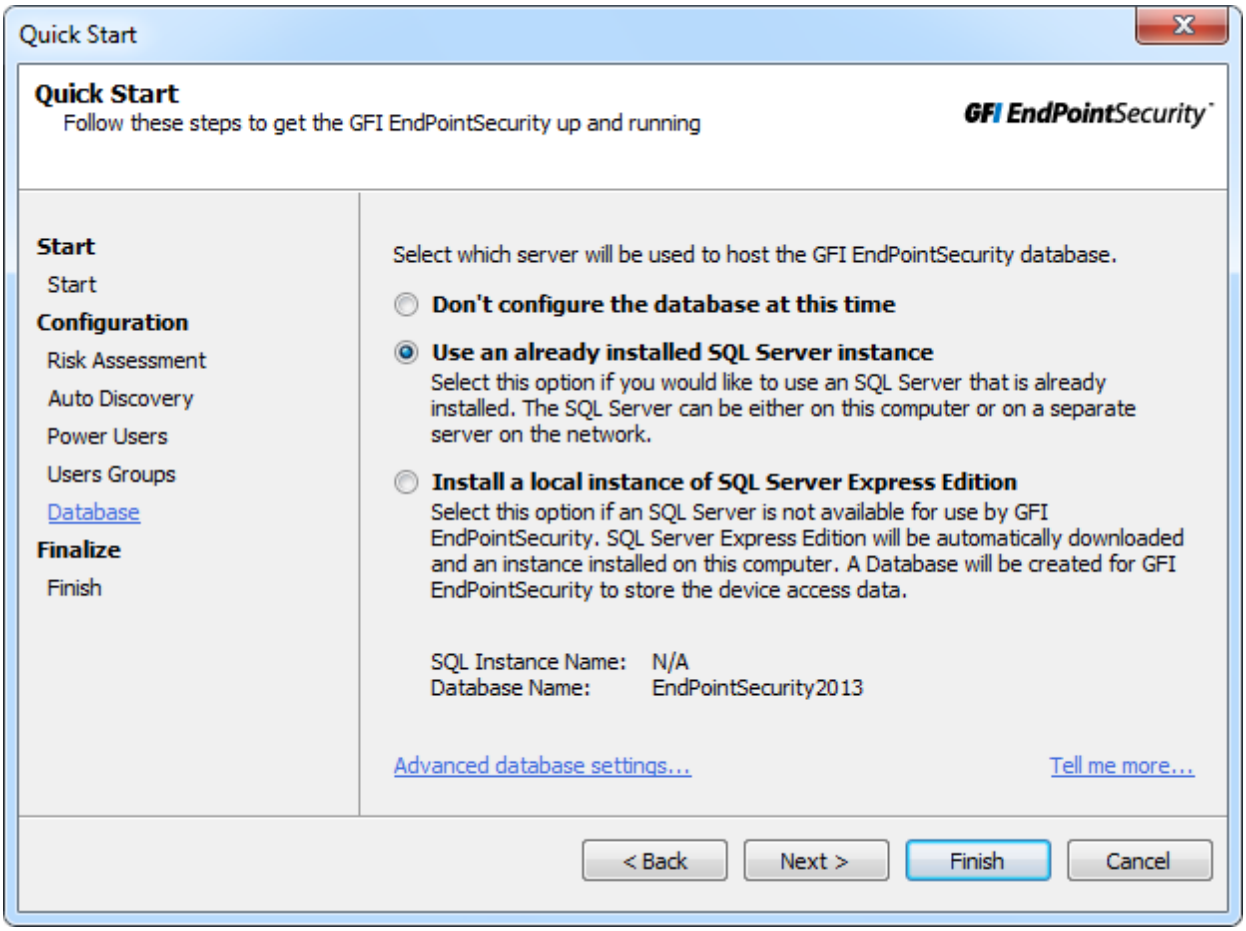


12. En **Users Groups**, seleccione o anule la selección de **Configure Users Groups** para crear usuarios del dominio/grupo de trabajo y enlazarlos con parámetros de configuración de categorías de dispositivos y puertos de conectividad seleccionados en el paso siguiente.



13. Haga clic en **Select which Users Groups to create...**. En el cuadro de diálogo Configure Users Groups, seleccione los dispositivos o puertos de conexión para los cuales se crean los usuarios. Para administrar todos los dispositivos y puertos admitidos desde esta directiva, haga clic en **Select All**.

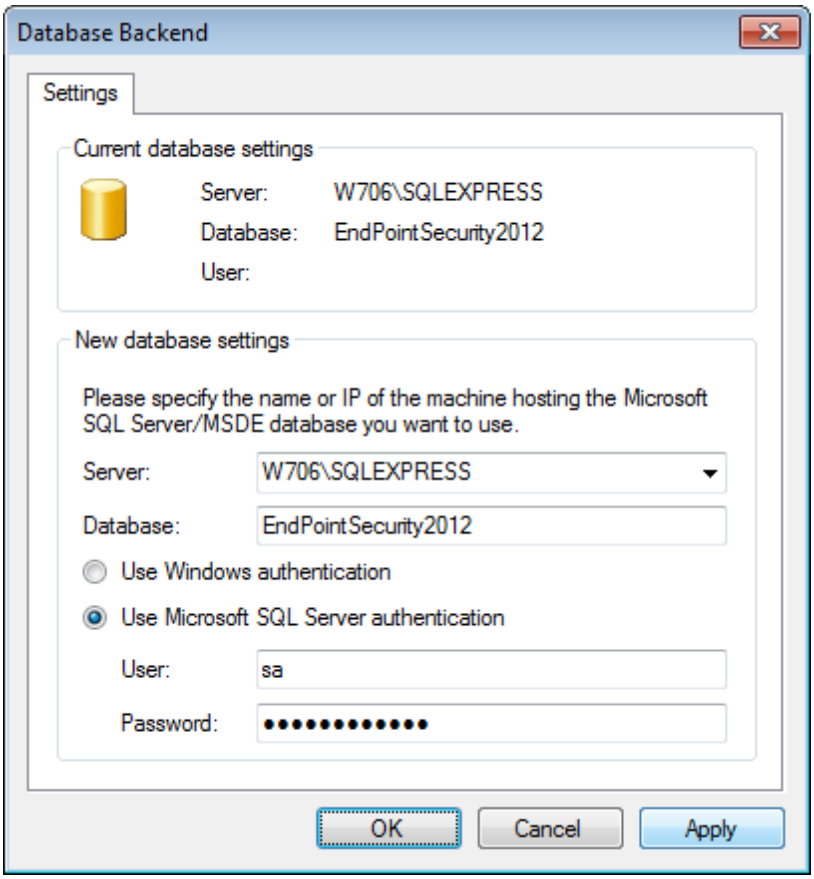
14. Haga clic en **Close** para cerrar **Configure Users Groups** y haga clic en **Next** en el asistente para inicio rápido.



15. Desde Database, seleccione el tipo de base de datos que desee usar como back-end de base de datos. Seleccione entre las opciones que se describen a continuación:

Tabla 8: Opciones de back-end de base de datos

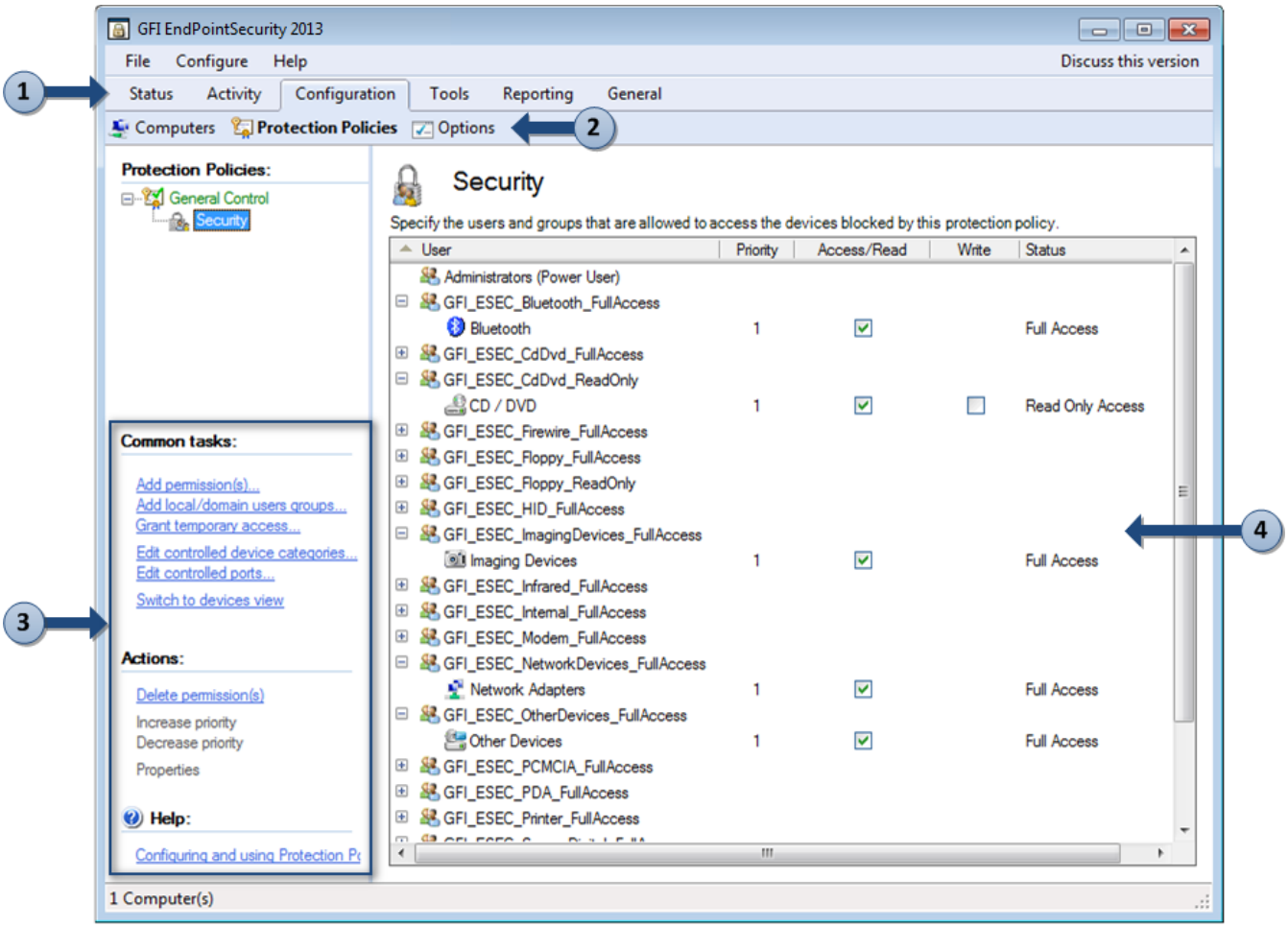
Opción	Descripción
Don't configure the database at this time	Finalice el asistente para inicio rápido y configure el back-end de base de datos más tarde. Para obtener más información, consulte ACM.
Use an already installed SQL Server instance	Use una instancia de Microsoft SQL Server que ya esté instalada en el mismo equipo en el que está instalando GFI EndPointSecurity o en otro equipo de la red.
Install a local instance of SQL Express Edition	Seleccione esta opción para descargar e instalar una instancia de Microsoft SQL Server Express en el mismo equipo en el que está instalando GFI EndPointSecurity. Se requiere una conexión a Internet.



16. Opcionalmente, haga clic en **Advanced database settings...** para especificar la dirección de SQL Server, el nombre de la base de datos, el método de inicio de sesión y las credenciales respectivas. Haga clic en **Apply** y en **OK** para cerrar el cuadro de diálogo Database Backend.
17. Haga clic en **Next** y espere que se aplique la configuración. Haga clic en **Finish** para cerrar el asistente para inicio rápido.

2.5 Exploración de la consola de administración

La consola de administración de GFI EndPointSecurity le proporciona todas las funciones de administración para supervisar y administrar el uso de acceso a dispositivos.



Captura de pantalla 3: Exploración de la interfaz de usuario de GFI EndPointSecurity

La consola de administración de GFI EndPointSecurity consta de las secciones que se describen a continuación:

Sección	Descripción
1	**Fichas** Explore entre las diferentes fichas de la consola de administración de GFI EndPointSecurity. Las fichas disponibles son las siguientes: » **Status**: Supervise el estado de GFI EndPointSecurity y la información estadística sobre el acceso a dispositivos. » **Activity**: Supervise los dispositivos utilizados en la red. » **Configuration**: Acceda y configure las directivas de protección predeterminadas. » **Scanning**: Examine los equipos de destino y detecte dispositivos conectados. » **Reporting**: Descargue o inicie GFI EndPointSecurity GFI ReportPack para generar sus informes. » **General**: Compruebe si hay actualizaciones de GFI EndPointSecurity, así como detalles de licencias y de la versión.
2	**Subfichas** Acceda a más parámetros de configuración o información acerca de la ficha seleccionada de la sección 1.
3	**Panel izquierdo** Acceda a las opciones de configuración proporcionadas en GFI EndPointSecurity. Las opciones de configuración se agrupan en tres secciones, que incluyen **Common Tasks**, **Actions** y **Help**. Están disponibles solo para algunas fichas.

Sección	Descripción
	**Panel derecho** Configure las opciones de configuración seleccionadas del panel izquierdo. Están disponibles solo para algunas fichas.

3 Prueba de la instalación

Una vez que GFI EndPointSecurity esté instalado y se haya completado el asistente para inicio rápido, pruebe su instalación para asegurarse de que GFI EndPointSecurity funcione correctamente. Siga las instrucciones que se incluyen en esta sección para verificar que la instalación de GFI EndPointSecurity y las operaciones de la directiva de protección predeterminada de envíos funcionen correctamente.

Temas de este capítulo

3.1 Condiciones previas a la prueba

Las siguientes condiciones previas a la prueba y configuraciones se requieren ÚNICAMENTE para esta prueba:

Configuración del dispositivo

Para la siguiente prueba se requiere:

- Unidad de CD/DVD conectada al equipo local
- Disco de CD/DVD que incluya contenido accesible (preferentemente un disco a cuyo contenido se haya podido acceder antes de la instalación GFI EndPointSecurity).

> **Nota**
>
> Pueden usarse otros dispositivos y medios, como disquetes o pen drives.

Cuentas de usuario

Para esta prueba, asegúrese de tener dos cuentas de usuario disponibles en el mismo equipo donde está instalado GFI EndPointSecurity:

- Una sin privilegios administrativos
- Otra con privilegios administrativos.

Parámetros de configuración

La configuración del asistente para inicio rápido le permite ajustar GFI EndPointSecurity para que se adapte a las necesidades de su compañía, que pueden no coincidir con los parámetros de configuración anteriores a la prueba necesarios. Como resultado, algunos parámetros de configuración de GFI EndPointSecurity deben establecerse como se indica a continuación para que la prueba se realice correctamente:

- Asegúrese de que el equipo local esté incluido en la vista **Status > Agents**. Si el equipo local no está incluido, inclúyalo manualmente en la lista de equipos. Para obtener más información, consulte el manual de administración y configuración de GFI EndPointSecurity.
- Asegúrese de que la directiva de protección predeterminada de envíos esté implementada y actualizada en el equipo local. Para verificarlo, en la vista **Status > Agents** compruebe que:

- la directiva de protección esté ajustada en control general
- la implementación esté actualizada
- el equipo local esté conectado.

> **Nota**
>
> Si la implementación del agente en el equipo local no está actualizada, implemente el agente manualmente. Para obtener más información, consulte el manual de administración y configuración de GFI.

» Asegúrese de que la cuenta de usuario sin privilegios administrativos no esté configurada como usuario avanzado en la directiva de protección de control general (directiva de protección pre-determinada de envíos).

> **Nota**
>
> Si la cuenta de usuario está establecida como usuario avanzado, elimínela manualmente del grupo de usuarios avanzados de la directiva de protección de control general (directiva de protección predeterminada de envíos). Para obtener más información, consulte el manual de administración y configuración de GFI EndPointSecurity.

3.2 Caso de prueba

Acceso a un disco de CD/DVD

Cuando se cumplan las condiciones previas a la prueba descritas anteriormente, los usuarios no administrativos ya no tendrán acceso a los dispositivos o puertos conectados al equipo local.

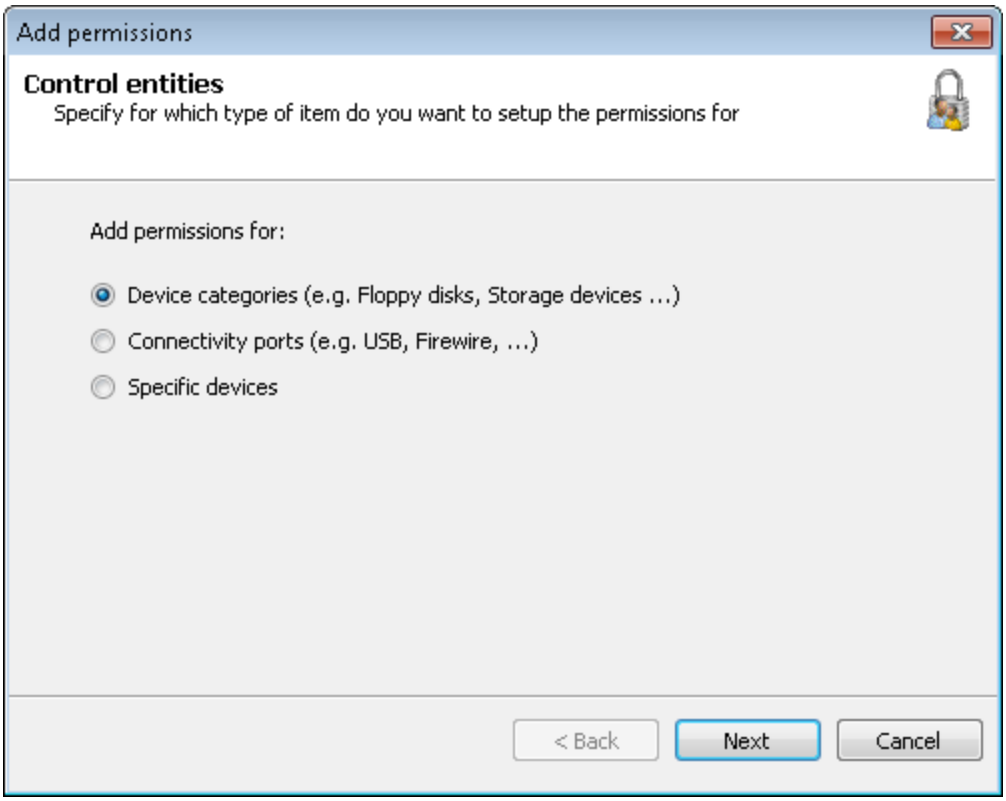
Para verificar que el usuario no administrativo no tenga acceso al dispositivo ni a los medios:

1. Inicie sesión en el equipo local como usuario sin privilegios administrativos.
2. Inserte el disco de CD/DVD en la unidad de CD/DVD.
3. En el **Explorador de Windows**, ubique la unidad de CD/DVD y confirme que no puede ver ni abrir el contenido almacenado en el disco de CD/DVD.

Asignación de permisos a usuarios sin privilegios administrativos

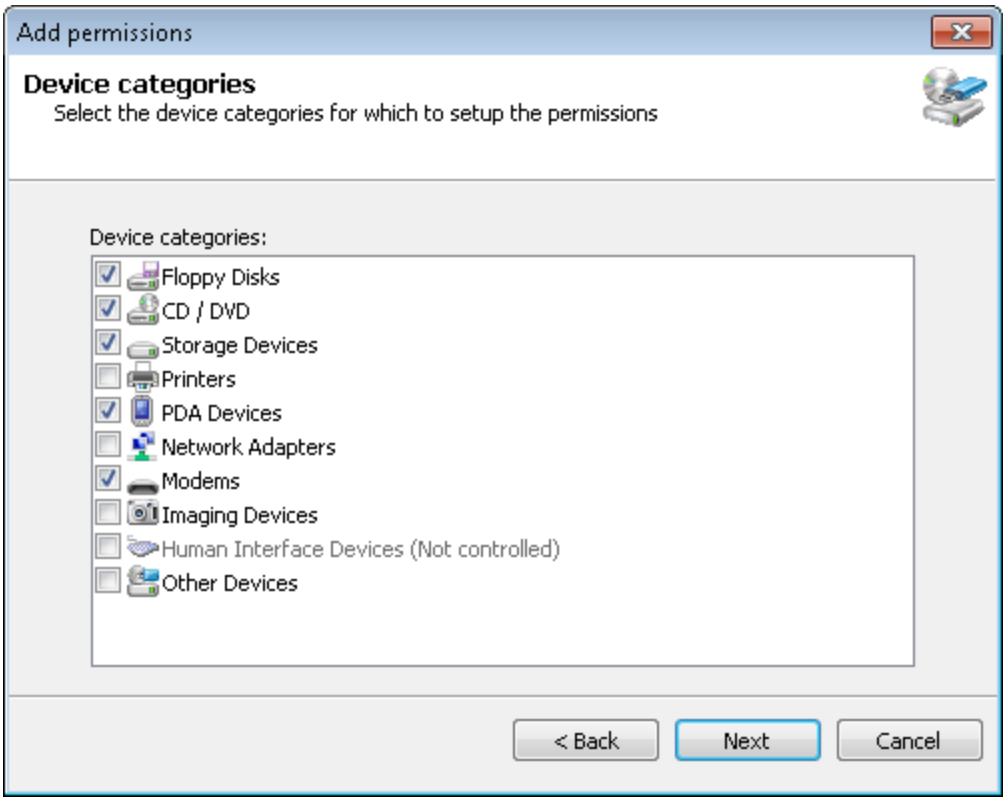
Para asignar permisos de acceso a dispositivos de CD/DVD al usuario sin privilegios administrativos:

1. Inicie sesión en el equipo local como usuario con privilegios administrativos.
2. Inicie GFI EndPointSecurity.
3. Haga clic en la ficha **Configuration**.
4. Haga clic en la subficha **Protection Policies**.
5. En el panel izquierdo, seleccione la directiva de protección **General Control**.
6. Haga clic en el subnodo **Security**.
7. En la sección **Common tasks** del panel izquierdo, haga clic en el hipervínculo **Add permission(s)…**.



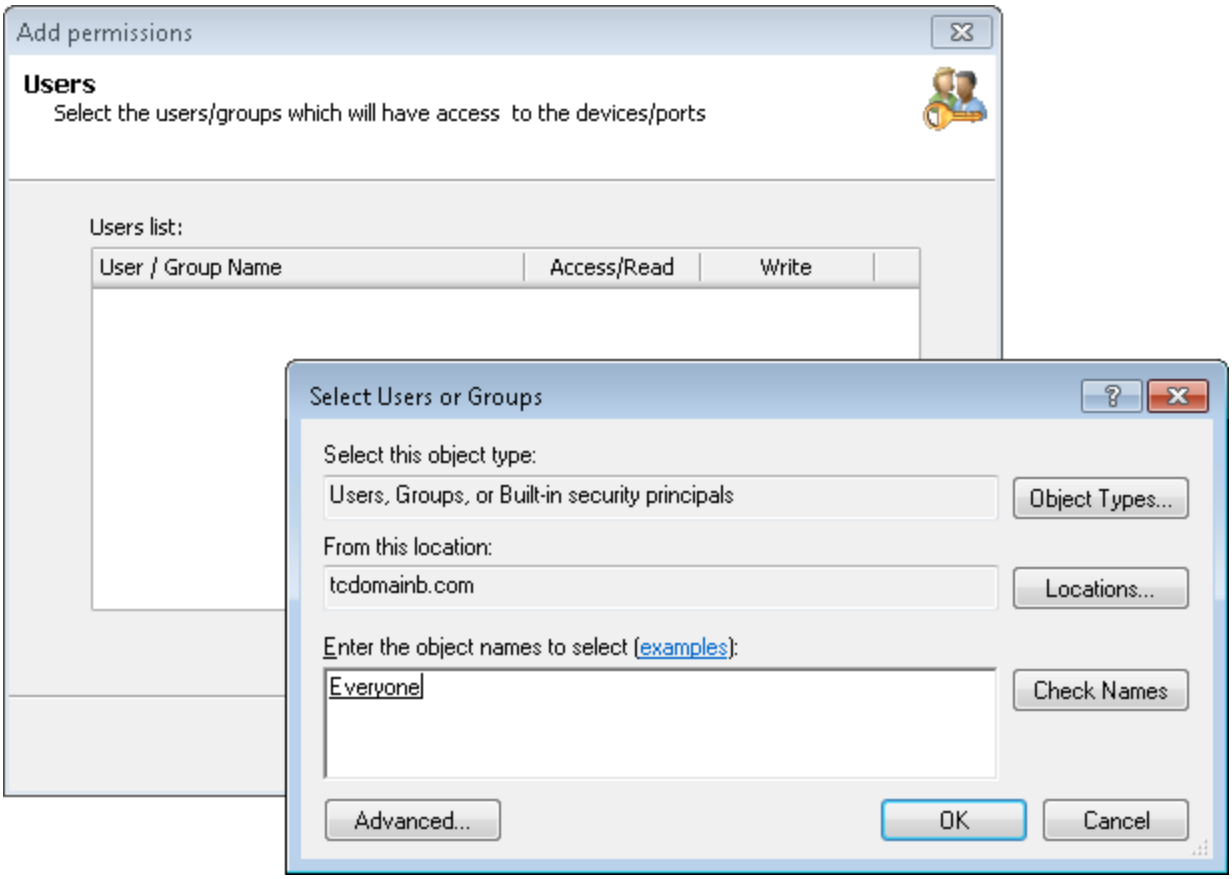
Captura de pantalla 4: Selección de entidades de control

8. En el cuadro de diálogo **Add permissions...**, seleccione la opción **Device categories** y haga clic en **Next** para continuar.



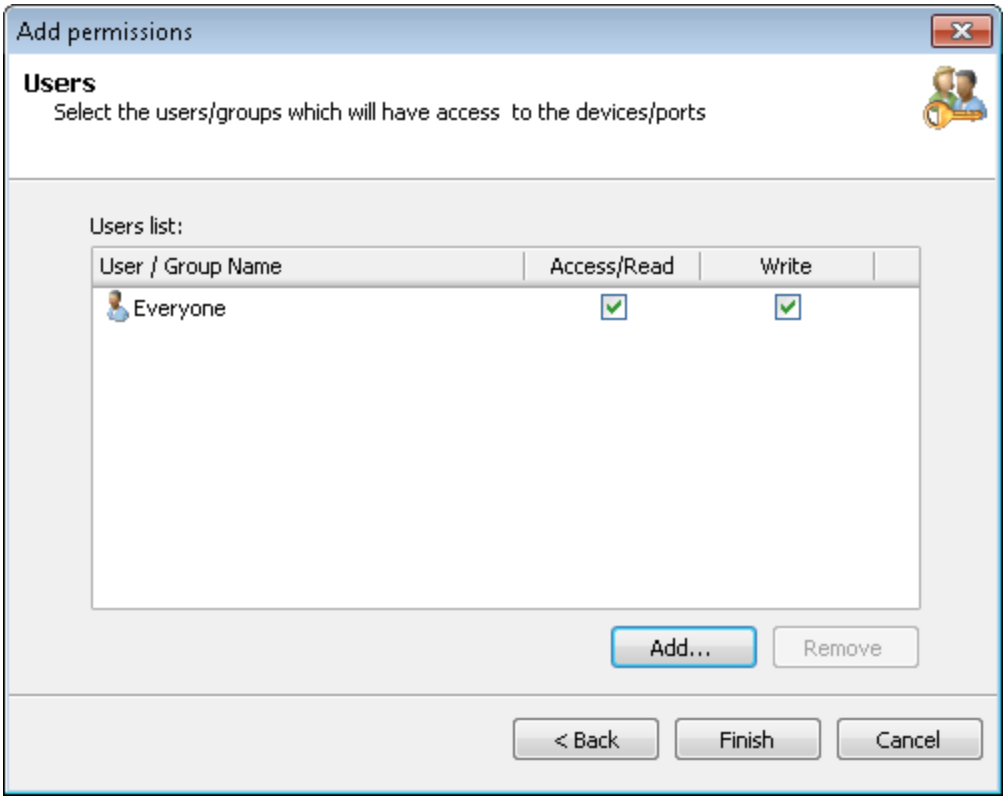
Captura de pantalla 5: Selección de categorías de dispositivos para asignar permisos

9. Habilite la categoría de dispositivo **CD/DVD** y haga clic en **Next**.



Captura de pantalla 6: Incorporación de usuarios o grupos

10. Haga clic en **Add…** y especifique el usuario sin privilegios administrativos que tendrá acceso a la categoría de dispositivo CD/DVD especificada en esta directiva de protección y, a continuación, haga clic en **OK**.



Captura de pantalla 7: Selección de tipos de permisos por usuario o grupo

11. Habilite los permisos **Access/Read** y **Write** y haga clic en **Finish**.

Para implementar actualizaciones de la directiva de protección en el equipo local:

1. En el panel derecho, haga clic en el mensaje de advertencia superior para implementar las actualizaciones de la directiva de protección. La vista debe cambiar automáticamente a **Status > Deployment**.

2. En el área **Deployment History**, confirme que la actualización en el equipo local haya finalizado correctamente.

Nuevo acceso a un disco de CD/DVD

Una vez que se asignen permisos de usuario, el usuario especificado sin privilegios administrativos ahora debe poder acceder a los discos de CD/DVD a través de unidades de CD/DVD conectadas al equipo local.

Para verificar que el usuario no administrativo ahora pueda acceder al dispositivo y a los medios:

1. Inicie sesión en el equipo local como usuario sin privilegios administrativos.

2. Inserte el mismo disco de CD/DVD en la unidad de CD/DVD.

3. En el **Explorador de Windows**, ubique la unidad de CD/DVD y confirme que ahora puede ver y abrir el contenido almacenado en el disco de CD/DVD.

3.3 Volver a la configuración predeterminada

Para volver los parámetros de configuración de GFI EndPointSecurity al escenario anterior a la prueba, realice lo siguiente para el usuario sin privilegios administrativos:

1. Si se creó únicamente para esta prueba y ya no es necesaria, quite la cuenta de usuario del equipo local.

2. Incluya al usuario manualmente en la lista de usuarios avanzados, si se configuró como un usuario avanzado antes de esta prueba. Para obtener más información, consulte el manual de administración y configuración de GFI EndPointSecurity.

3. Elimine los permisos de acceso a dispositivos de CD/DVD para el usuario, si no tenía permisos de acceso a dispositivos de CD/DVD antes de esta prueba. Para obtener más información, consulte el manual de administración y configuración de GFI EndPointSecurity.

4 Varios

En el capítulo sobre varios, se recopila toda la demás información que no se relaciona con la configuración inicial de GFI EndPointSecurity.

Temas de este capítulo

4.1 Licencias del producto

Después de instalar GFI EndPointSecurity, puede introducir su clave de licencia sin volver a instalar ni configurar la aplicación.

Para introducir la clave de licencia:

1. Haga clic en la ficha **General**.
2. En el panel izquierdo, seleccione **Licensing**.

Captura de pantalla 8: Edición de la clave de licencia

3. En el panel derecho, haga clic en **Edit…**.
4. En el cuadro de texto **License Key**, escriba la clave de licencia proporcionada por GFI Software Ltd.
5. Haga clic en **OK** para aplicar la clave de licencia.

4.2 Información de versión del producto

GFI Software Ltd. lanza actualizaciones del producto que pueden descargarse manual o automáticamente del sitio web de GFI.

Para comprobar si hay una versión más reciente de GFI EndPointSecurity disponible para descargar:

1. Haga clic en la ficha **General**.
2. En el panel izquierdo, seleccione **Version Information**.
3. En el panel derecho, haga clic en **Check for newer version** para comprobar manualmente si hay una versión más reciente de GFI EndPointSecurity disponible. Como alternativa, seleccione **Check for newer version at startup** para comprobar automáticamente si hay una versión más reciente de GFI EndPointSecurity disponible para descargar cada vez que se inicie la consola de administración.

5 Solución de problemas y asistencia técnica

Este capítulo explica cómo resolver los problemas detectados durante la instalación de GFI EndPointSecurity. Las principales fuentes de información disponibles para solucionar estos problemas son:

Esta sección y el resto de la Guía del administrador de GFI EndPointSecurity contiene soluciones a todos los posibles problemas que puede detectar. Si no puede resolver un problema, comuníquese con el Servicio técnico de GFI para obtener más ayuda.

Problemas comunes

En la tabla que se incluye a continuación, se muestran los problemas más comunes que puede detectar durante la configuración inicial y el primer uso de GFI EndPointSecurity y una posible solución a cada uno de ellos:

Tabla 9: Solución de problemas: Problemas comunes

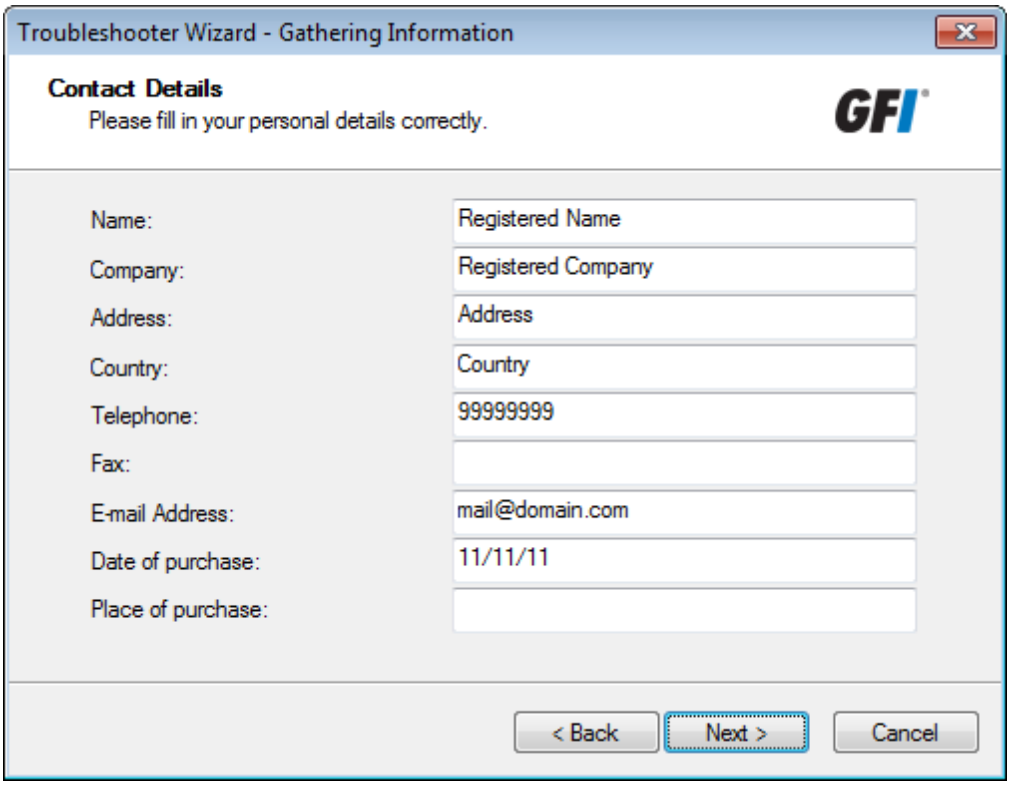
Problema	Causa posible	Solución posible
El equipo está desconectado.	La consola de administración de GFI EndPointSecurity hace ping en el equipo de destino en la implementación para determinar si está en línea y, de lo contrario, se muestra este mensaje.	Si un equipo de destino está desconectado, la implementación de la directiva de protección relevante se reprogramará para una hora más tarde. GFI EndPointSecurity sigue intentando implementar esa directiva cada hora, hasta que el equipo de destino se vuelve a conectar. Asegúrese de que el equipo de destino esté encendido y conectado a la red.
Error al conectarse con el registro remoto (error).	GFI EndPointSecurity no pudo extraer los datos del registro del equipo de destino.	Asegúrese de que la configuración del cortafuegos habilite la comunicación entre los equipos de destino y el servidor de GFI EndPointSecurity. Para obtener más información, consulte Requisitos del sistema.
Error al recopilar la información necesaria (error).	GFI EndPointSecurity no pudo extraer los datos relacionados con la versión del equipo de destino (versión del sistema operativo y versión del agente de GFI EndPointSecurity).	Para obtener más detalles acerca de la causa del error y una posible solución, consulte el mensaje de error del sistema dentro de los paréntesis.
Error al crear los archivos de instalación necesarios (error).	GFI EndPointSecurity no pudo agregar los archivos de configuración necesarios dentro del archivo de implementación (archivo de instalación .msi) del agente de GFI EndPointSecurity. Este error ocurre antes de que el archivo de implementación se copie en el equipo de destino.	Para obtener más detalles acerca de la causa del error y una posible solución, consulte el mensaje de error del sistema dentro de los paréntesis.
Error al copiar los archivos en el equipo remoto (error).	GFI EndPointSecurity no pudo copiar el archivo de implementación (archivo de instalación .msi) en el equipo remoto. Una posible causa puede ser que el recurso compartido administrativo (C$) que utiliza GFI EndPointSecurity para conectarse al equipo de destino esté deshabilitado.	Para obtener más detalles acerca de la causa del error y una posible solución, consulte el mensaje de error del sistema dentro de los paréntesis. Para obtener más información acerca de la conectividad de red y los permisos de seguridad, consulte: http://kb.gfi.com/articles/SkyNet_Article/KBID003754?retURL=%2Fapex%2FSupportHome&popup=true

Problema	Causa posible	Solución posible
Tiempo de espera	La implementación del agente en el equipo de destino está tardando demasiado en finalizar o está bloqueada.	Intente volver a implementar el agente de GFI EndPointSecurity.
Error en la instalación del servicio de implementación (error).	El servicio que está en ejecución en el equipo de destino no pudo instalar o desinstalar el agente de GFI EndPointSecurity.	Para obtener más detalles acerca de la causa del error y una posible solución, consulte el mensaje de error del sistema dentro de los paréntesis.
Error en la instalación.	Se completó la instalación del agente de GFI EndPointSecurity, pero no está marcado como instalado dentro del registro. Los números de versión y compilación del agente de GFI EndPointSecurity no son los mismos que los de la consola de administración de GFI EndPointSecurity.	Para obtener más detalles acerca de la causa del error y una posible solución, consulte los archivos de registro de instalación del agente en el equipo de destino en: **%windir%\EndPointSecurity**.
Error en la desinstalación.	Se completó la desinstalación del agente de GFI EndPointSecurity, pero no está marcado como desinstalado dentro del registro.	Para obtener más detalles acerca de la causa del error y una posible solución, consulte los archivos de registro de instalación del agente en el equipo de destino en: **%windir%\EndPointSecurity**.
Se produjo un error en la operación debido a una excepción desconocida.	GFI EndPointSecurity ha detectado un error inesperado.	Utilice el asistente para el solucionador de problemas para comunicarse con el equipo de asistencia técnica de GFI. Para abrir el asistente para el solucionador de problemas, vaya a **Inicio > Programas > GFI EndPointSecurity 2013 > GFI EndPointSecurity 2013 Troubleshooter**.

Uso de GFI EndPointSecurity Troubleshooter

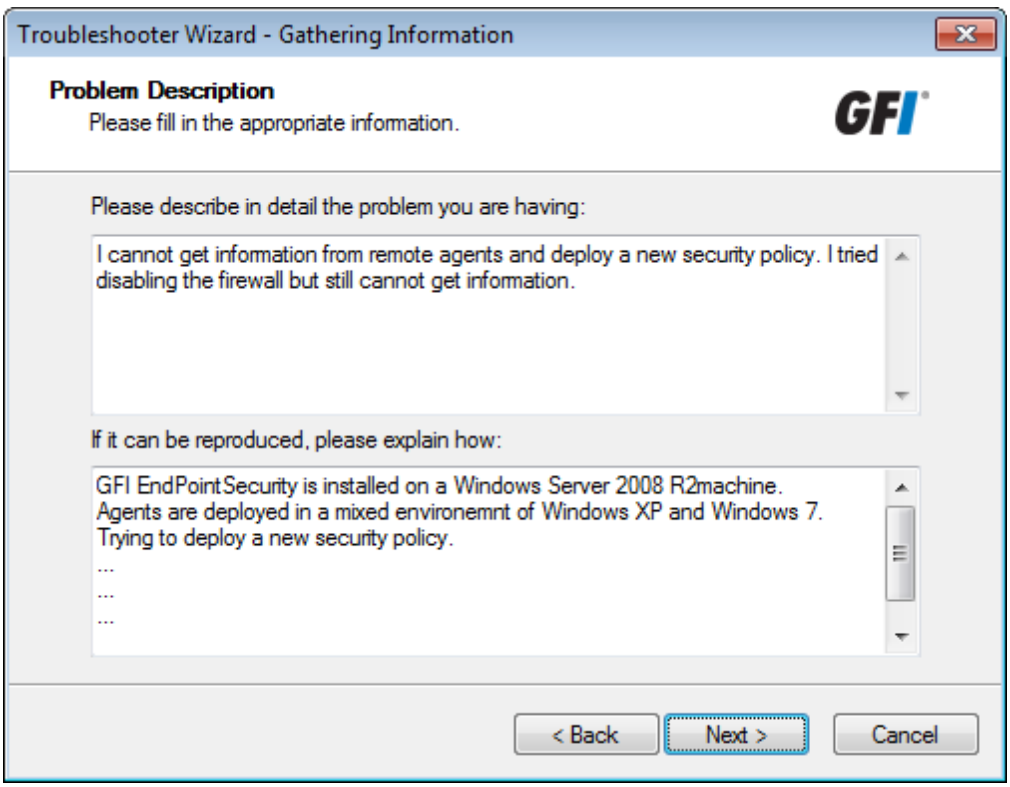
Para usar el solucionador de problemas proporcionado por GFI EndPointSecurity:

1. Haga clic en **Inicio > Programas > GFI EndPointSecurity2013 > GFI EndPointSecurity2013 Troubleshooter**.
2. Haga clic en **Next** en la pantalla de bienvenida del asistente.



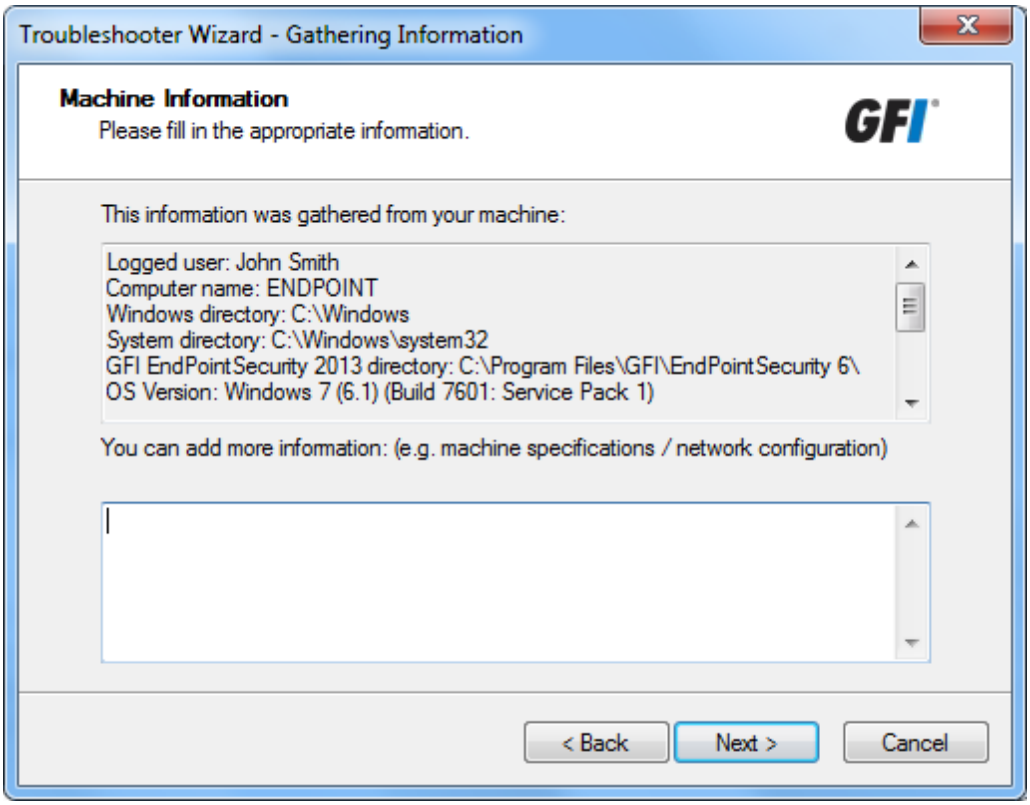
Captura de pantalla 9: Especificación de los detalles de contacto y de compra

3. Especifique sus datos de contacto para que nuestro equipo de soporte pueda comunicarse con usted para obtener más información de análisis. Haga clic en **Next**.



Captura de pantalla 10: Especificación de los detalles del problema y otra información relevante para recrear el problema

4. Especifique el error que se genera y otros datos que podrían ayudar a nuestro equipo de soporte a recrear este problema. Haga clic en **Next**.



Captura de pantalla 11: Recopilación de información del equipo

5. El solucionador de problemas analiza su sistema para obtener información acerca del hardware. Puede agregar manualmente más información en el espacio proporcionado o hacer clic en **Next**.

Captura de pantalla 12: Finalizar el asistente para el solucionador de problemas

6. En esta etapa, el solucionador de problemas crea un paquete con la información recopilada en los pasos anteriores. A continuación, se debe enviar el paquete a nuestro equipo de soporte para que

pueda analizar y resolver el problema. Haga clic en los botones que se describen a continuación para ver las opciones de envío:

- **Open Containing Folder**: Permite abrir la carpeta que contiene el paquete generado por el solucionador de problemas de modo que pueda enviarlo manualmente por correo electrónico.
- **Go to GFI Support**: Permite abrir la página de soporte del sitio web de GFI.

7. Haga clic en **Finish**.

GFI SkyNet

GFI mantiene un exhaustivo repositorio de su base de conocimientos, que incluye respuestas a los problemas más habituales. GFI SkyNet tiene siempre la lista más actualizada de preguntas y revisiones de soporte técnico. Si la información de esta guía no soluciona sus problemas, consulte GFI SkyNet; para ello, visite http://kb.gfi.com/.

Foro en la red

La asistencia técnica de usuario a usuario está disponible a través del foro de la red de GFI. Para acceder al foro web, visite: http://forums.gfi.com/.

Solicitar soporte técnico

Si ninguno de los recursos especificados anteriormente le permite solucionar los problemas, póngase en contacto con el equipo de Soporte técnico de GFI rellenando un formulario de solicitud de soporte técnico en línea, o bien de forma telefónica.

- **En línea**: Complete el formulario de solicitud de soporte técnico y siga las instrucciones detalladas que se indican en esta página para enviar su solicitud de soporte técnico en: http://support.gfi.com/supportrequestform.asp.
- **Teléfono**: Para obtener el número de teléfono de soporte técnico correspondiente a su región, visite: http://www.gfi.com/company/contact.htm.

> **NOTA**
>
> Antes de ponerse en contacto con el Centro de soporte técnico, tenga su identificación de cliente a mano. Su ID de cliente es el número de cuenta en línea que se le asigna cuando registra por primera vez sus claves de licencia en el área de clientes de GFI en: http://customers.gfi.com.

Le responderemos en 24 horas, o antes, en función de su huso horario.

Documentación

Si este manual no cumple sus expectativas o si cree que esta documentación se puede mejorar, indíquenoslo enviando un correo electrónico a: documentation@gfi.com.

6 Glosario

A

Acceso temporal

Un período durante el cual los usuarios pueden acceder a los dispositivos y puertos de conexión (cuando normalmente ese acceso está bloqueado) en equipos de destino protegidos durante una duración y un intervalo de tiempo determinados.

Active Directory

Tecnología que proporciona diversos servicios de red, entre los que se incluyen los servicios de directorio similares a LDAP.

Agente de GFI EndPointSecurity

Un servicio del cliente responsable de la implementación y la aplicación de las directivas de protección en los equipos de destino.

Alertas

Un conjunto de notificaciones (alertas por correo electrónico, mensajes de red o mensajes SMS) que se envían a destinatarios de alertas cuando se generan eventos específicos.

Aplicación GFI EndPointSecurity

Aplicación de seguridad del servidor que ayuda a mantener la integridad de datos mediante la prevención del acceso y la transferencia de contenido no autorizados hacia y desde dispositivos y puertos de conexión.

Archivo MSI

Un archivo generado por GFI EndPointSecurity para la implementación posterior con GPO u otras opciones de implementación. Se puede generar para cualquier directiva de protección y contiene todos los parámetros de seguridad relevantes configurados, incluida la configuración de instalación para equipos de destino no protegidos.

Asistente para inicio rápido

Un asistente que lo guía en la configuración de GFI EndPointSecurity con parámetros de configuración personalizados. Se inicia después de que se abre la consola de administración de GFI EndPointSecurity por primera vez y está previsto para el primer uso.

Asistente para la creación de directivas de protección

Un asistente que lo guía en la creación y configuración de directivas de protección nuevas. Los parámetros de configuración incluyen la selección de categorías de dispositivos y puertos para controlar y si desea bloquear o permitir el acceso a ellos. Este asistente también le permite configurar filtros por tipo de archivo, permisos de cifrado y opciones de alerta y registro.

B

Back-end de base de datos

Una base de datos que utiliza GFI EndPointSecurity para realizar un seguimiento de las auditorías de todos los eventos generados por agentes de GFI EndPointSecurity implementados en los equipos de destino.

BitLocker To Go

En Microsoft Windows 7, una función para proteger y cifrar los datos en dispositivos extraíbles.

C

Categoría del dispositivo

Un grupo de periféricos organizados en una categoría.

Cifrado de seguridad

Un conjunto de restricciones configuradas para bloquear o permitir que usuarios o grupos accedan a tipos de archivo específicos almacenados en dispositivos cifrados con BitLocker To Go. Estas restricciones se aplican cuando los dispositivos cifrados se conectan a los equipos de destino abarcados por la directiva de protección.

Consola de administración de GFI EndPointSecurity

La interfaz de usuario de la aplicación del servidor de GFI EndPointSecurity.

Cuenta de administrador de alertas

Una cuenta de destinatario de alerta que GFI EndPointSecurity crea automáticamente después de la instalación.

D

Destinatario de alerta

Una cuenta de perfil de GFI EndPointSecurity para contener los detalles de contacto de los usuarios que desea que reciban alertas por correo electrónico, mensajes de red y mensajes SMS.

Detección automática

Una función de GFI EndPointSecurity para buscar y detectar equipos que se conectaron recientemente a la red en períodos programados configurados.

Directiva de protección

Un conjunto de permisos de puertos de conectividad y acceso a dispositivos que se puede configurar para que se ajuste a las directivas de seguridad de acceso de su compañía.

Dispositivos de interfaz humana (HID)

Una especificación que es parte del estándar de bus serie universal (USB) para una clase de dispositivos periféricos. Estos dispositivos, como mouse, teclado y joystick, les permiten a los usuarios introducir datos o interactuar directamente con el equipo.

E

Equipo de destino

Un equipo protegido con una directiva de protección de GFI EndPointSecurity.

Examen de dispositivos

Una función de GFI EndPointSecurity para buscar todos los dispositivos que están o han estado conectados a los equipos de destino examinados.

F

Filtros por tipo de archivo

Un conjunto de restricciones que se asignan a los usuarios y grupos por tipo de archivo. El filtrado se basa en comprobaciones de extensión de archivo y comprobaciones de firma de tipo de archivo real.

G

GPO

Véase Objetos de directiva de grupo

H

Herramienta GFI EndPointSecurity Temporary Access

Una herramienta que está disponible en los equipos de destino. El usuario la usa para generar un código de solicitud y después para introducir el código de desbloqueo para activar el acceso temporal una vez que el administrador lo concede. Después de la activación, el usuario tendrá acceso a dispositivos y puertos de conexión (cuando normalmente ese acceso está bloqueado) en su equipo de destino protegido por la duración y el intervalo de tiempo especificados.

I

Informe de resumen

Un informe de resumen que ofrece un reporte de la estadística de actividad detectada por GFI EndPointSecurity.

L

Lista blanca de dispositivos

Una lista de dispositivos específicos cuyo uso está permitido cuando se accede a ellos desde todos los equipos de destino abarcados por la directiva de protección.

Lista negra de dispositivos

Una lista de dispositivos específicos cuyo uso está bloqueado cuando se accede a ellos desde todos los equipos de destino abarcados por la directiva de protección.

M

Mensaje de usuario

Un mensaje que muestran los agentes de GFI EndPointSecurity en los equipos de destino cuando se accede a los dispositivos.

Mensajes de error de implementación

Errores que pueden surgir después de la implementación de agentes de GFI EndPointSecurity desde la consola de administración de GFI EndPointSecurity.

O

Objetos de directiva de grupo

Gestión centralizada de Active Directory y sistema de configuración que controla lo que los usuarios pueden y no pueden hacer en una red informática.

P

Permisos de acceso

Un conjunto de permisos (acceso, lectura y escritura) que se asignan a los usuarios y grupos por categoría de dispositivo, puerto de conectividad o dispositivo específico.

Permisos globales

Un paso del asistente para la creación de directivas de protección que le pide al usuario que bloquee o permita el acceso a todos los dispositivos incluidos en una categoría o que están conectados a un puerto de los equipos de destino abarcados por la directiva de protección.

Puerto de conectividad

Una interfaz entre los equipos y los dispositivos.

R

Registro de eventos

Una función para registrar eventos relacionados con los intentos realizados para acceder a dispositivos y a puertos de conexión en los equipos de destino y operaciones de servicio.

U

Usuario avanzado

Un usuario avanzado obtiene automáticamente acceso total a los dispositivos conectados a cualquier equipo de destino abarcado por la directiva de protección.

7 Índice

EE.UU., CANADÁ, AMÉRICA CENTRAL Y AMÉRICA DEL SUR

15300 Weston Parkway, Suite 104, Cary, NC 27513, EE.UU.

Teléfono: +1 (888) 243-4329

Fax: +1 (919) 379-3402

ussales@gfi.com

REINO UNIDO Y REPÚBLICA DE IRLANDA

Magna House, 18-32 London Road, Staines-upon-Thames, Middlesex, TW18 4BP, REINO UNIDO

Teléfono: +44 (0) 870 770 5370

Fax: +44 (0) 870 770 5377

sales@gfi.com

EUROPA, ORIENTE MEDIO Y ÁFRICA

GFI House, San Andrea Street, San Gwann, SGN 1612, Malta

Teléfono: +356 2205 2000

Fax: +356 2138 2419

sales@gfi.com

AUSTRALIA Y NUEVA ZELANDA

83 King William Road, Unley 5061, Australia Meridional

Teléfono: +61 8 8273 3000

Fax: +61 8 8273 3099

sales@gfiap.com