Manual do produto GFI

GFI EndPointSecurity™

Guia de introdução

As informações e o conteúdo deste documento são apenas informativos e fornecidos "no estado em que se encontram" sem nenhuma garantia de qualquer tipo, expressa ou implícita, incluindo, sem limitação, as garantias de comercialização, adequação a uma finalidade específica e não violação. A GFI Software não se responsabiliza por danos de qualquer natureza, incluindo danos indiretos, resultantes do uso deste documento. As informações foram obtidas de fontes disponíveis ao público. Apesar do razoável esforço para garantir a precisão dos dados fornecidos, a GFI não alega, promete ou garante que as informações sejam íntegras, precisas, recentes ou adequadas, e não se responsabiliza por falhas na impressão, informações desatualizadas ou outros erros. A GFI não oferece garantia expressa ou implícita e não assume obrigação ou responsabilidade legal pela precisão ou integridade das informações contidas neste documento.

Se você acredita que este documento contenha erros efetivos, entre em contato conosco. Analisaremos a questão assim que possível.

Versão do documento: 1.1.1

Última atualização (dia/mês/ano): 3/20/2014

Índice

1 Introdução **1**

1.1 Sobre o GFI EndPointSecurity 1
1.2 Componentes do GFI EndPointSecurity 5
1.2.1 Console de gerenciamento do GFI EndPointSecurity 5
1.2.2 Agente do GFI EndPointSecurity 5
1.3 Guia do administrador 5
1.4 Convenções usadas neste manual 5
1.5 Portas de conectividade suportadas 6
1.6 Categorias de dispositivos suportados 6

2 Instalação do GFI EndPointSecurity **8**

2.1 Requisitos de sistema 8
2.2 Atualizar o GFI EndPointSecurity 9
2.3 Instalar uma nova instância do GFI EndPointSecurity 10
2.4 Configurações de pós-instalação 11
2.5 Navegar no console de gerenciamento 20

3 Testar a sua instalação **22**

3.1 Pré-condições de teste 22
3.2 Caso de teste 23
3.3 Voltar às configurações padrão 26

4 Diversos **27**

4.1 Licenciamento de produtos 27
4.2 Informações sobre a versão do produto 27

5 Solução de problemas e suporte **28**

6 Glossário **33**

7 Índice **37**

Lista de figuras

Screenshot 1: Instalação do GFI EndPointSecurity: configuração da conta de administrador de domínio 10
Screenshot 2: Instalação do GFI EndPointSecurity: detalhes da chave de licença 11
Screenshot 3: Navegar na interface de usuário do GFI EndPointSecurity 21
Screenshot 4: Selecionar entidades de controle 24
Screenshot 5: Selecionar categorias de dispositivo para atribuir permissões 24
Screenshot 6: Adicionar usuários ou grupos 25
Screenshot 7: Selecionar tipos de permissões por usuário ou grupo 25
Screenshot 8: Editar chave de licença 27
Screenshot 9: Especificar detalhes de contacto e compra 29
Screenshot 10: Especificar detalhes do problema e outras informações relevantes para recriar o problema .30
Screenshot 11: Coleta de informações da máquina 30
Screenshot 12: Finalizar o assistente de solução de problemas 31

Lista de tabelas

Table 1: Política de proteção de implantação e monitoramento 2
Table 2: Política de proteção de implantação e monitoramento 4
Table 3: Política de proteção de implantação e monitoramento 4
Table 4: Termos e convenções usados neste manual 5
Table 5: Requisitos do sistema – Hardware 8
Table 6: Configurações da descoberta automática 13
Table 7: Configurações da descoberta automática 15
Table 8: Opções de back-end do banco de dados 19
Table 9: Solução de problemas comuns 28

1 Introdução

A proliferação de dispositivos do consumidor, como iPods, dispositivos USB e smartphones, tem aumentado o risco de vazamentos de dados deliberados e não intencionais e outra atividade maliciosa. É muito simples para um funcionário copiar grandes quantidades de dados sensíveis para um iPod ou USB stick ou introduzir software malicioso e ilegal em sua rede por meio destes dispositivos. O GFI EndPointSecurity ajuda-o rápida e facilmente a combater estas ameaças críticas sem necessitar de bloquear todas as portas.

Tópicos neste capítulo

1.1 Sobre o GFI EndPointSecurity 1

1.2 Componentes do GFI EndPointSecurity 5

1.3 Guia do administrador 5

1.4 Convenções usadas neste manual 5

1.5 Portas de conectividade suportadas 6

1.6 Categorias de dispositivos suportados 6

1.1 Sobre o GFI EndPointSecurity

O GFI EndPointSecurity habilita administradores a gerenciar ativamente o acesso de usuário e registrar a atividade de:

- mídia portáteis, incluindo iPods, Creative Zen e outros
- unidades USB, CompactFlash, cartões de memória, CD, disquetes e outros dispositivos de armazenagem portáteis
- iPhone, BlackBerry e handhelds Android, celulares, smartphones e dispositivos de comunicação similares
- placas de rede, laptops e outras conexões de rede.

Como funciona o GFI EndPointSecurity – implantação e monitoramento

As operações de implantação e monitoramento da política de proteção do GFI EndPointSecurity podem ser divididas em quatro estágios lógicos descritos abaixo:

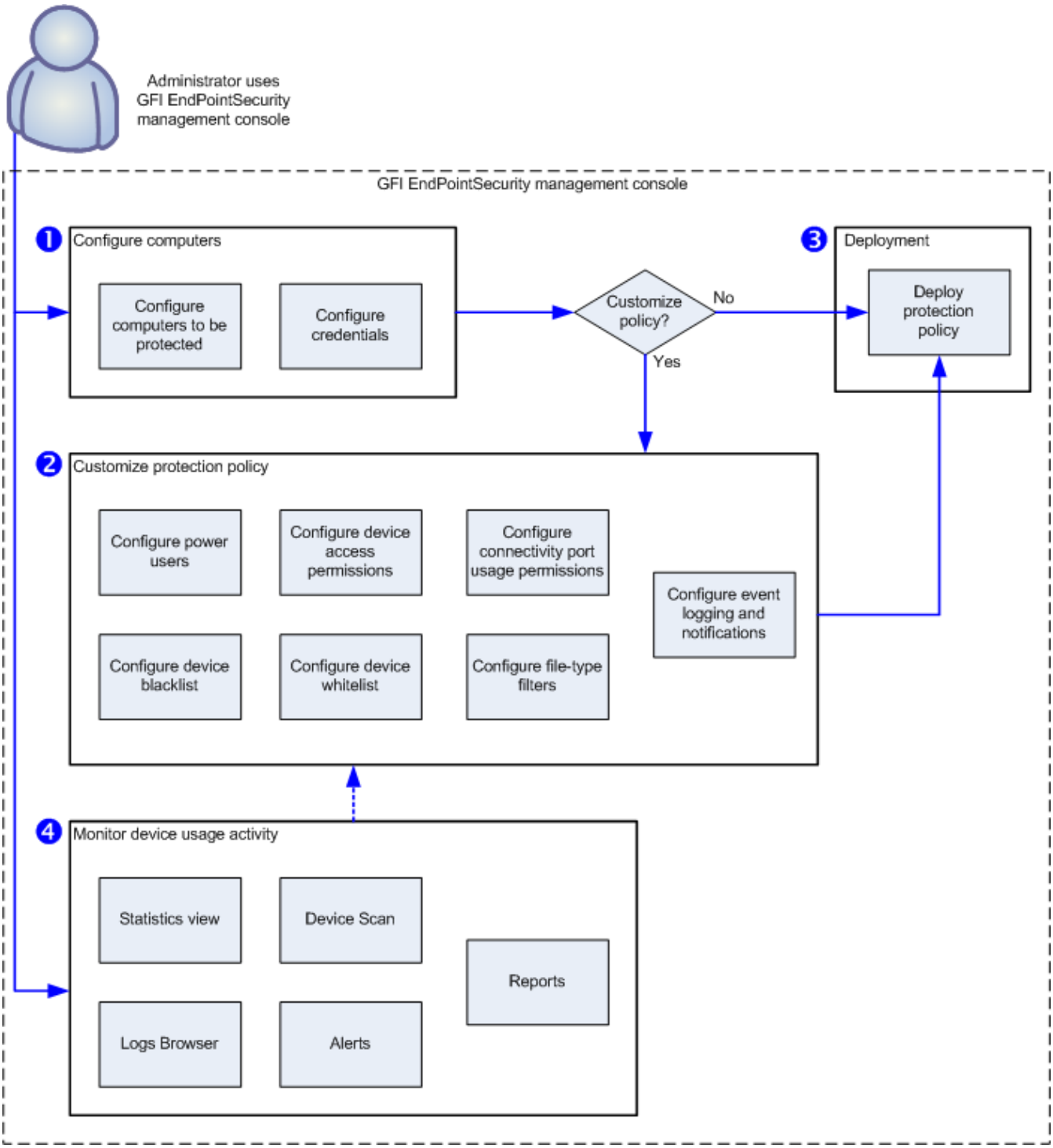


Figure 1: Política de proteção - implantação e monitoramento

A tabela abaixo descreve os estágios representados acima:

Table 1: Política de proteção de implantação e monitoramento

Estágio	Descrição
Estágio 1 - Configurar computadores	O administrador especifica qual a política de proteção atribuída a que computadores e as credenciais de logon a serem usados pelo GFI EndPointSecurity para acessar os computadores de destino e implantar os agentes.
Estágio 2 - Personalizar política de proteção	O administrador pode personalizar uma política de proteção antes ou depois de sua implantação. As opções de personalização incluem a criação de usuários avançados, adição de dispositivos inseridos na lista de exclusão/lista de permissão e permissões de acesso a dispositivos.

Estágio	Descrição
Estágio 3 - Implantar política de proteção	O administrador implanta a política de proteção. Após a primeira implantação de uma política de proteção, é instalado automaticamente um agente do GFI EndPointSecurity no computador de destino de rede remota. Após as seguintes implantações da mesma política de proteção, o agente será atualizado e não será novamente instalado.
Estágio 4 - Monitorar acesso a dispositivos	Quando tiverem sido implantados agentes, o administrador pode monitorar todas as tentativas de acesso a dispositivos pelo console de gerenciamento, receber alertas e gerar relatórios por meio do GFI EndPointSecurityGFI ReportPack.

Como funciona o GFI EndPointSecurity - acesso a dispositivos

As operações de acesso a dispositivos do GFI EndPointSecurity podem ser divididas em três estágios lógicos:

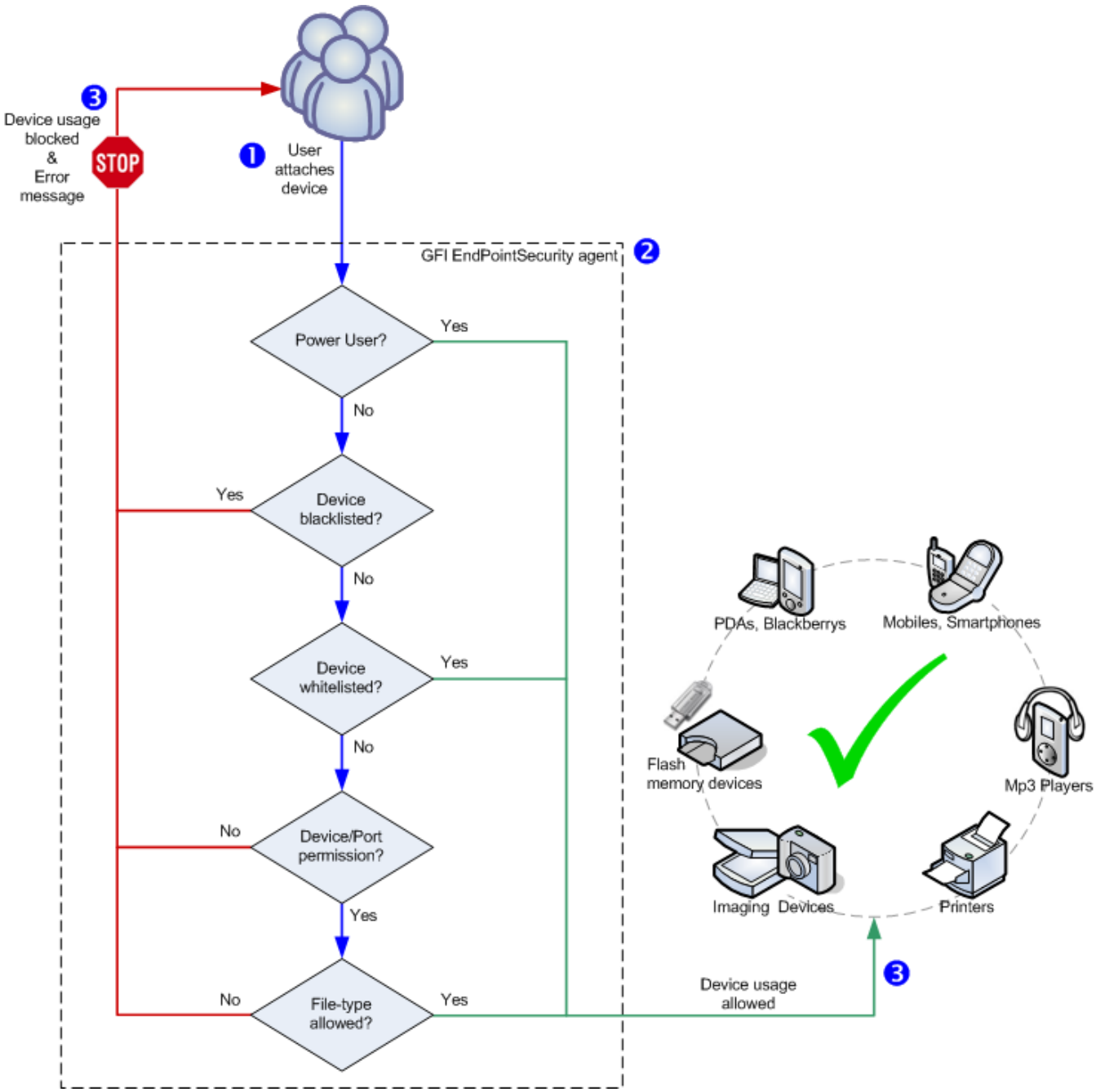


Figure 2: Acesso a dispositivos

A tabela abaixo descreve os estágios representados acima:

Table 2: Política de proteção de implantação e monitoramento

Estágio	Descrição
Estágio 1 - Dispositivo conectado a um computador	O usuário conecta um dispositivo a um computador de destino protegido pelo GFI EndPointSecurity.
Estágio 2 - Reforço da política de proteção	O agente do GFI EndPointSecurity instalado no computador de destino detecta o dispositivo conectado e segue as regras da política de proteção aplicáveis ao computador/usuário. Esta operação determina se o dispositivo tem o acesso permitido ou bloqueado.
Estágio 3 - Uso do dispositivo permitido/bloqueado	O usuário recebe uma mensagem de erro indicando que o uso do dispositivo foi bloqueado ou que tem permissão para acessar o mesmo.

Como funciona o GFI EndPointSecurity - acesso temporário

As operações de acesso temporário do GFI EndPointSecurity podem ser divididas em três estágios lógicos:

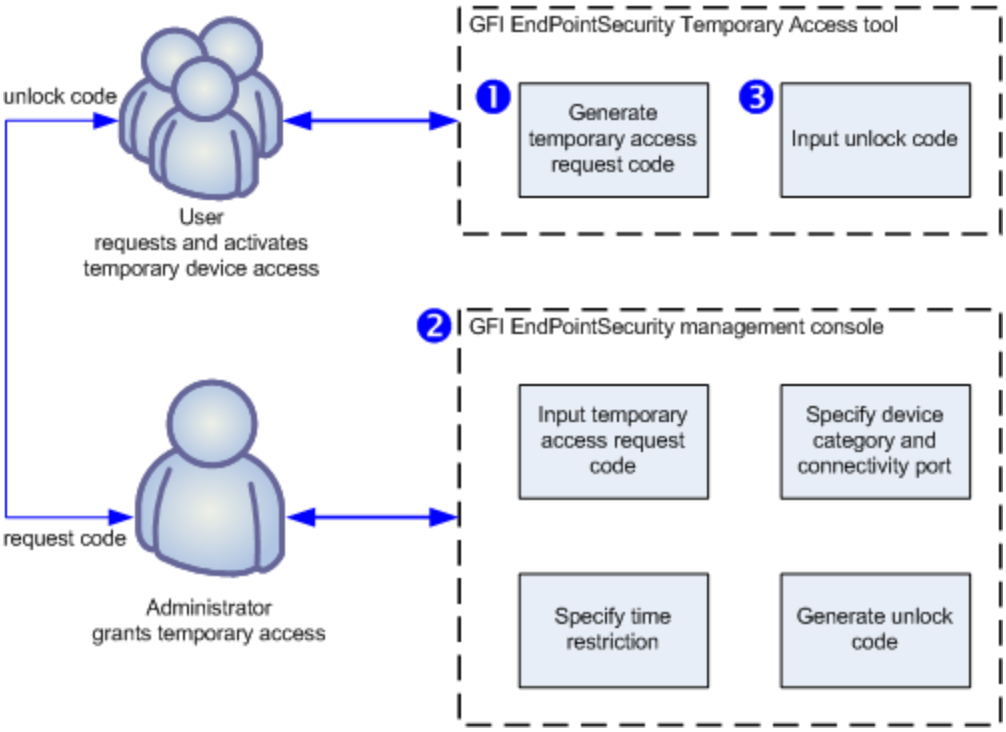


Figure 3: Solicitar/conceder acesso temporário

A tabela abaixo descreve os estágios representados acima:

Table 3: Política de proteção de implantação e monitoramento

Estágio	Descrição
Estágio 1 - Usuário solicita acesso temporário a dispositivos	O usuário executa a ferramenta Temporary Access do GFI EndPointSecurity do computador em que o dispositivo deverá ser acessado. A ferramenta é usada para gerar um código de solicitação que o usuário comunica ao administrador. O usuário também necessita de informar o administrador sobre os tipos de dispositivos ou portas de conexão que necessitam ser acessados e por quanto tempo será necessário o acesso aos dispositivos/portas.
Estágio 2 - Administrador concede acesso temporário	O administrador usa o recurso Temporary Access no console de gerenciamento do GFI EndPointSecurity para introduzir o código de solicitação, especificar os dispositivos/as portas e as restrições de tempo. É gerado um código de desbloqueio que o administrador depois comunica ao usuário.

Estágio	Descrição
Estágio 3 - Usuário ativa acesso temporário a dispositivos	Assim que o usuário receber o código de desbloqueio enviado pelo administrador, este código é inserido na ferramenta Temporary Access do GFI EndPointSecurity para ativar o acesso temporário e para poder usar os dispositivos/as portas necessários.

1.2 Componentes do GFI EndPointSecurity

Quando instalar o GFI EndPointSecurity, são implantados os seguintes componentes:

- Console de gerenciamento do GFI EndPointSecurity
- Agente do GFI EndPointSecurity

1.2.1 Console de gerenciamento do GFI EndPointSecurity

Por meio do console de gerenciamento do GFI EndPointSecurity é possível:

- Criar e gerenciar políticas de proteção e especificar as categorias de dispositivo e portas de conectividade que devem ser controladas
- Implantar remotamente políticas de proteção e agentes em seus computadores de destino Conceder acesso temporário a computadores de destino para o uso de dispositivos específicos
- Exibir o status de proteção do dispositivo de cada computador que esteja sendo monitorado
- Realizar verificações em computadores de destino para identificar dispositivos atual ou previamente conectados
- Verificar logs e analisar que dispositivos foram conectados a cada computador de rede
- Controlar os computadores que têm um agente implantado e os agentes que necessitam de atualização.

1.2.2 Agente do GFI EndPointSecurity

O agente do GFI EndPointSecurity é um serviço do lado do cliente responsável pela implantação das políticas de proteção em computador(es) de destino. Este serviço é instalado automaticamente no computador de destino de rede remota, depois de ser implantada, pela primeira vez, a política de proteção relevante por meio do console de gerenciamento do GFI EndPointSecurity. Após as seguintes implantações da mesma política de proteção, o agente será atualizado e não será novamente instalado.

1.3 Guia do administrador

Administração detalhada e diretrizes de configuração são fornecidas no GFI EndPointSecurity – Guia do administrador, que é instalado com o produto ou é baixado em separado a partir de: http://www.gfi.com/esec/esecmanual.pdf.

O Guia do administradorcomplementa este Guia de início rápido e fornece mais informações sobre como usar e personalizar ferramentas e recursos do GFI EndPointSecurity.

1.4 Convenções usadas neste manual

Table 4: Termos e convenções usados neste manual

Termo	Descrição
	Informações adicionais e referências essenciais para a operação do GFI EndPointSecurity.

Termo	Descrição
	Notificações e precauções importantes quanto aos problemas que costumam ser encontrados.
>	Instruções de navegação passo a passo para acessar uma função específica.
Texto em negrito	Itens para selecionar, como nós, opções do menu ou botões de comando.
Texto em itálico	Parâmetros e valores que devem ser substituídos pelo valor aplicável, como caminhos e nomes de arquivos personalizados.
`Código`	Indica valores de texto que deve ser inseridos, como comandos e endereços.

1.5 Portas de conectividade suportadas

O GFI EndPointSecurity verifica dispositivos que estão ou estiveram conectados nas seguintes portas:

USB

Secure Digital (SD)

Firewire

Bluetooth

Infravermelho

PCMCIA

Serial e paralela

Interna (exemplo: unidades óticas conectadas internamente no PCI).

1.6 Categorias de dispositivos suportados

No GFI EndPointSecurity, os dispositivos são organizados nas seguintes categorias:

Disquetes

CD/DVD

Impressoras

PDA, incluindo:

- PC de bolso
- Smartphones

Adaptadores de rede, incluindo:

- Adaptadores de Ethernet
- Adaptadores de Wi-Fi
- Adaptadores removíveis (USB, Firewire, PCMCIA)

Modems, incluindo:

- Smartphones
- Telefones celulares

Dispositivos de geração de imagens:

- Câmeras digitais
- Webcams

- Scanners

Dispositivos de interface humana:

- Teclados
- Mouses
- Controladores de jogo

Dispositivos de armazenamento, incluindo:

- Pen drives USB
- Leitores de mídia digital (por exemplo: leitores de MP3/MP4)
- Leitores de cartões de memória e flash
- Dispositivos USB de várias unidades (por ex., dispositivos que não se montam como uma única unidade)

Outros dispositivos:

- Dongles/portas Bluetooth
- Dongles/portas por infravermelho
- Unidades Zip
- Unidades de fita
- Unidades MO (magneto-óticas) (internas e externas).

2 Instalação do GFI EndPointSecurity

Este capítulo disponibiliza informações sobre como preparar o seu ambiente de rede para uma implantação bem-sucedida do GFI EndPointSecurity.
Tópicos neste capítulo

2.1 Requisitos de sistema 8

2.2 Atualizar o GFI EndPointSecurity 9

2.3 Instalar uma nova instância do GFI EndPointSecurity 10

2.4 Configurações de pós-instalação 11

2.5 Navegar no console de gerenciamento 20

2.1 Requisitos de sistema

Requisitos de hardware

A tabela abaixo lista as exigências de hardware para GFI EndPointSecurity e agente do GFI EndPointSecurity:

Table 5: Requisitos do sistema - Hardware

	GFI EndPointSecurity	GFI EndPointSecurityAgente do
Processor	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
Espaço livre	Mínimo: 100 MB Recomendado: 100 MB	Mínimo: 50 MB Recomendado: 50 MB

Sistemas operacionais compatíveis (x64/x86)

GFI EndPointSecurity e agente GFI EndPointSecurity podem ser instalados em uma máquina executando um dos seguintes sistemas operacionais:

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

Requisitos de hardware do agente

- Processador: Velocidade de clock do processador de 1GHz ou maior
- RAM: 256 MB (mínimo); 512 MB (recomendado)
- Disco rígido: 50 MB de espaço disponível

Requisitos de software do agente

- Processador: Velocidade de clock do processador de 1GHz ou maior
- RAM: 256 MB (mínimo); 512 MB (recomendado)
- Disco rígido: 50 MB de espaço disponível

Other software components

O GFI EndPointSecurity necessita dos seguintes componentes de software para uma implantação completamente funcional:

- Microsoft Internet Explorer 5.5 ou superior
- Microsoft .NET Framework 2.0 ou superior
- Microsoft SQL Server 2000, 2005 ou 2008 como banco de dados de back-end

Obs.

Um back-end do banco de dados é necessário para armazenar dados de acesso ao dispositivo e para fins de comunicação. O GFI EndPointSecurity fornece a opção de usar um Microsoft SQL Server disponível ou baixar automaticamente e instalar Microsoft SQL Server 2005 Express no mesmo computador onde o console de gerenciamento do GFI EndPointSecurity está instalado.

Portas de firewall

TCP port 1116 (padrão) – requerida pelos agentes do GFI EndPointSecurity para notificar o GFI EndPointSecurity de seus status e enviar eventos de acesso ao dispositivo. Sem esta porta aberta, o administrador tem de monitorar manualmente os eventos de cada computador de destino ou automaticamente por GFI EventsManager. Para obter mais informações, consulte http://www.gfi.com/eventsmanager.

2.2 Atualizar o GFI EndPointSecurity

Atualizar do GFI EndPointSecurity 3 ou posterior

Se tiver o GFI LanGuard Portable Storage Control ou uma versão anterior do GFI EndPointSecurity, é possível realizar a atualização para a versão mais recente do GFI EndPointSecurity. A atualização do GFI EndPointSecurity 3 ou posterior para o GFI EndPointSecurity 2013 é simples. O processo de atualização faz parte do processo de instalação do GFI EndPointSecurity 2013 e inclui:

- Desinstalar o GFI EndPointSecurity 3 ou posterior
- Importar ajustes de configuração do GFI EndPointSecurity 3.

Ao instalar o GFI EndPointSecurity é solicitada a confirmação da importação de configurações a partir da versão anterior. Clique em **Yes** para importar as configurações. É solicitada a especificação das seguintes configurações a importar:

- Políticas de proteção:
  - Computer
  - Configurações de segurança
- Opções:
  - Opções de registro em log
  - Opções de banco de dados.

Atualizar do GFI LanGuard Portable Storage Control

Se o computador no qual você está instalando o GFI EndPointSecurity estiver protegido por um agente GFI LanGuard Portable Storage Control, primeiro necessita de desinstalar esse agente. Para fazer isso:

1. Abra o console de configuração do GFI LanGuard Portable Storage Control.

2. Exclua o agente do computador onde será instalado o GFI EndPointSecurity.

> **Obs.**
>
> Este processo deve ser realizado somente para o computador onde será instalado o GFI EndPointSecurity.

3. Feche o aplicativo do console de configuração do GFI LanGuard Portable Storage Control e continue instalando o GFI EndPointSecurity.

4. Ao instalar o GFI EndPointSecurity é solicitada a confirmação da importação de configurações a partir da versão anterior. Clique em **Yes** para importar as configurações.

> **Obs.**
>
> Os agentes do GFI LanGuard Portable Storage Control que estavam protegendo seus computadores serão automaticamente adicionados a uma política de proteção designada **LegacyAgents** no GFI EndPointSecurity.

2.3 Instalar uma nova instância do GFI EndPointSecurity

Para instalar o GFI EndPointSecurity:

1. Faça logon da máquina na qual GFI EndPointSecurity será instalado, usando os privilégios administrativos.

2. Clique duas vezes no arquivo executável do GFI EndPointSecurity.

2. Selecione o idioma que você deseja instalar e clique em **Next**.

3. Clique em **Next** na tela inicial de boas-vindas.

4. Leia atentamente o contrato de licença de usuário final. Se você concordar, selecione **I accept the license agreement** e clique em **Next**.

Screenshot 1: Instalação do GFI EndPointSecurity: configuração da conta de administrador de domínio

5. Digite as credenciais de uma conta com privilégios administrativos e clique em **Next** para continuar.

Screenshot 2: Instalação do GFI EndPointSecurity: detalhes da chave de licença

6. Digite o **Full Name** e **Company**. Se tiver uma chave de licença, atualize os detalhes **License Key** e clique em **Next**.

> **Obs.**
>
> A chave de licença pode ser digitada após instalação ou vencimento do período de avaliação do GFI EndPointSecurity. Para obter mais informações, consulte Licenciamento de produtos (página 27).

7. Digite ou procure selecionar um caminho de instalação alternativo ou clique em **Next** para usar o caminho predefinido e prossiga a instalação.

8. Clique em **Back** para introduzir novamente a informação da instalação e clique em **Next** e aguarde que seja concluída.

9. Ao completar a instalação, habilitar ou desabilitar a abertura da caixa de seleção GFI EndPointSecurity e clique em **Finish** para finalizar instalação.

2.4 Configurações de pós-instalação

Iniciando o console de gerenciamento do GFI EndPointSecurity, é iniciado automaticamente o assistente de início rápido. Isto permite ajustar configurações importantes do GFI EndPointSecurity no primeiro uso.

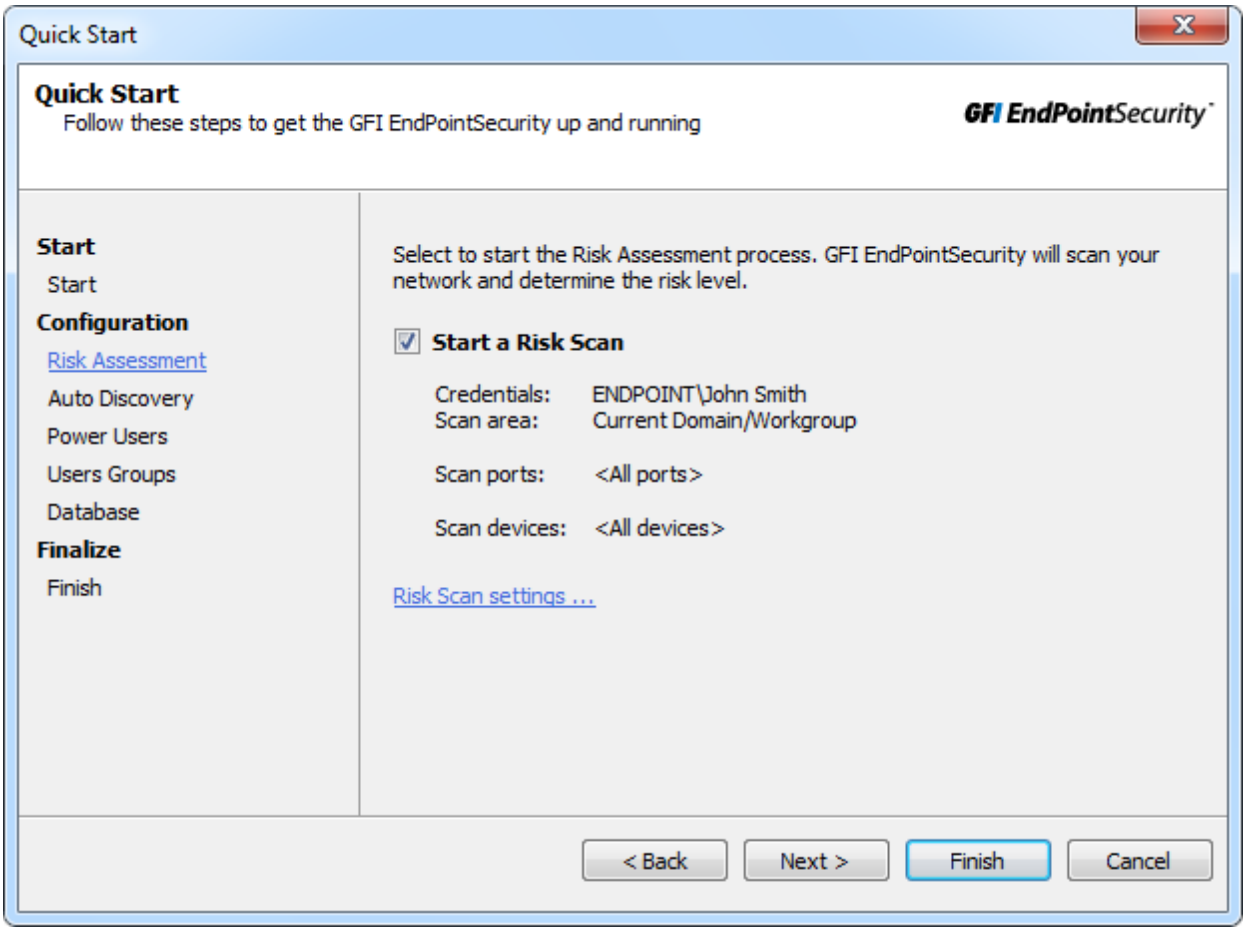
O assistente de início rápido é constituído pelas seguintes etapas e serve de guia na configuração:

- Avaliação do risco
- Descoberta automática
- Usuários avançados
- Grupos de usuários
- Back-end do banco de dados.

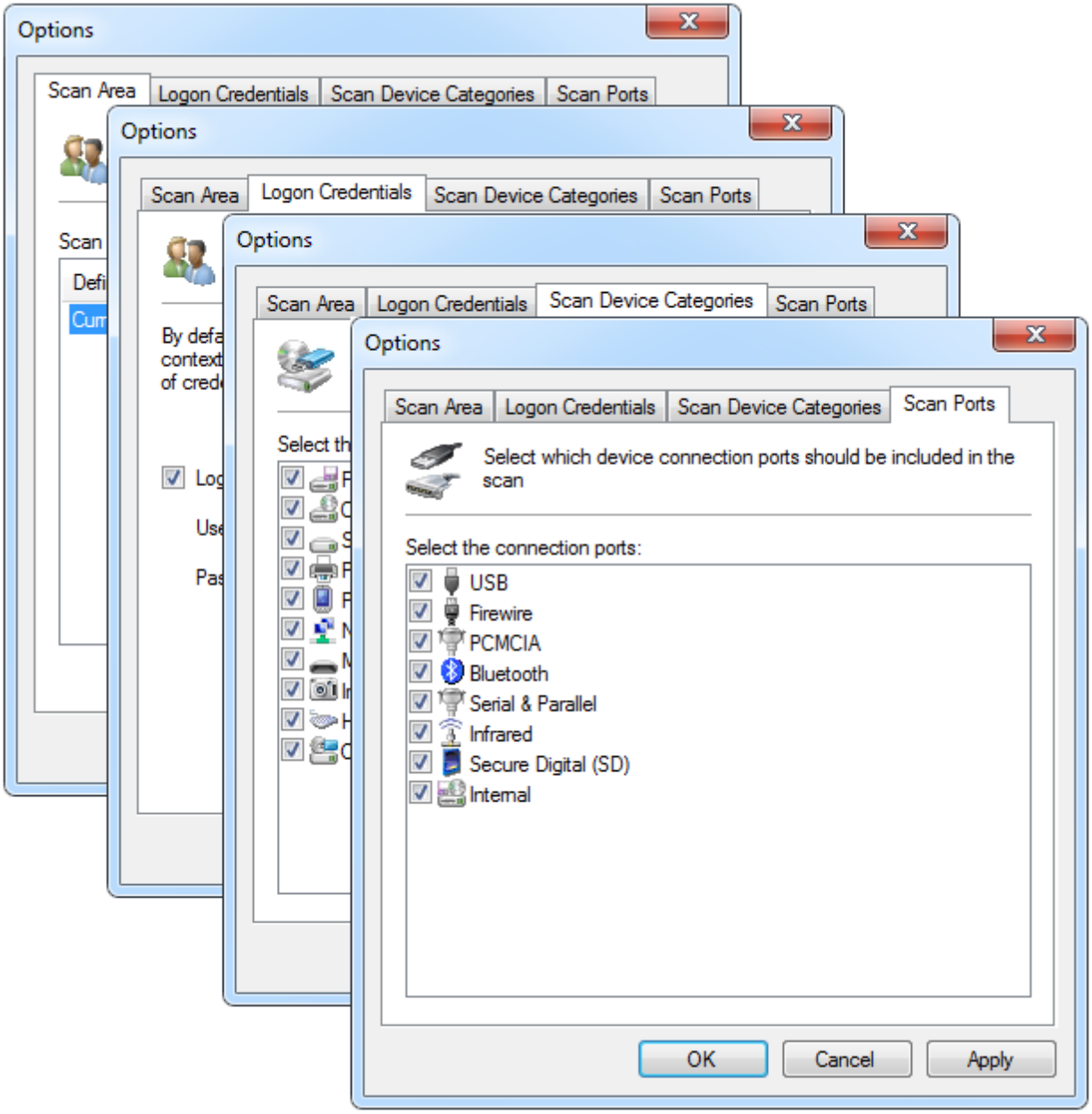
> **Obs.**
>
> O assistente de início rápido pode ser reiniciado a partir de **File > Quick Start Wizard**.

Para usar o assistente de início rápido:

1. Clique em **Next** na tela inicial do assistente.



2. A partir de **Risk Assessment**, marque/desmarque **Start a Risk Scan** para habilitar/desabilitar a função para iniciar uma verificação em sua rede para determinar o nível de risco.



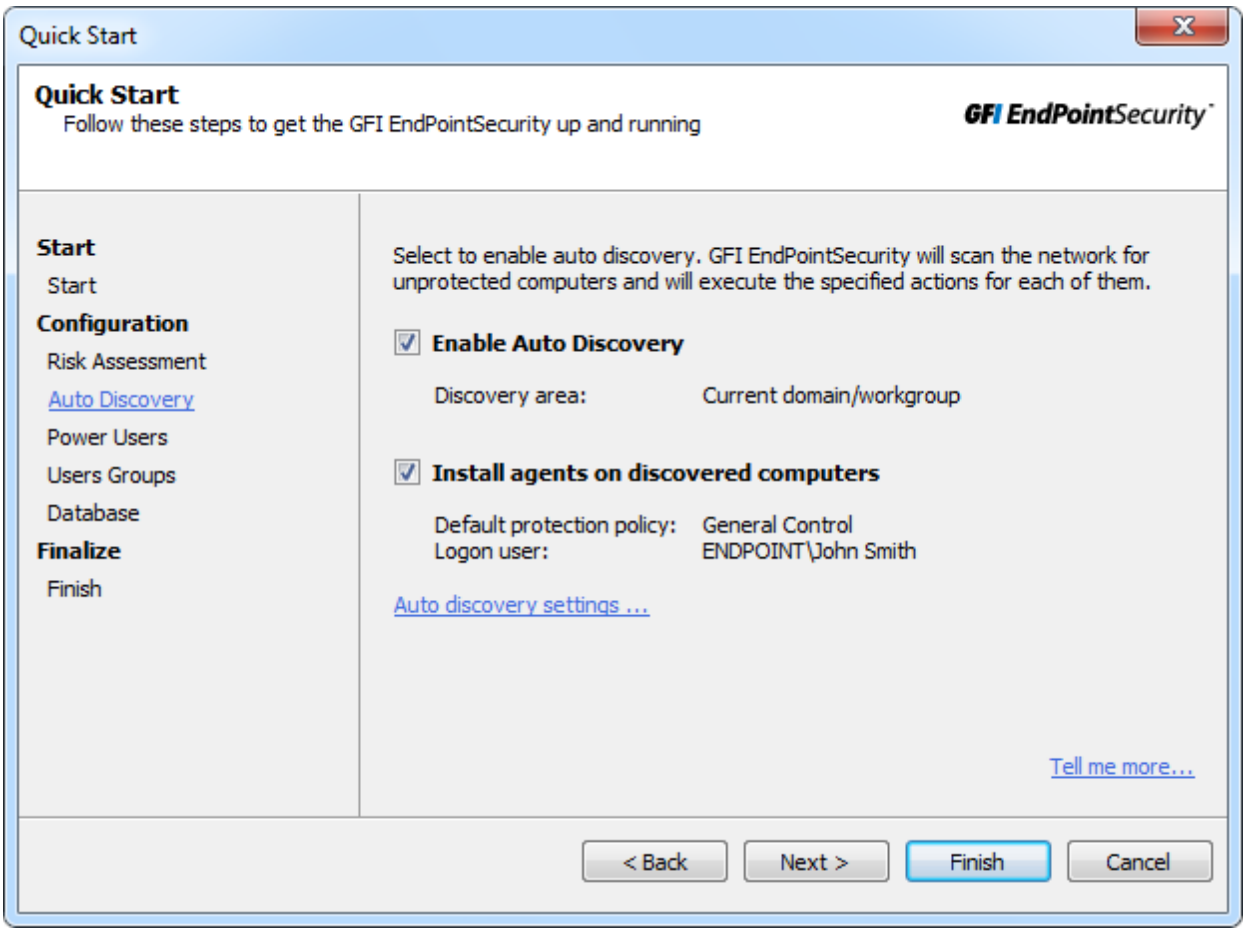
3. (Opcional) Clique em **Risk scan settings...** e ajuste as configurações das guias descritas abaixo:

Table 6: Configurações da descoberta automática

Guia	Descrição
Scan Area	Selecione a área de destino na qual o GFI EndPointSecurity verifica os computadores na rede. » **Current domain/workgroup** - O GFI EndPointSecurity busca novos computadores no mesmo domínio/grupo de trabalho onde está instalado. » **The following domains/workgroups** - Selecione esta opção e clique em **Add**. Especifique os domínios onde o GFI EndPointSecurity busca novos computadores e clique em **OK**. » **Entire network except** - Selecione esta opção e clique em **Add**. Especifique o domínio/grupo de trabalho que deve ser excluído durante a descoberta automática e clique em **OK**. » **IP range** - Selecione esta opção e clique em **Add**. Especifique o intervalo de endereços IP que deve ser incluído ou excluído durante a descoberta automática e clique em **OK**. » **Computer list** - Selecione esta opção e clique em **Add**. Especifique o domínio/grupo de trabalho que deve ser incluído ou excluído durante a descoberta automática e clique em **OK**.

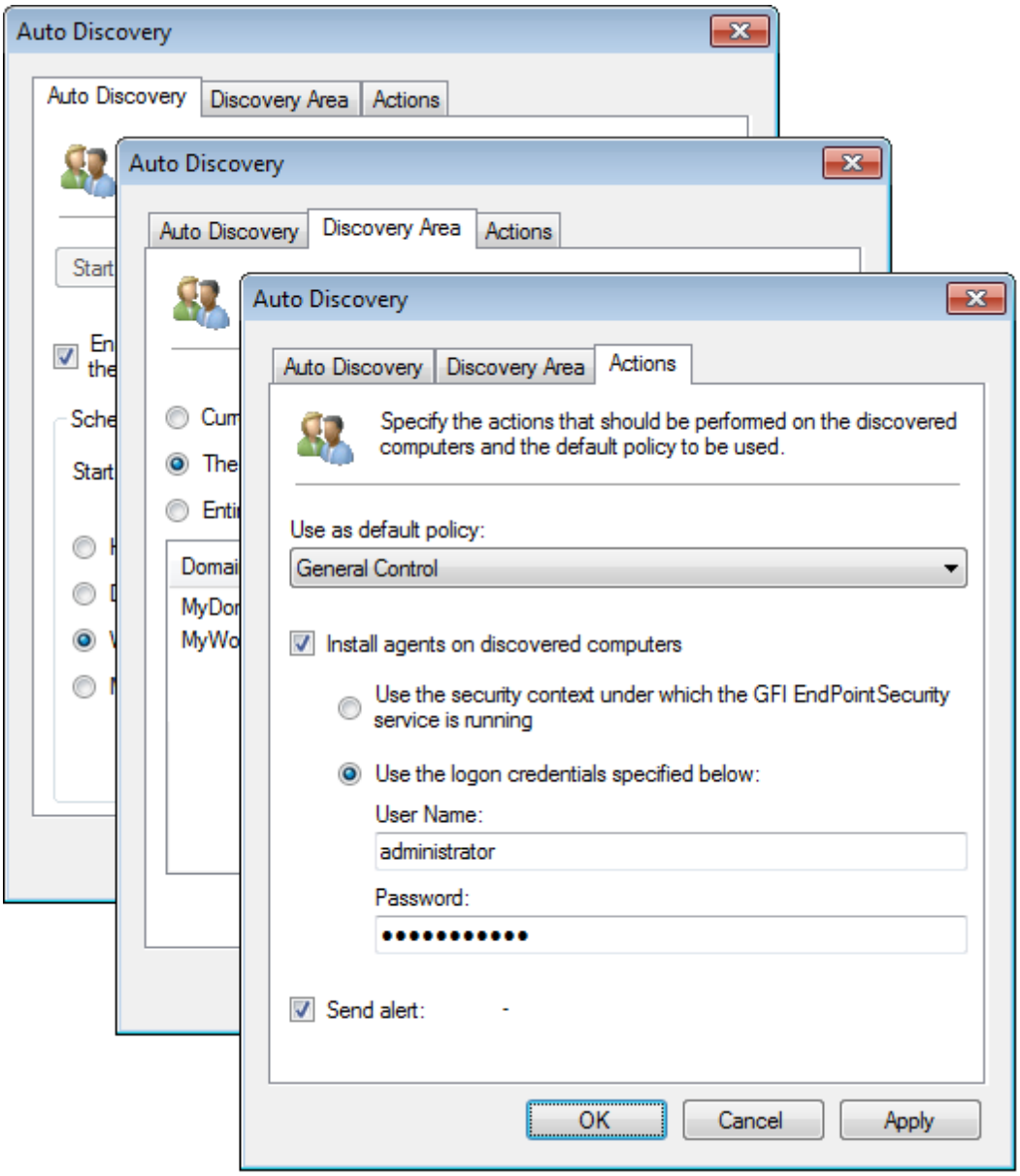
Guia	Descrição
Logon Credentials	Habilite/desabilite **Logon using credentials below** e especifique um conjunto de credenciais que o GFI EndPointSecurity usará para acessar computadores que serão verificados.
Scan Device Categories	Selecione as categorias do dispositivo que o GFI EndPointSecurity incluirá na verificação.
Scan ports	Selecione as portas de conexão do dispositivo que o GFI EndPointSecurity incluirá na verificação.

4. Clique em **Apply** e **OK** para fechar a caixa de diálogo Risk Assessment e clique em **Next** no assistente de início rápido.



5. A partir de **Auto Discovery**, marque/desmarque **Enable Auto Discovery** para habilitar/desabilitar a descoberta automática. Quando a descoberta automática estiver ativa, o GFI EndPointSecurity verifica periodicamente a sua rede relativamente a novos computadores.

6. Marque/desmarque **Install agents on discovered computers** para habilitar/desabilitar a implantação automática dos agentes do GFI EndPointSecurity em computadores recentemente descobertos.

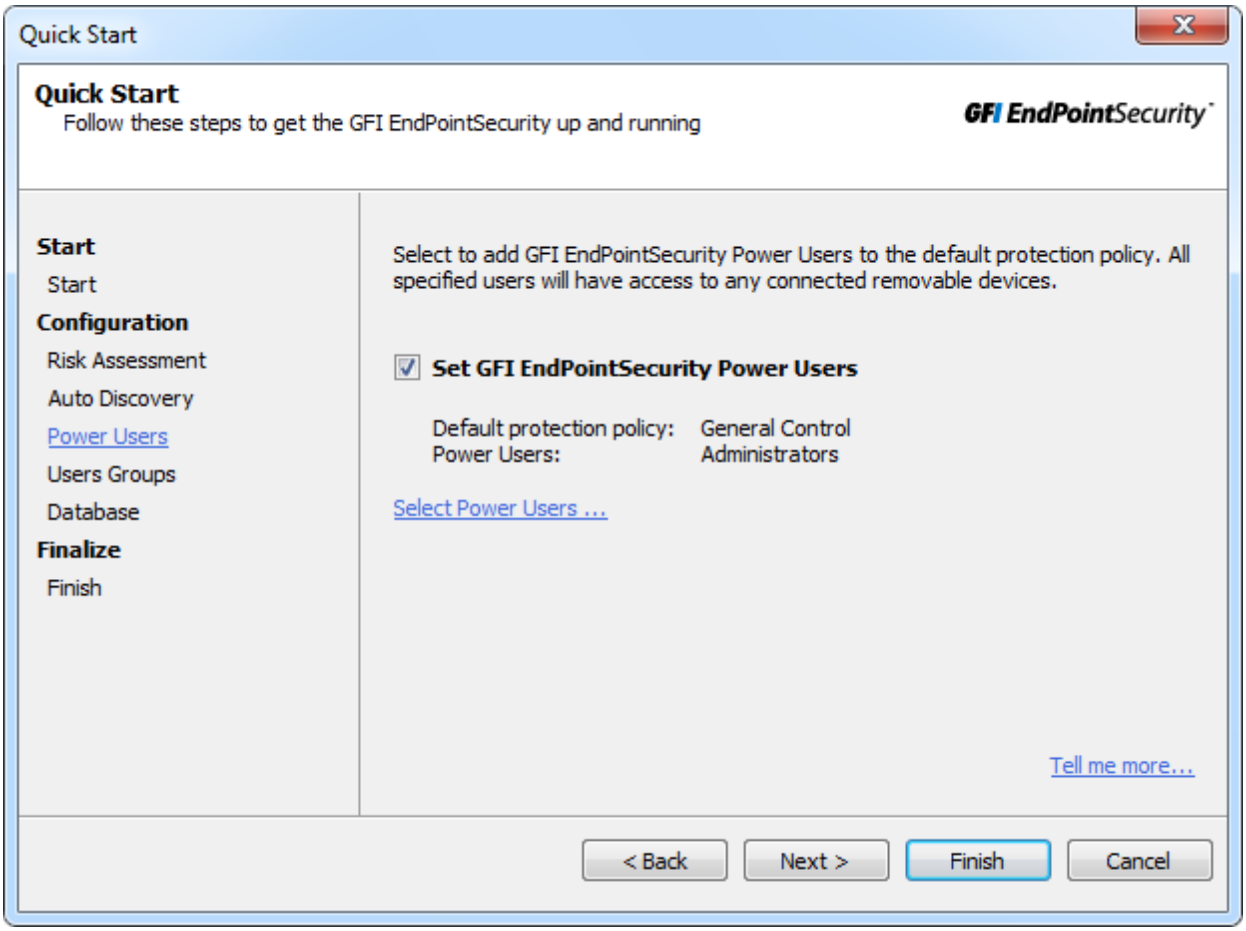


7. (Opcional) Clique em **Auto discovery settings...** e ajuste as configurações nas guias descritas abaixo:

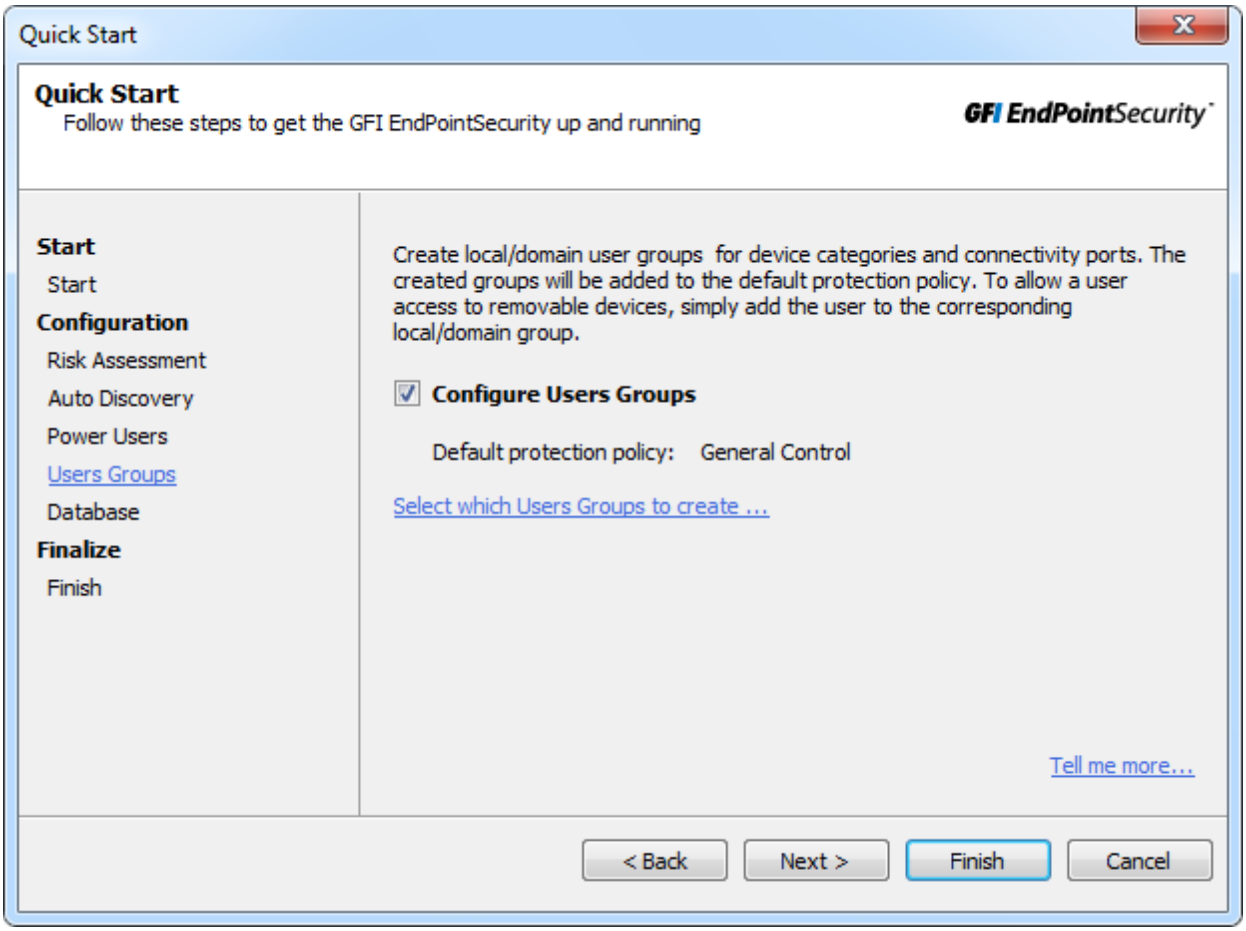
Table 7: Configurações da descoberta automática

Guia	Descrição
Auto Discovery	Habilite/desabilite a descoberta automática e configure um agendamento quando o GFI EndPointSecurity verificar a sua rede quanto a novos computadores.
Discovery Area	Selecione o local onde o GFI EndPointSecurity busca novos computadores. Selecione a partir do seguinte: » **Current domain/workgroup** - O GFI EndPointSecurity busca novos computadores no mesmo domínio/grupo de trabalho onde está instalado. » **The following domains/workgroups** - Selecione esta opção e clique em **Add**. Especifique os domínios onde o GFI EndPointSecurity busca novos computadores e clique em **OK**. » **Entire network except** - Selecione esta opção e clique em **Add**. Especifique o domínio/grupo de trabalho que deve ser excluído durante a descoberta automática e clique em **OK**.
Actions	Configure as ações executadas pelo GFI EndPointSecurity quando é descoberto um novo computador. Selecione também a política à qual se aplicam estas configurações.

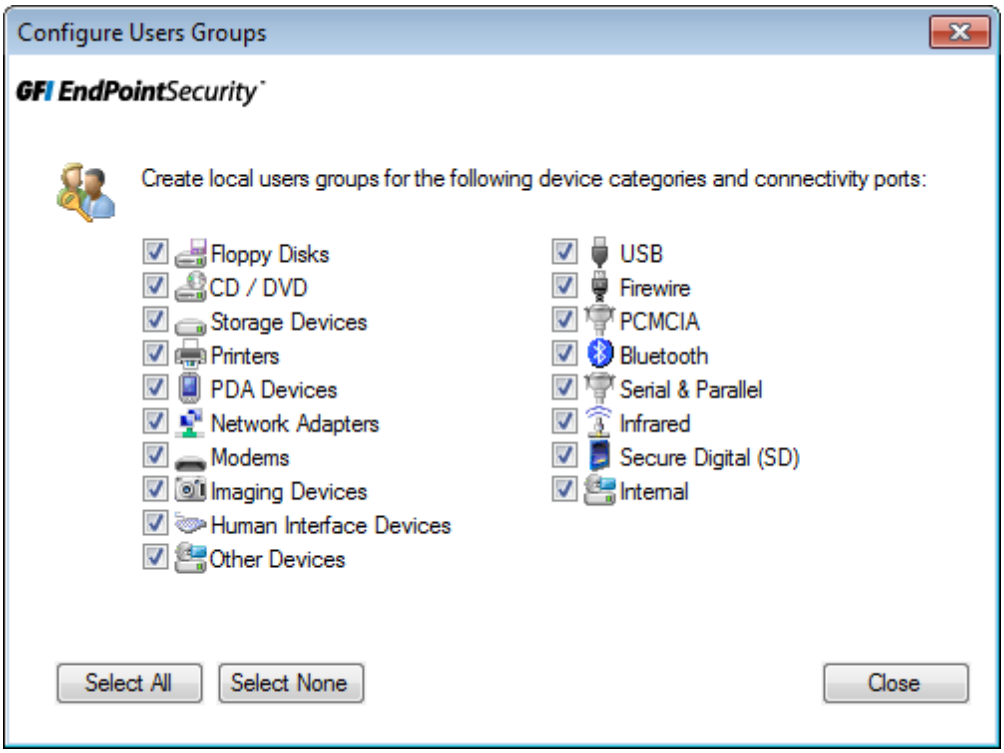
8. Clique em **Apply** e **OK** para fechar a caixa de diálogo Auto Discovery e clique em **Next** no Assistente de início rápido.



9. Em **Power Users**, marque/desmarque **Set GFI EndPointSecurity Power Users** para habilitar/desabilitar recursos dos usuários avançados. Os membros do grupo de usuários avançados têm acesso a qualquer dispositivo conectado afetado por esta política.
10. Clique em **Select Power Users...** e, a partir da caixa de diálogo Power Users, clique em **Add...** para adicionar usuários do seu domínio/grupo de trabalho.
11. Clique em **Apply** e **OK** para fechar a caixa de diálogo Power Users e clique em **Next** no assistente de início rápido.

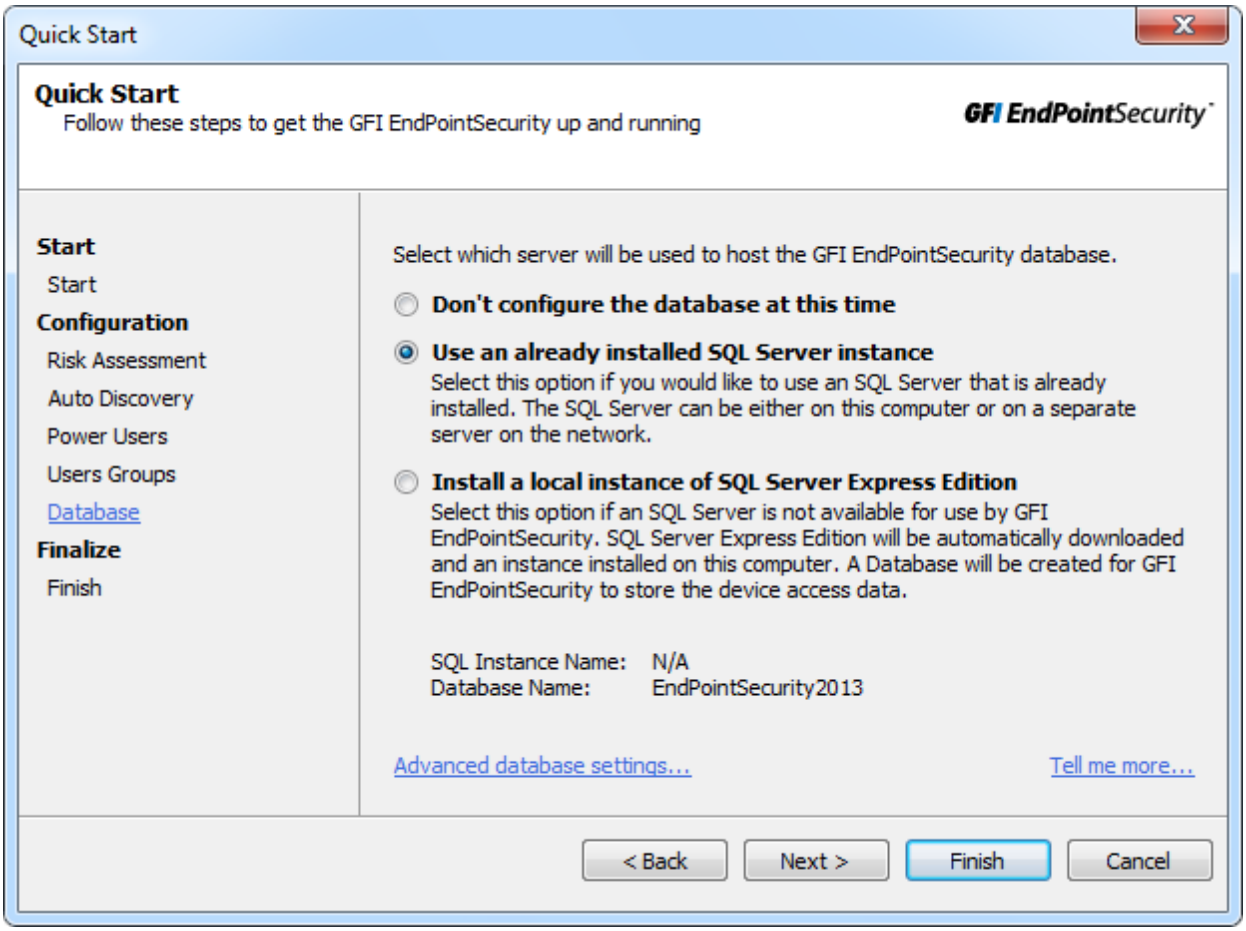


12. Em **Users Groups**, marque/desmarque **Configure Users Groups** para criar usuários do domínio/grupo de trabalho e associe-os a categorias de dispositivos e configurações de portas de conectividade selecionadas na etapa seguinte.



13. Clique em **Select which Users Groups to create...**. Na caixa de diálogo Configure Users Groups, marque os dispositivos e/ou as portas de conexão para os quais são criados usuários. Para gerenciar cada dispositivo e porta suportados desta política, clique em **Select All**.

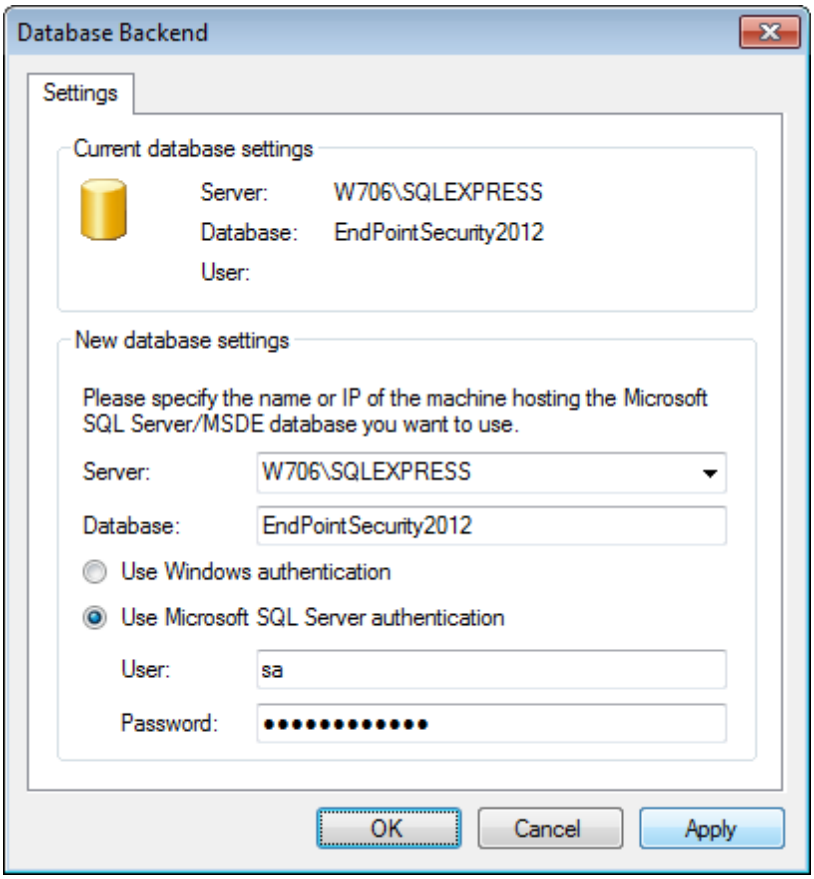
14. Clique em **Close** para fechar **Configure Users Groups** e clique em **Next** no assistente de início rápido.



15. Em Database, selecione o tipo de banco de dados que pretende usar como back-end do banco de dados. Selecione a partir das opções descritas abaixo:

Table 8: Opções de back-end do banco de dados

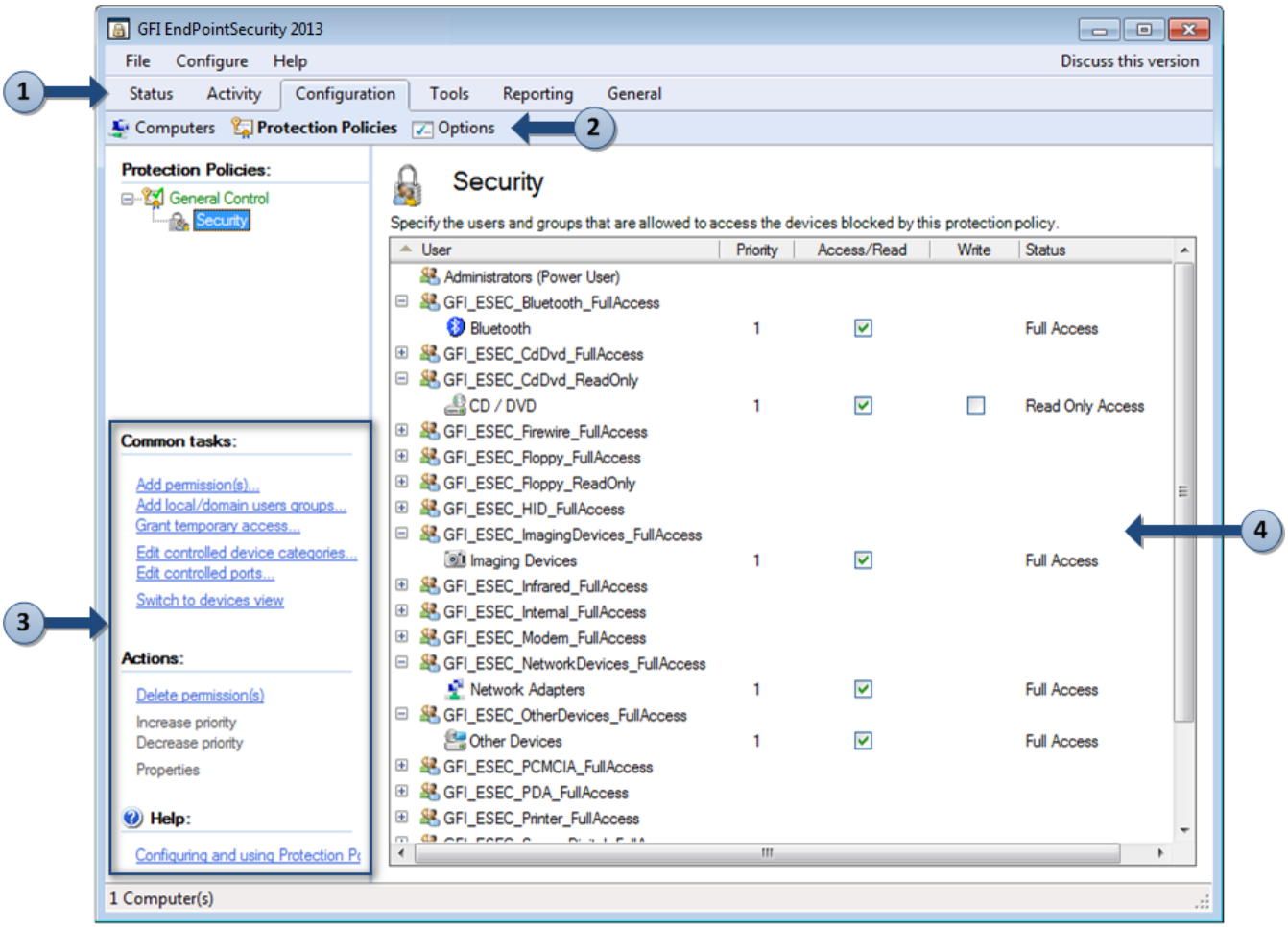
Opção	Descrição
Don't configure the database at this time	Conclua o assistente de início rápido e configure o back-end do banco de dados mais tarde. Para obter mais informações, consulte a ACM.
Use an already installed SQL Server instance	Use uma instância do Microsoft SQL Server instalado na mesma máquina onde você está instalando o GFI EndPointSecurity ou em qualquer outra máquina na rede.
Install a local instance of SQL Express Edition	Selecione esta opção para baixar e instalar uma instância do Microsoft SQL Server Express na mesma máquina onde você estiver instalando o GFI EndPointSecurity. É necessária uma conexão com a Internet.



16. (Opcional) Clique em **Advanced database settings...** para especificar o endereço do SQL Server, nome do banco de dados, método de logon e as respectivas credenciais. Clique em **Apply** e **OK** para fechar a caixa de diálogo Database Backend.
17. Clique em **Next** e aguarde que as configurações sejam aplicadas. Clique em **Finish** para fechar o assistente de início rápido.

2.5 Navegar no console de gerenciamento

O console de gerenciamento do GFI EndPointSecurity permite, com todas as funcionalidades administrativas, monitorar e gerenciar uso do acesso do dispositivo.



Screenshot 3: Navegar na interface de usuário do GFI EndPointSecurity

O console de gerenciamento do GFI EndPointSecurity é constituído pelas seções abaixo:

Seção	Descrição
1	**Guias** Navegue entre as diferentes guias do console de gerenciamento do GFI EndPointSecurity. As guias disponíveis são: » **Status** - Monitora o status do GFI EndPointSecurity e informação estatística no acesso do dispositivo. » **Activity** - Monitora dispositivos usados na rede. » **Configuration** - Acessa e configura as políticas de proteção padrão. » **Scanning** - Verifica computadores de destino e descobre os dispositivos conectados. » **Reporting** - Baixa ou abre GFI EndPointSecurity GFI ReportPack para gerar seus relatórios. » **General** - Verifica atualizações do GFI EndPointSecurity assim como detalhes da versão e do licenciamento.
2	**Sub-tabs** Acessar mais definições e/ou informações sobre a guia selecionada da seção 1.
3	**Left Pane** Acessa opções de configuração fornecidas em GFI EndPointSecurity. As opções de configuração são agrupadas em três seções, incluindo **Common Tasks**, **Actions** e **Help**. Disponível somente para algumas guias.
4	**Right Pane** Defina as opções de configuração selecionadas do painel esquerdo. Disponível somente para algumas guias.

3 Testar a sua instalação

Assim que o GFI EndPointSecurity estiver instalado e o assistente de início rápido estiver concluído, teste sua instalação para assegurar que o GFI EndPointSecurity está funcionando corretamente. Siga as instruções presentes nesta seção para verificar que tanto a instalação como as operações da política de proteção padrão de envio do GFI EndPointSecurity se encontram corretas.

Tópicos neste capítulo

3.1 Pré-condições de teste 22

3.2 Caso de teste 23

3.3 Voltar às configurações padrão 26

3.1 Pré-condições de teste

As configurações e pré-condições de teste seguintes são necessárias SOMENTE para este teste:

Configuração do dispositivo

Para o teste seguinte você necessita de:

- Unidade de CD/DVD conectada ao computador local
- CD/DVD com conteúdos acessíveis (preferencialmente um disco com conteúdos que estavam acessíveis antes da instalação do GFI EndPointSecurity).

> **Obs.**
>
> Podem ser usados outros dispositivos e outra mídia, tais como disquetes ou pen drives.

Contas do usuário

Para este teste garanta a disponibilidade de duas contas de usuário no mesmo computador em que o GFI EndPointSecurity está instalado:

- Uma sem privilégios administrativos
- Uma com privilégios administrativos.

Ajustes de configuração

A configuração do assistente de início rápido permite ajustar o GFI EndPointSecurity para se adequar às necessidades da sua empresa que podem não corresponder às configurações de pré-teste exigidas por este teste. Como resultado, alguns ajustes de configuração do GFI EndPointSecurity necessitam ser definidos conforme indicado abaixo para que este teste tenha êxito:

- Certifique-se de que o computador local se encontre listado na vista **Status > Agents**. Se o computador local não se encontrar listado, inclua-o manualmente na lista de computadores. Para obter mais informações, consulte o Manual de administração e configuração do GFI EndPointSecurity.
- Certifique-se de que a política de proteção padrão de envio é implantada no computador local e que se encontra atualizada. Para confirmar, verifique na vista **Status > Agents** o seguinte:
  - a política de proteção está definida para General Control

- a implantação está atualizada
- o computador local está Online.

> **Obs.**
>
> Se a implantação do agente no computador local não estiver atualizada, implante manualmente o agente no mesmo. Para obter mais informações, consulte o Manual de administração e configuração do GFI.

» Certifique-se de que a conta do usuário sem privilégios administrativos não se encontra definida como usuário avançado na política geral para proteção de controle (política de proteção padrão de envio).

> **Obs.**
>
> Se a conta de usuário estiver definida como usuário avançado, remova-a manualmente do grupo de usuários avançados da política geral para proteção de controle (política de proteção padrão de envio). Para obter mais informações, consulte o Manual de administração e configuração do GFI EndPointSecurity.

3.2 Caso de teste

Acessar um CD/DVD

Em conformidade com as pré-condições de teste delineadas anteriormente, os usuários não administrativos já não têm acesso permitido a quaisquer dispositivos ou portas conectadas ao computador local.

Para verificar se os dispositivos e a mídia estão inacessíveis para o usuário não administrativo:

1. Efetue logon no computador local como usuário sem privilégios administrativos.

2. Insira o CD/DVD na unidade de CD/DVD.

3. A partir do **Windows Explorer**, localize a unidade de CD/DVD e confirme que não consegue visualizar e abrir os conteúdos salvos no CD/DVD.

Atribuir permissões ao usuário sem privilégios administrativos

Para atribuir permissões de acesso ao dispositivo de CD/DVD ao usuário sem privilégios administrativos:

1. Efetue logon no computador local como usuário com privilégios administrativos.

2. Abra o GFI EndPointSecurity.

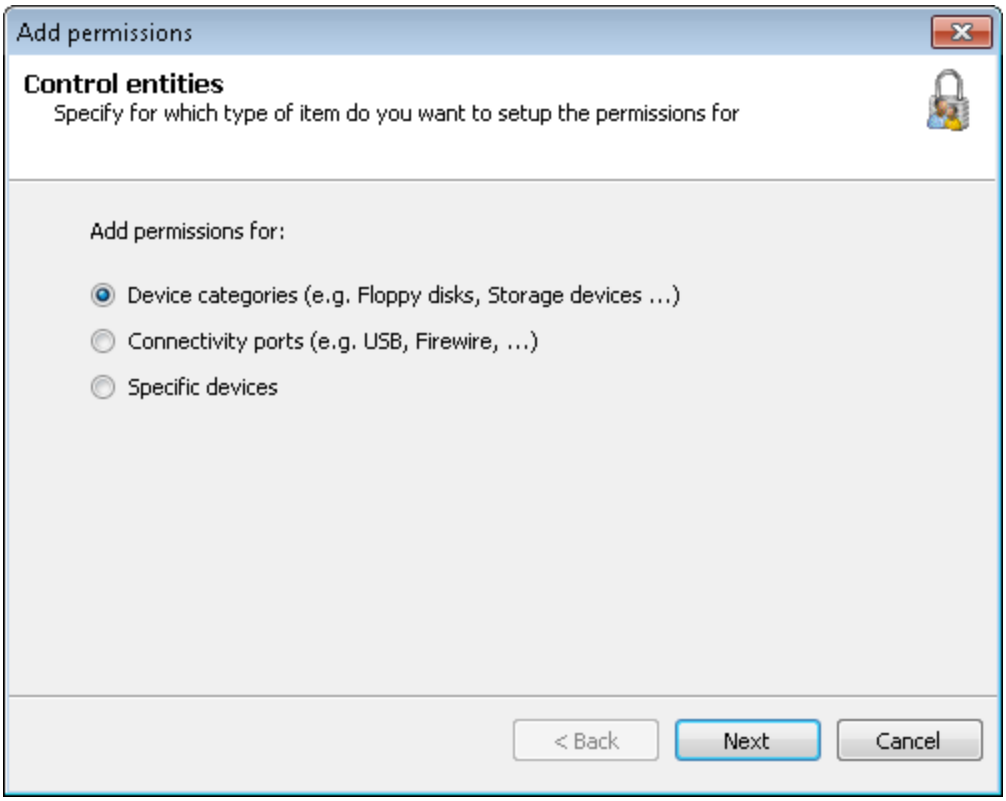
3. Clique na guia **Configuration**.

4. Clique na subguia **Protection Policies**.

5. No painel esquerdo, selecione a política de proteção **General Control**.

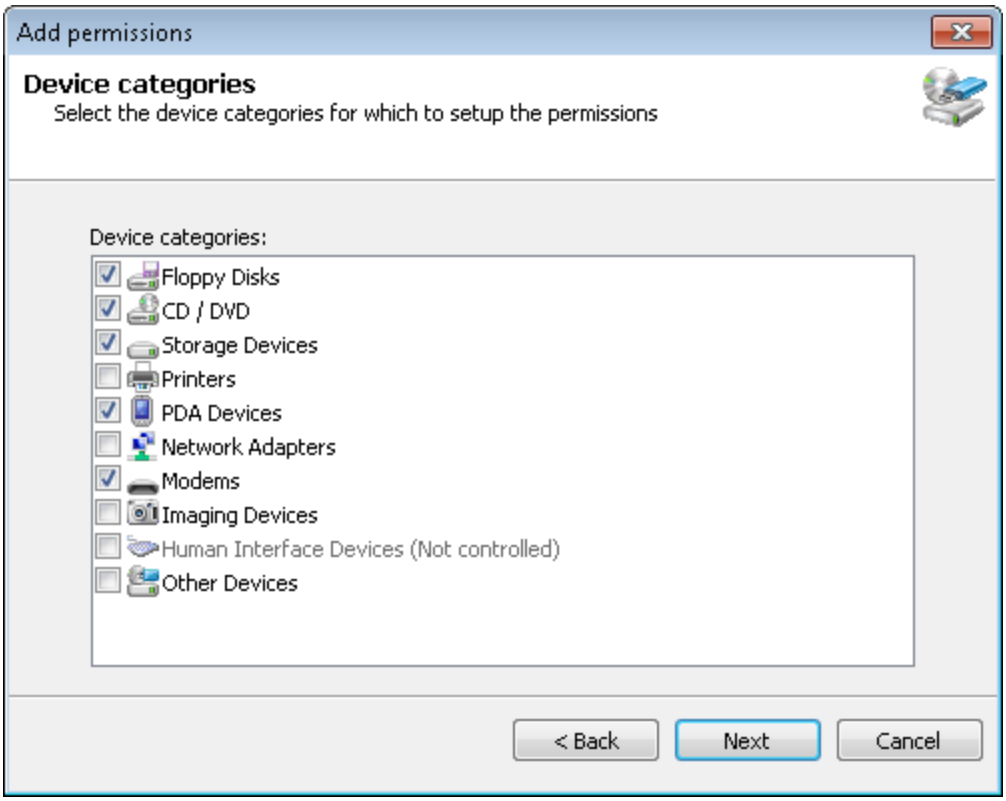
6. Clique no subnó **Security**.

7. A partir do painel esquerdo, clique no hyperlink **Add permission(s)…** na seção **Common tasks**.



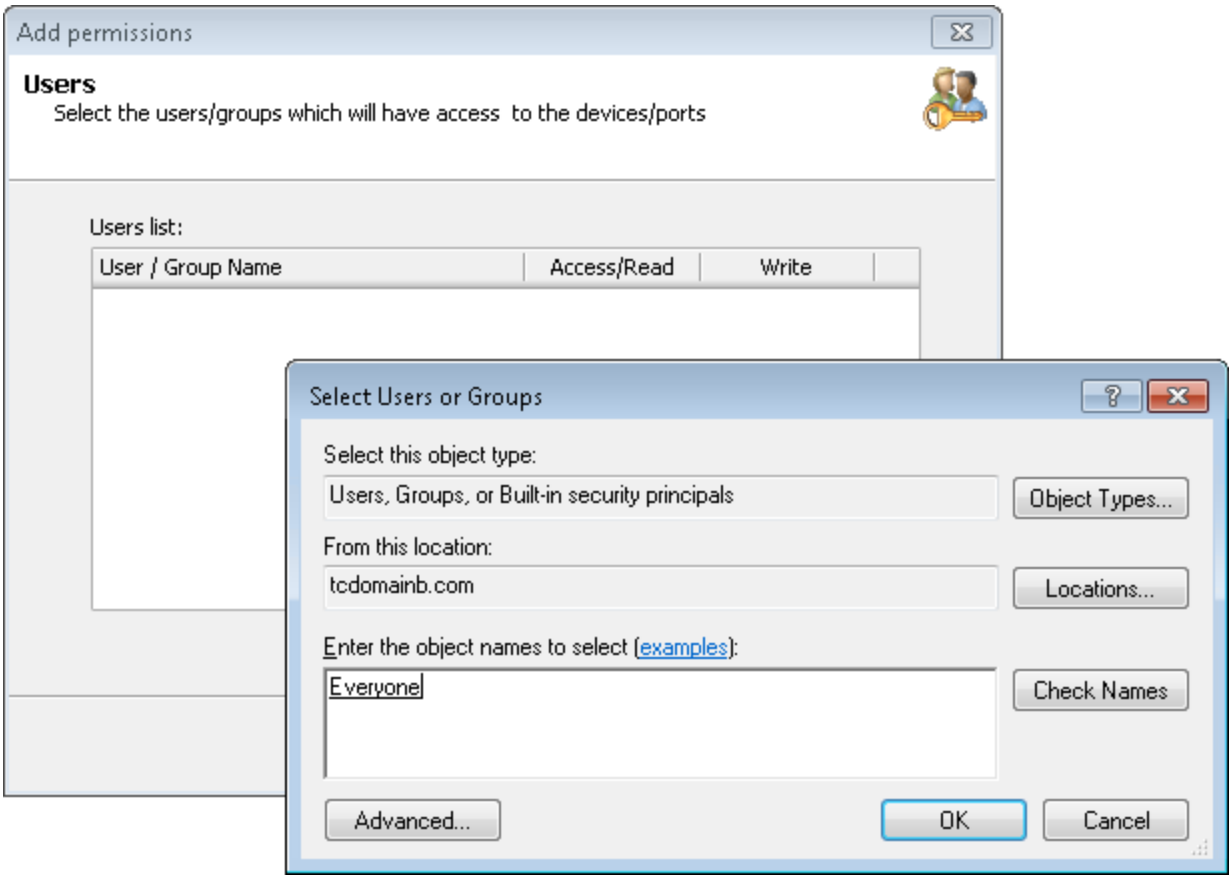
Screenshot 4: Selecionar entidades de controle

8. Na caixa de diálogo **Add permissions...**, selecione a opção **Device categories** e clique em **Next** para continuar.



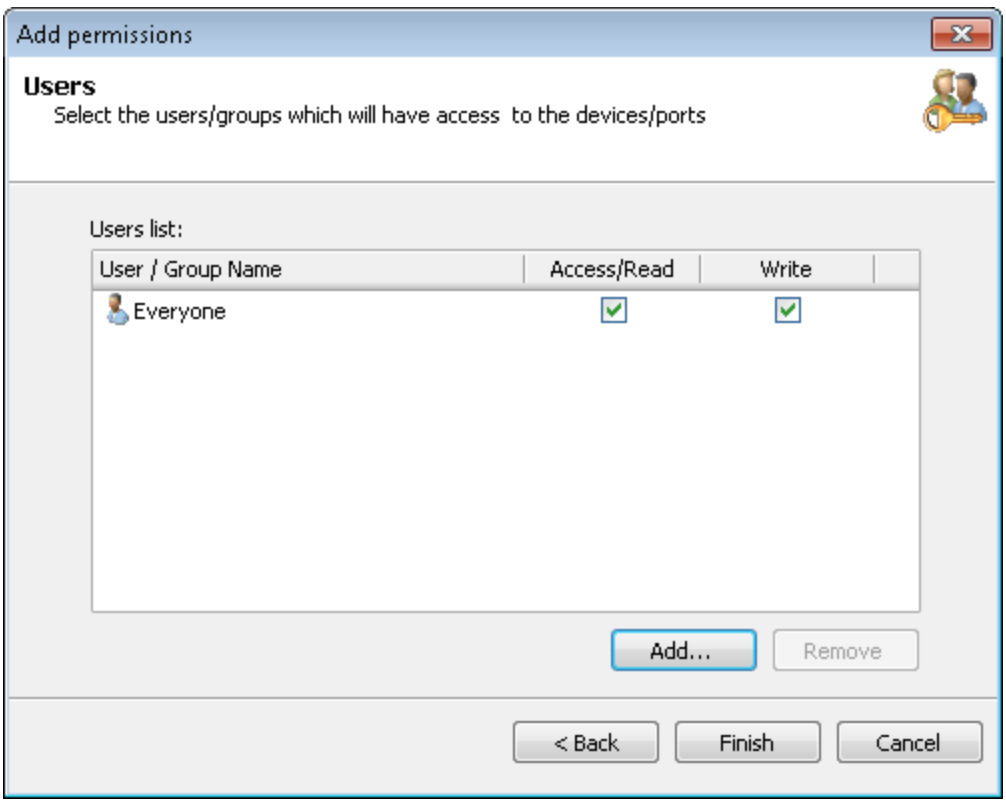
Screenshot 5: Selecionar categorias de dispositivo para atribuir permissões

9. Habilite a categoria do dispositivo de **CD/DVD** e clique em **Next**.



Screenshot 6: Adicionar usuários ou grupos

10. Clique em **Add…** para especificar o usuário sem privilégios administrativos para ter acesso à categoria do dispositivo de CD/DVD especificada nesta política de proteção e clique em **OK**.



Screenshot 7: Selecionar tipos de permissões por usuário ou grupo

11. Habilite as permissões **Access/Read** e **Write** e clique em **Finish**.

Para implantar as atualizações da política de proteção no computador local:

1. A partir do painel direito, clique na mensagem de aviso superior para implantar as atualizações da política de proteção. A exibição deve mudar automaticamente para **Status > Deployment**.

2. A partir da área **Deployment History**, confirme se a atualização foi concluída com êxito no computador local.

Acessar novamente um CD/DVD

Após a atribuição das permissões do usuário, o usuário especificado sem privilégios administrativos deve ter permissão para acessar CD/DVD por meio de unidades de CD/DVD conectadas ao computador local.

Para verificar se os dispositivos e a mídia estão agora acessíveis ao usuário não administrativo:

1. Efetue logon no computador local como usuário sem privilégios administrativos.

2. Insira o mesmo CD/DVD na unidade de CD/DVD.

3. A partir do **Windows Explorer**, localize a unidade de CD/DVD e confirme que agora consegue visualizar e abrir os conteúdos salvos no CD/DVD.

3.3 Voltar às configurações padrão

Para reverter quaisquer ajustes de configuração do GFI EndPointSecurity, volte ao cenário anterior ao teste e efetue o seguinte para o usuário sem privilégios administrativos:

1. Remova a conta do usuário do computador local se tiver sido criada somente para este teste e não for mais necessária.

2. Inclua manualmente o usuário na lista de usuários avançados se tiver sido definido como um usuário avançado anteriormente a este teste. Para obter mais informações, consulte o Manual de administração e configuração do GFI EndPointSecurity.

3. Exclua as permissões de acesso ao dispositivo de CD/DVD para o usuário se não tiverem sido atribuídas permissões de acesso ao dispositivo de CD/DVD antes deste teste. Para obter mais informações, consulte o Manual de administração e configuração do GFI EndPointSecurity.

4 Diversos

O capítulo Diversos compreende toda a informação que não está relacionada com a configuração inicial do GFI EndPointSecurity.

Tópicos neste capítulo

4.1 Licenciamento de produtos 27

4.2 Informações sobre a versão do produto 27

4.1 Licenciamento de produtos

Após instalar GFI EndPointSecurity pode inserir a chave de licença sem reinstalar ou reconfigurar o aplicativo.

Para inserir sua chave de licença:

1. Clique na guia **General**.
2. No painel esquerdo, selecione **Licensing**.

Screenshot 8: Editar chave de licença

3. No painel direito, clique em **Edit…**.
4. Na caixa de texto **License Key**, digite a chave de licença fornecida pela GFI Software Ltd.
5. Clique em **OK** para aplicar a chave de licença.

4.2 Informações sobre a versão do produto

A GFI Software Ltd. liberta atualizações do produto que podem ser manual ou automaticamente baixados do website da GFI.

Para verificar se está disponível uma versão mais recente do GFI EndPointSecuritypara baixar:

1. Clique na guia **General**.
2. No painel esquerdo, selecione **Version Information**.
3. No painel direito, clique em **Check for newer version** para verificar manualmente se está disponível uma versão mais recente do GFI EndPointSecurity. Como alternativa, selecione **Check for newer version at startup** para uma versão mais recente do GFI EndPointSecurity para baixar sempre que o console de gerenciamento for iniciado.

5 Solução de problemas e suporte

Este capítulo explica como resolver os problemas encontrados durante a instalação do GFI EndPointSecurity. As principais fontes de informação disponíveis para solucionar esses problemas são:

Esta seção e o resto da Guia do administrador do GFI EndPointSecurity contêm soluções para todos os possíveis problemas que possam ocorrer. Se não for capaz de resolver um problema, entre em contacto com o suporte da GFI para mais assistência.

Problemas comuns

A tabela abaixo lista os problemas mais comuns que possam ocorrer durante a configuração inicial e durante a primeira utilização do GFI EndPointSecurity e uma possível solução para cada um deles:

Table 9: Solução de problemas comuns

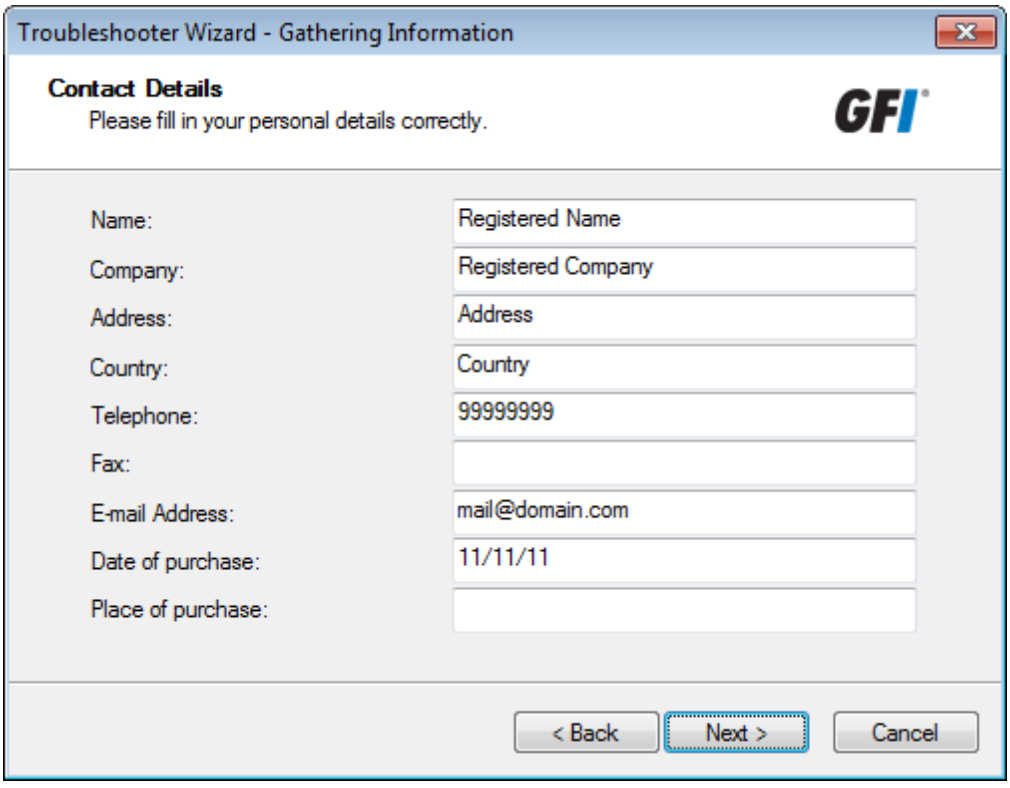
Problema	Possível causa	Possível solução
O computador encontra-se offline.	O console de gerenciamento do GFI EndPointSecurity executa ping no computador de destino na implantação para determinar se está online e se não é exibida esta mensagem.	Se um computador de destino se encontrar offline, a implantação da política relevante é reagendada para uma hora depois. O GFI EndPointSecurity continua tentando implantar essa política a cada hora, até que o computador de destino esteja de novo online. Assegure que o computador de destino está ligado e conectado à rede.
Falha ao conectar ao registro remoto. (erro)	O GFI EndPointSecurity não foi capaz de extrair dados do registro do computador de destino.	Assegure que as configurações de firewall habilitam a comunicação entre computadores de destino e o servidor do GFI EndPointSecurity. Para obter mais informações, consulte Requisitos do sistema.
Falha ao reunir as informações necessárias. (erro)	O GFI EndPointSecurity não foi capaz de extrair dados relacionados com a versão do computador de destino (versão do Sistema operacional e versão de agente do GFI EndPointSecurity).	Para mais detalhes sobre a causa do erro e uma possível solução, consulte a mensagem de erro do sistema entre parênteses.
Falha ao criar os arquivos de instalação necessários. (erro)	O GFI EndPointSecurity não foi capaz de adicionar os arquivos de configuração necessários no arquivo de implantação (arquivo de instalação .msi) do agente GFI EndPointSecurity. Este erro ocorre antes de o arquivo de implantação ser copiado para o computador de destino.	Para mais detalhes sobre a causa do erro e uma possível solução, consulte a mensagem de erro do sistema entre parênteses.
Falha a copiar os arquivos para o computador remoto. (erro)	O GFI EndPointSecurity não foi capaz de copiar o arquivo de implantação (arquivo de instalação .msi) para o computador de destino. Uma causa possível pode ser que o compartilhamento administrativo (C$) que o GFI EndPointSecurity está usando para conectar o computador de destino esteja desabilitado.	Para mais detalhes sobre a causa do erro e uma possível solução, consulte a mensagem de erro do sistema entre parênteses. Para mais informações sobre a conectividade de rede e permissões de segurança, consulte: http://kb.gfi.com/articles/SkyNet_Article/KBID003754?retURL=%2Fapex%2FSupportHome&popup=true
Tempo limite	A implantação do agente no computador de destino está a demorar muito a concluir ou está bloqueada.	Tente implantar novamente o agente do GFI EndPointSecurity.

Problema	Possível causa	Possível solução
Falha ao instalar o serviço de implantação. (erro)	O agente GFI EndPointSecurity não foi capaz de ser instalado ou desinstalado pelo serviço a executar no computador de destino.	Para mais detalhes sobre a causa do erro e uma possível solução, consulte a mensagem de erro do sistema entre parênteses.
Falha na instalação.	A instalação do agente do GFI EndPointSecurity está completa, mas não está assinalada como instalada no registro. Os números da versão e da compilação do agente do GFI EndPointSecurity não são os mesmos que o console de gerenciamento do GFI EndPointSecurity.	Para mais detalhes sobre a causa do erro e uma possível solução, consulte os arquivos de log de instalação do agente no computador de destino em: **%windir%\EndPointSecurity**.
Falha na desinstalação.	A desinstalação do agente do GFI EndPointSecurity está completa, mas não está assinalada como desinstalada no registro.	Para mais detalhes sobre a causa do erro e uma possível solução, consulte os arquivos de log de instalação do agente no computador de destino em: **%windir%\EndPointSecurity**.
Falha na operação devido a uma exceção desconhecida.	No GFI EndPointSecurity ocorreu um erro inesperado.	Use o Assistente de solução de problemas para contatar equipe de suporte técnico GFI. Para abrir o Assistente de solução de problemas, vá para **Start > Programs > GFI EndPointSecurity 2013 > GFI EndPointSecurity 2013 Troubleshooter**.

Usar o Assistente de solução de problemas do GFI EndPointSecurity

Para usar a ferramenta do assistente de solução de problemas fornecido pelo GFI EndPointSecurity:

1. Clique em **Start > Programs > GFI EndPointSecurity2013 > GFI EndPointSecurity2013 Troubleshooter**.
2. Clique em **Next** na tela inicial do assistente.

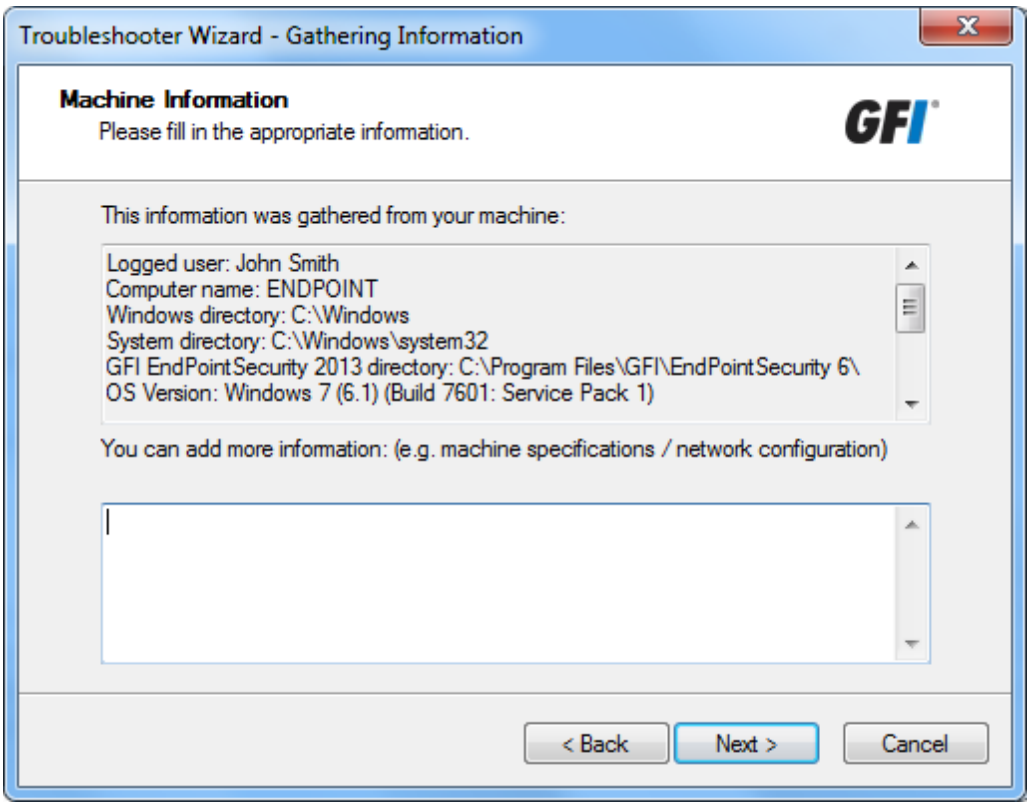


Screenshot 9: Especificar detalhes de contacto e compra

3. Digite os detalhes do contato para que a equipe de suporte possa contatá-lo para mais informação de análise. Clique em **Next**.

Screenshot 10: Especificar detalhes do problema e outras informações relevantes para recriar o problema

4. Especifique o erro recebido e outras informações para ajudar a equipe de suporte a recriar este problema. Clique em **Next**.



Screenshot 11: Coleta de informações da máquina

5. O assistente de solução de problemas analisa o sistema para obter informação do hardware. É possível adicionar manualmente mais informações no espaço fornecido ou clicar em **Next**.

Screenshot 12: Finalizar o assistente de solução de problemas

6. Neste estágio, o assistente de solução de problemas cria um pacote com as informações coletadas nas etapas anteriores. Em seguida, envie este pacote à nossa equipe de suporte para analisar e solucionar o problema. Clique nos botões descritos abaixo para enviar opções:

» **Open Containing Folder** - Abre a pasta que contém o pacote de solução de problemas para que você possa enviá-lo manualmente por email

» **Go to GFI Support** – Abre a página de suporte do website da GFI.

7. Clique em **Finish**.

GFI SkyNet

A GFI mantém um repositório de base de dados de conhecimento que contém respostas para os problemas mais comuns. A GFI SkyNet sempre tem a listagem mais atualizada de perguntas e patches do suporte técnico. Caso as informações deste guia não resolvam seus problemas, consulte a GFI SkyNet em http://kb.gfi.com/.

Fórum da Web

O fórum da Web da GFI oferece suporte técnico de usuário para usuário. Acesse o fórum da Web visitando http://forums.gfi.com/.

Solicitar suporte técnico

Se os recursos aqui mencionados não ajudarem você a resolver seus problemas, contate a equipe de suporte técnico GFI preenchendo o formulário de solicitação de suporte online ou por telefone.

» **Online**: Para enviar a solicitação de suporte, preencha o formulário e siga rigorosamente as instruções desta página: http://support.gfi.com/supportrequestform.asp

» **Telefone**: Para obter o número de telefone do suporte técnico de sua região, visite: http://www.gfi.com/company/contact.htm

> **OBS.**
>
> Ao contatar o suporte técnico, tenha sua ID de cliente em mãos. A ID de cliente é o número da conta online atribuído a você durante o registro das suas chaves de licença na área do cliente GFI em: http://customers.gfi.com.

Responderemos à sua pergunta em até 24 horas, dependendo do seu fuso horário.

Documentação

Se o manual não atender às suas expectativas ou se você tiver sugestões para melhorá-lo, envie um email para documentation@gfi.com.

6 Glossário

A

Acesso temporário

Um período de tempo durante o qual estes usuários podem acessar dispositivos e portas de conexão (quando esse acesso está normalmente bloqueado) em computadores de destino protegidos, para uma janela de duração e tempo específica.

Active Directory

Uma tecnologia que fornece diversos serviços de rede, incluindo serviços de diretório semelhantes a LDAP.

Agente do GFI EndPointSecurity

Um serviço do lado do cliente responsável pela implantação/reforço das políticas de proteção no(s) computador(es) de destino.

Alertas

Um conjunto de notificações (alertas de email, mensagens de rede ou mensagens de SMS) que são enviadas aos destinatários de alerta, quando forem gerados determinados eventos.

Aplicativo GFI EndPointSecurity

Um aplicativo do lado do servidor que ajuda a manter a integridade dos dados, impedindo o acesso não autorizado e a transferência de conteúdo de e para os seguintes dispositivos ou portas de conexão.

Arquivo MSI

Um arquivo gerado por GFI EndPointSecurity para implantação posterior usando GPO ou outras opções de implantação. Pode ser gerado para qualquer política de proteção e contém todas as configurações de segurança definidas, incluindo configurações da instalação para computadores de destino desprotegidos.

Assistente de início rápido

Um assistente para guiá-lo na configuração das definições personalizadas do GFI EndPointSecurity. Abre-se no arranque inicial do console de gerenciamento do GFI EndPointSecurity e serve para uso na primeira vez.

Assistente para criação de políticas de proteção

Um assistente para guiá-lo na criação e configuração de novas políticas de proteção. Ajuste de configuração inclui a seleção de categorias de dispositivo e portas para serem controlados e para ser bloqueado ou permitido a todos o acesso a eles. Este assistente também permite a configuração de filtros com base no tipo de arquivo, permissões de criptografia bem como criação de logs e opção de alertas.

B

Back-end do banco de dados

Um banco de dados pelo GFI EndPointSecurity para manter uma trilha de auditoria de todos os eventos gerados pelos agentes do GFI EndPointSecurity implantados nos computadores de

destino.

BitLocker To Go

Um recurso do Microsoft Windows 7 para proteger e criptografar dados nos dispositivos removíveis.

C

Categoria do dispositivo

Um grupo de periféricos organizado por uma categoria.

Computador de destino

Um computador que é protegido por uma política de proteção de GFI EndPointSecurity.

Console de gerenciamento do GFI EndPointSecurity

A interface do usuário do aplicativo do lado do servidor do GFI EndPointSecurity.

Conta de administrador de alertas

Uma conta do destinatário de alerta que é criada automaticamente pelo GFI EndPointSecurity na instalação.

Criação de log de eventos

Um recurso para gravar eventos relacionados com tentativas feitas para acessar dispositivos e portas de conexão em computadores de destino e operações de serviço.

Criptografia de segurança

Um conjunto de restrições configurado para bloquear ou permitir aos usuários/grupos para acessar tipos de arquivo específicos armazenados em dispositivos que são criptografados com BitLocker To Go. Estas restrições são aplicadas quando os dispositivos criptografados são conectados a computadores de destino abrangidos pela política de proteção.

D

Descoberta automática

Um recurso do GFI EndPointSecurity para buscar e descobrir computadores que forem conectados recentemente à rede nos períodos agendados configurados.

Destinatário de alerta

Uma conta de perfil do GFI EndPointSecurity para manter os detalhes de contacto dos usuários que pretendem receber alertas de email, mensagens de rede e mensagens SMS.

Dispositivos de interface humana

Uma especificação que é parte do Universal Serial Bus (USB) padrão para uma classe de dispositivos periféricos. Estes dispositivos, como mouses, teclados e joysticks, permitem aos usuários introduzir dados ou interagir diretamente com o computador.

F

Ferramenta Temporary Access do GFI EndPointSecurity

Uma ferramenta que está disponível nos computadores de destino. É usado pelo usuário para gerar um código de solicitação e mais tarde introduzir um código de desbloqueio para ativar o acesso temporário, uma vez que for concedido pelo administrador. Na ativação, o usuário terá acesso a dispositivos e portas de conexão (quando tal acesso é normalmente bloqueado) em seu computador de destino protegido para a janela de duração e hora específica.

Filtros do tipo de arquivo

Um conjunto de restrições que são atribuídas a usuários e grupos por tipo de arquivo. A filtragem é baseada nas verificações da extensão de arquivo e nas verificações da assinatura real do tipo de arquivo.

G

GPO

Consulte Objetos de Diretiva de Grupo.

L

Lista de exclusão do dispositivo

Uma lista de dispositivos específicos em que o uso está bloqueado, quando acedido a todos os computadores alvo abrangidos pela política de proteção.

Lista de permissão do dispositivo

Uma lista de dispositivos específicos em que o uso é permitido, quando acedido por todos os computadores de destino abrangidos pela política de proteção.

M

Mensagem do usuário

Uma mensagem que é exibida pelos agentes do GFI EndPointSecurity nos computadores de destino, quando os dispositivos são acessados.

Mensagens de erro de implantação

Erros que podem ocorrer na implantação dos agentes do GFI EndPointSecurity a partir do console de gerenciamento do GFI EndPointSecurity.

O

Objetos de Diretiva de Grupo

Sistema centralizado de gerenciamento e configuração do Active Directory que controla o que os usuários podem ou não fazer em uma rede de computadores.

P

Permissões de acesso

Um conjunto de permissões (acesso, leitura, escrita) que são atribuídas a usuários e grupos por categoria de dispositivos, porta de conectividade ou um dispositivo específico.

Permissões globais

Uma etapa do assistente para criação de políticas de proteção que solicita ao usuário para bloquear ou para permitir acesso a todos os dispositivos inseridos em uma categoria ou que são conectados a uma porta dos computadores de destino abrangidos pela política de proteção.

Política de proteção

Um conjunto de permissões da porta de conectividade e acesso ao dispositivo que pode ser configurada para se adaptar às suas políticas de segurança da empresa de acesso ao dispositivo.

Porta de conectividade

Uma interface entre computadores e dispositivos.

R

Relatório resumido

Um relatório resumido dando uma conta da estatística de atividade como detectado pelo GFI EndPointSecurity.

U

Usuário avançado

É dado automaticamente a um usuário avançado completo acesso a dispositivos conectados a qualquer computador de destino abrangido pela política de proteção.

V

Verificação de dispositivos

Um recurso do GFI EndPointSecurity busca todos os dispositivos que estão ou foram conectados aos computadores de destino verificados.

7 Índice

A

acesso temporário 4-5

alertas 3

assistente

Assistente para criação de políticas de proteção

assistente de início rápido

assistente de solução de problemas 11, 29

assistente de início rápido 11, 22

assistente de solução de problemas 29

B

back-end do banco de dados 9, 19

C

categoria do dispositivo 24

computador de destino 3, 5, 9, 28

D

descoberta automática 13

Dispositivos de interface humana 7

F

Fórum da Web 31

G

GFI EndPointSecurity

agente

aplicativo

management console

Ferramenta Temporary Access

versão 1, 5-6, 8-11, 20, 22-23, 26-28

Glossário 33

L

licenciamento 21

P

política de proteção 1, 5, 10, 22-23

Problemas comuns 28

S

Solução de problemas 28

U

usuários avançados 2, 16, 23, 26

EUA, CANADÁ E AMÉRICA DO SUL E CENTRAL

15300 Weston Parkway, Suite 104 Cary, NC 27513, EUA

Telefone: +1 (888) 243-4329

Fax: +1 (919) 379-3402

ussales@gfi.com

REINO UNIDO E REPÚBLICA DA IRLANDA

Magna House, 18-32 London Road, Staines-upon-Thames, Middlesex, TW18 4BP, Reino Unido

Telefone: +44 (0) 870 770 5370

Fax: +44 (0) 870 770 5377

sales@gfi.com

EUROPA, ORIENTE MÉDIO E ÁFRICA

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

Telefone: +356 2205 2000

Fax: +356 2138 2419

sales@gfi.com

AUSTRÁLIA E NOVA ZELÂNDIA

83 King William Road, Unley 5061, Austrália do Sul

Telefone: +61 8 8273 3000

Fax: +61 8 8273 3099

sales@gfiap.com