Manual do produto GFI

GFI EndPointSecurity™

Guia do administrador

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

Lista de figuras

Lista de tabelas

1 Introdução

A proliferação de dispositivos do consumidor, como iPods, dispositivos USB e smartphones, tem aumentado o risco de vazamentos de dados deliberados e/ou 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 e de perturbar as suas operações diárias.

Tópicos neste capítulo

1.0.1 Termos e convenções usados neste guia

Table 1: Termos e convenções usados neste manual

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

1.1 Ameaças ao dispositivo de mídia portátil

A principal vantagem de dispositivos de mídia portáteis (ou dispositivos portáteis) é o acesso fácil. Em teoria, esta pode ser uma grande vantagem para organizações, mas, ainda assim, é um fato bem reportado de que o acesso e a segurança se encontram em posições opostas do continuum da segurança.

Os desenvolvimentos na tecnologia de mídia removível estão a aumentar. As diferentes versões de dispositivos portáteis, tais como a memória Flash, foram otimizados em termos de:

- Melhor capacidade de armazenamento
- Desempenho melhorado
- Instalação mais fácil e rápida
- Fisicamente pequenos o suficiente para transportar em um bolso.

Como resultado, os usuários internos podem deliberada ou acidentalmente:

- Remover dados confidenciais
- Expor informações confidenciais
- Introduzir códigos maliciosos (exemplo: vírus, cavalos de troia) que podem tornar toda a rede empresarial inativa
- Transferir material inapropriado ou ofensivo para o hardware corporativo
- Efetuar cópias pessoais dos dados e da propriedade intelectual da empresa
- Ficar distraído durante a hora de expediente.

Em uma tentativa para controlar estas ameaças, as organizações começaram a proibir o uso de dispositivos (pessoais) no trabalho. A melhor prática determina que você nunca deverá confiar na conformidade voluntária e que a melhor forma de garantir um controle completo sobre os dispositivos portáteis é colocando barreiras tecnológicas.

1.2 Sobre o GFI EndPointSecurity

O GFI EndPointSecurity é a solução que o 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:

- Portas USB (exemplo: leitores de cartões de memória e flash, pen drives)
- Portas Firewire (exemplo: câmeras digitais, leitores de cartões Firewire)
- Conexões de dados sem fio (exemplo: dongles de infravermelho e Bluetooth)
- Unidades de disquete (internas e externas)
- Unidades óticas (exemplo: CD, DVD)
- Unidades magneto-óticas (internas e externas)
- Unidades de disco rígido USB removíveis
- Outras unidades, como unidades Zip e unidades de fita (internas e externas).

Por meio de sua tecnologia, o GFI EndPointSecurity possibilita permitir ou negar o acesso e atribuir privilégios "totais" ou "somente leitura" para:

- Dispositivos (exemplo: unidades de CD/DVD, PDAs)
- Usuários/grupos de usuários locais ou do Active Directory.

Com o GFI EndPointSecurity é também possível registrar a atividade de todos os dispositivos ou portas de conexão usados em seus computadores de destino (incluindo a data/hora de uso e por quem os dispositivos foram usados).

1.3 Componentes do GFI EndPointSecurity

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

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

1.3.1 Console de gerenciamento do GFI EndPointSecurity

Por meio do Console de gerenciamento 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.

1.3.2 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.

1.4 Recursos principais

O GFI EndPointSecurity oferece os recursos principais seguintes:

Table 2: Recursos do GFI EndPointSecurity

Recursos do GFI EndPointSecurity	
Group-based protection control	No GFI EndPointSecurity é possível configurar e colocar computadores em grupos que são regidos por uma política de proteção. Isto permite configurar uma política de proteção individual e aplicá-la a todos os computadores que pertencem a esse grupo.
Granular access control	O GFI EndPointSecurity possibilita permitir ou negar o acesso a um dispositivo em específico, bem como atribuir (se aplicável) privilégios "totais" ou "somente leitura" a cada dispositivo suportado (por ex., unidades de CD/DVD, PDAs) em uma base de usuário por usuário.
Scheduled deployment	O GFI EndPointSecurity permite agendar a implantação de políticas de proteção e quaisquer alterações de configuração relacionadas sem a necessidade de manter o console de gerenciamento do GFI EndPointSecurity aberto. O recurso de implantação também lida com implantações que falharam por meio do reagendamento automático.

Recursos do GFI EndPointSecurity	
Access control	Além de bloquear uma variedade de categorias de dispositivos, o GFI EndPointSecurity permite também bloquear: » **By file type** - por exemplo, permite ao usuário ler arquivos *.doc, mas bloqueia o acesso a todos os arquivos *.exe » **By physical port** - todos os dispositivos conectados a portas físicas em particular, por exemplo, todos os dispositivos conectados a portas USB » **By device ID** - bloqueia o acesso a um dispositivo individual baseado em uma ID exclusiva de hardware do dispositivo. **OBS.** No Microsoft Windows 7, um recurso denominado BitLocker To Go pode ser usado para proteger e criptografar dados em dispositivos removíveis. O GFI EndPointSecurity realiza verificações em tipos de arquivos reais criptografados com o Windows 7 BitLocker To Go.
Device whitelist and blacklist	O administrador pode definir uma lista de dispositivos específicos que são permitidos permanentemente e outros que são banidos permanentemente.
Power users	O administrador pode especificar usuários ou grupos que teriam sempre acesso total a dispositivos que, de outra forma, estariam bloqueados pelo GFI EndPointSecurity.
Temporary access	O administrador pode conceder acesso temporário a um dispositivo (ou grupo de dispositivos) em um computador específico. Este recurso permite ao administrador gerar um código de desbloqueio que o usuário final pode usar para obter um acesso limitado no tempo a um dispositivo ou porta em particular, mesmo quando o agente do GFI EndPointSecurity não se encontra conectado à rede.
Status dashboard	A interface do usuário do painel mostra os status dos agentes ativos e implantados, os servidores do banco de dados e de alertas, o serviço do GFI EndPointSecurity, bem como dados estatísticos com gráficos. O aplicativo principal mantém o registro do status do agente ativo comunicando com seus agentes implantados. As tarefas de manutenção são realizadas automaticamente assim que um agente ficar online.
Active Directory deployment through MSI	A partir do console de gerenciamento do GFI EndPointSecurity é possível gerar arquivos MSI que podem, posteriormente, ser implantados usando o recurso Group Policy Object (GPO) incluído no Active Directory ou em outras opções de implantação. Um arquivo MSI conterá todas as configurações de segurança ajustadas em uma política de proteção em particular.
Agent management password	As funções de gerenciamento do agente (tais como a atualização e desinstalação) estão protegidas por uma senha configurável pelo usuário. Isto significa que nenhuma outra instância do GFI EndPointSecurity terá acesso às opções de gerenciamento do agente.
Device discovery	O mecanismo do GFI EndPointSecurity pode ser usado para verificar e detectar a presença de dispositivos na rede, mesmo em computadores que não possuem qualquer política de proteção. As informações coletadas sobre dispositivos detectados podem ser usadas para formar políticas de segurança e atribuir os direitos de acesso a dispositivos específicos.
Logs browser	Uma ferramenta integrada permite ao administrador procurar logs da atividade do usuário e do uso do dispositivo que é detectado pelo GFI EndPointSecurity.
Alerting	O GFI EndPointSecurity permite configurar alertas de email, mensagens de rede e mensagens de SMS que podem ser enviados para destinatários especificados quando os dispositivos são conectados ou desconectados, quando o acesso a dispositivos é permitido ou bloqueado e em caso de eventos gerados por serviços.
Custom messages	Quando os usuários são bloqueados relativamente ao uso de dispositivos, são exibidas mensagens pop-up explicando os motivos pelos quais o dispositivo foi bloqueado. O GFI EndPointSecurity permite a personalização destas mensagens.
Database maintenance	Para manter o tamanho do back-end do banco de dados, o GFI EndPointSecurity pode ser definido para efetuar backup ou excluir os eventos mais antigos que um número personalizado de horas ou dias.
Device encryption	Para máxima segurança, o GFI EndPointSecurity pode ser configurado para criptografar dispositivos de armazenamento usando a criptografia AES 256. A criptografia pode ser reforçada em computadores específicos que executam agentes na rede.

Recursos do GFI EndPointSecurity	
Data leakage risk assessment	O painel permite aos usuários ver o potencial risco de vazamento de dados para cada ponto de extremidade. Use as dicas fornecidas e realize ações sugeridas para reduzir os níveis dos riscos.
Content awareness	O recurso de conscientização de conteúdo permite aos usuários verificar os arquivos que entram nos pontos de extremidade por meio de dispositivos removíveis. O conteúdo é identificado com base nas expressões regulares predefinidas (ou personalizadas) e em arquivos de dicionário. Por padrão, o recurso procura detalhes confidenciais protegidos, tais como senhas e números de cartão de crédito.

1.5 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:

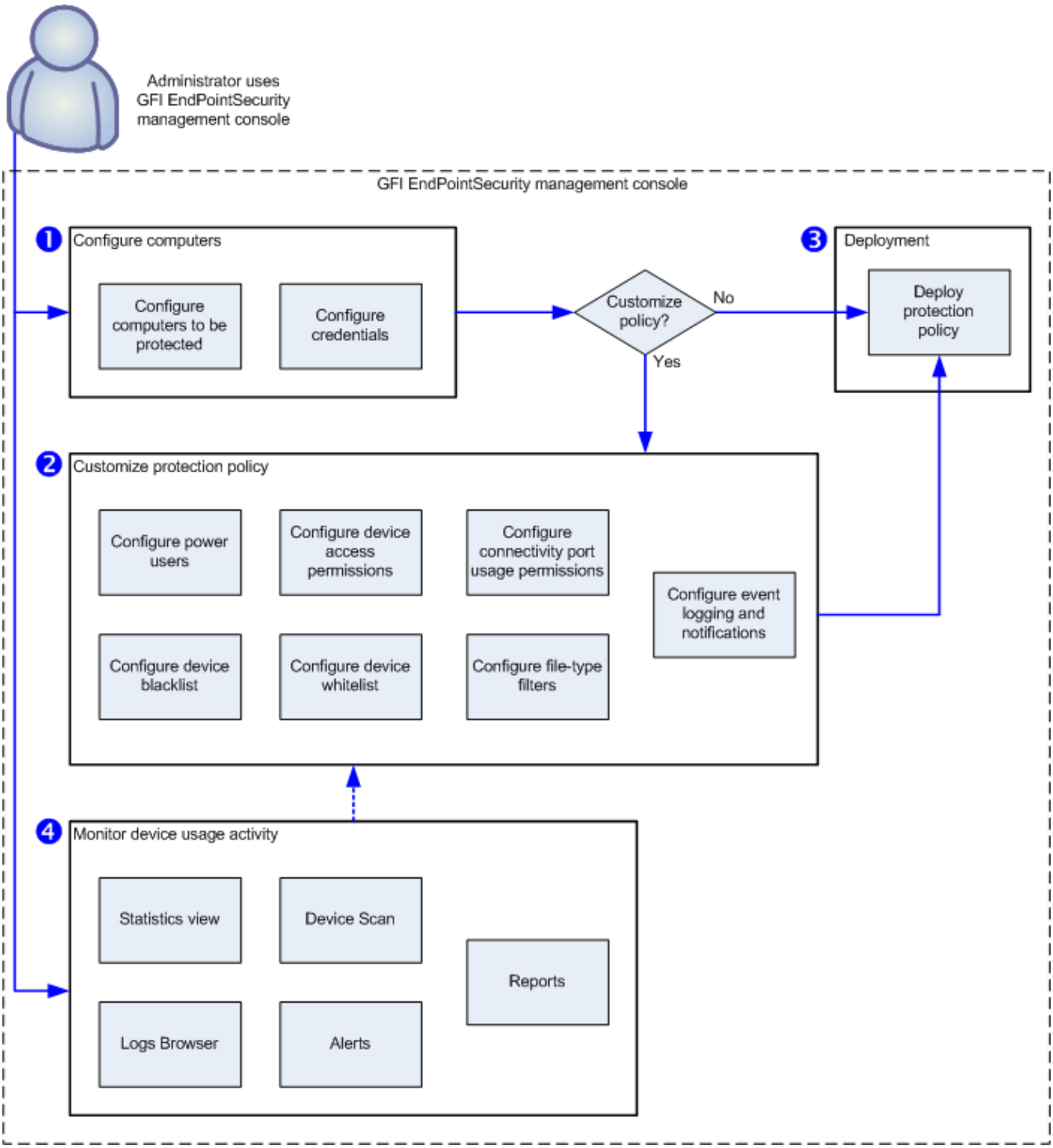


Figure 1: Política de proteção - implantação e monitoramento

A tabela abaixo descreve os estágios representados acima:

Table 3: 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.

1.6 Como funciona o GFI EndPointSecurity - acesso a dispositivos

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

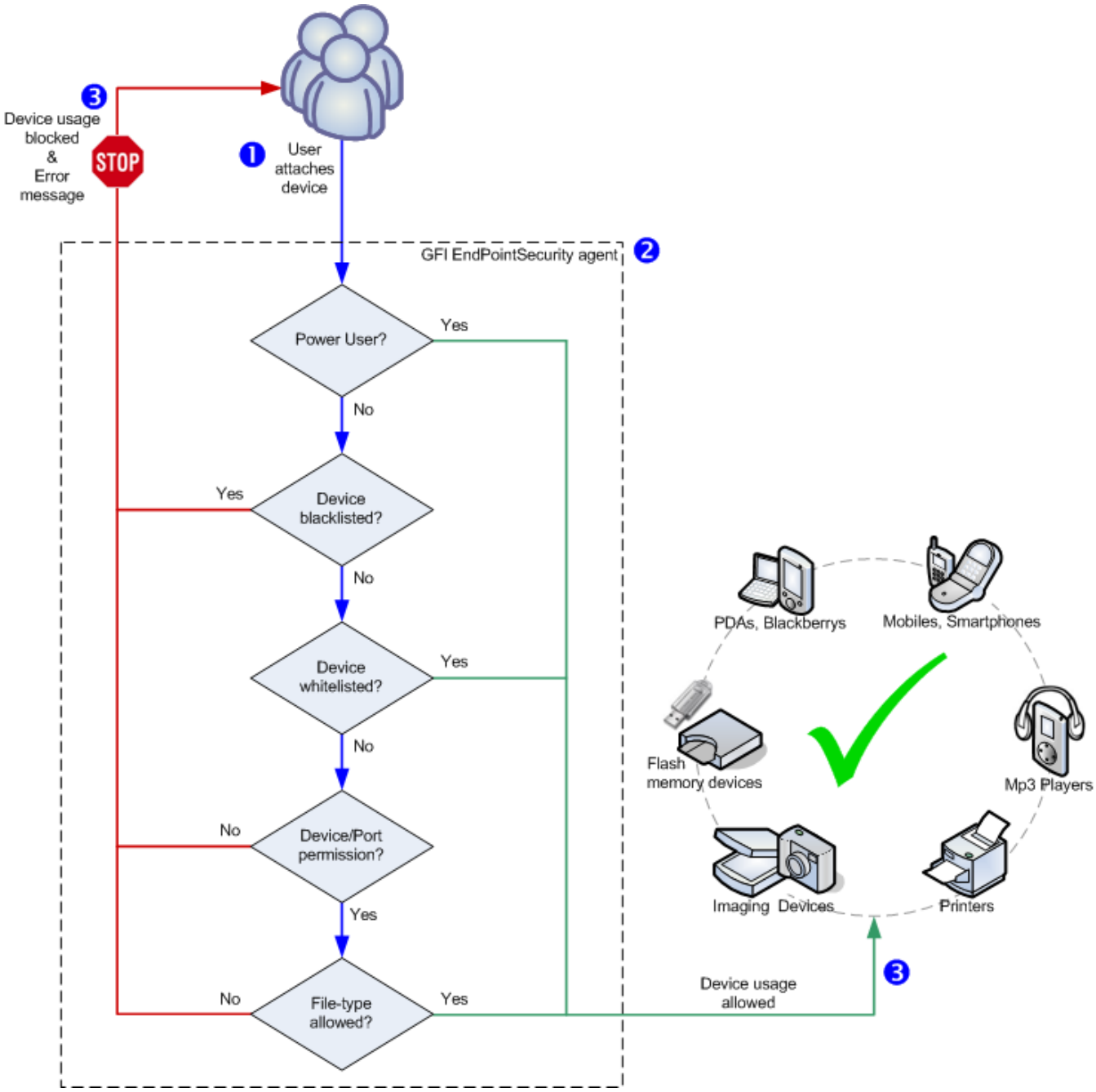


Figure 2: Acesso a dispositivos

A tabela abaixo descreve os estágios representados acima:

Table 4: 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.

1.7 Como funciona o GFI EndPointSecurity - acesso temporário

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

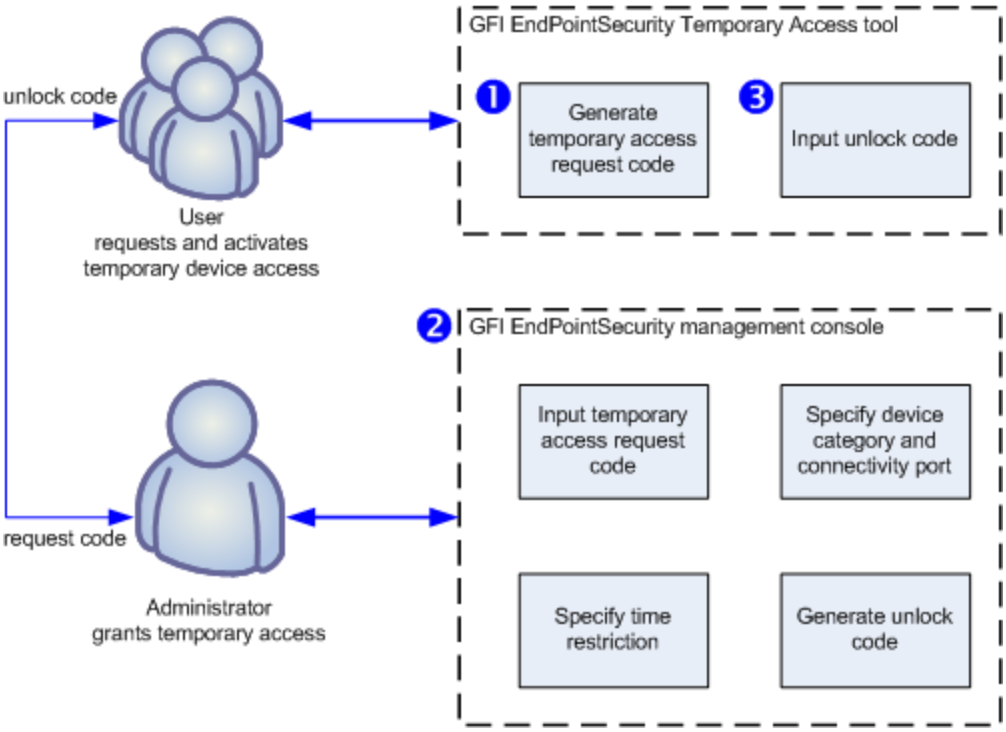


Figure 3: Solicitar/conceder acesso temporário

A tabela abaixo descreve os estágios representados acima:

Table 5: 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.

1.8 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 ex., 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).

1.9 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).

1.10 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 1: Navegar na interface de usuário do GFI EndPointSecurity

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

Seção	Descrição
	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.

Seção	Descrição
	Sub-tabs Acessar mais definições e/ou informações sobre a guia selecionada da seção 1.
	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.
	Right Pane Defina as opções de configuração selecionadas do painel esquerdo. Disponível somente para algumas guias.

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

Requisitos de hardware

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

Table 6: 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:

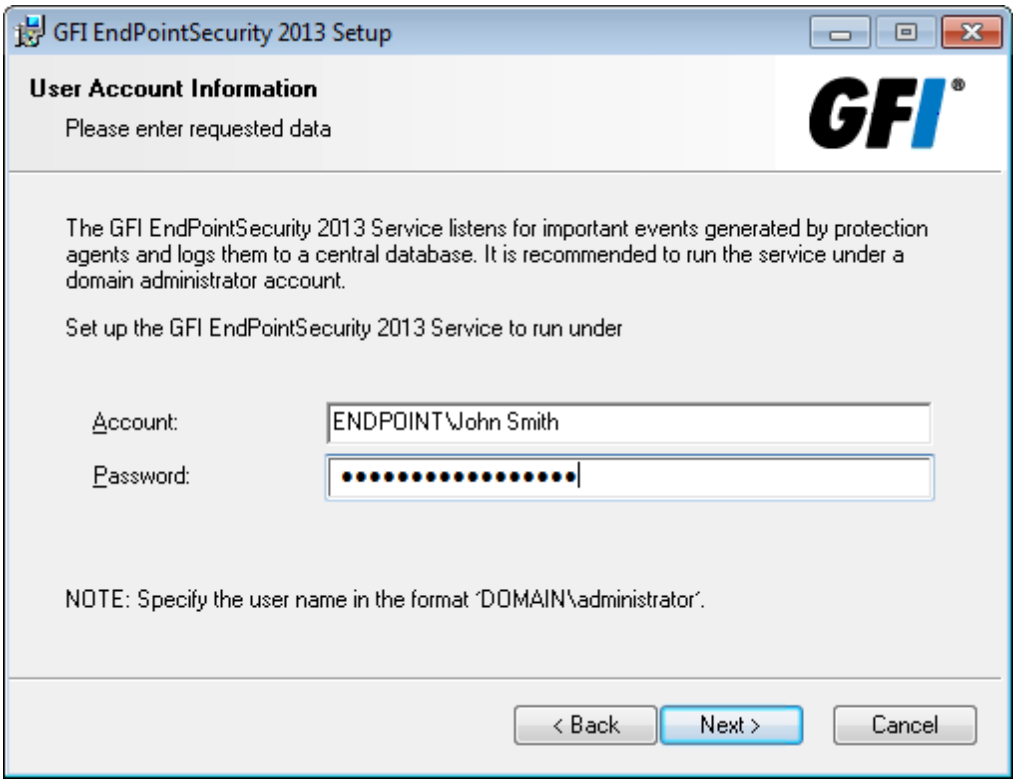
1. Faça logon da máquina na qual GFI EndPointSecurity será instalado, usando os privilégios administrativos.

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

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

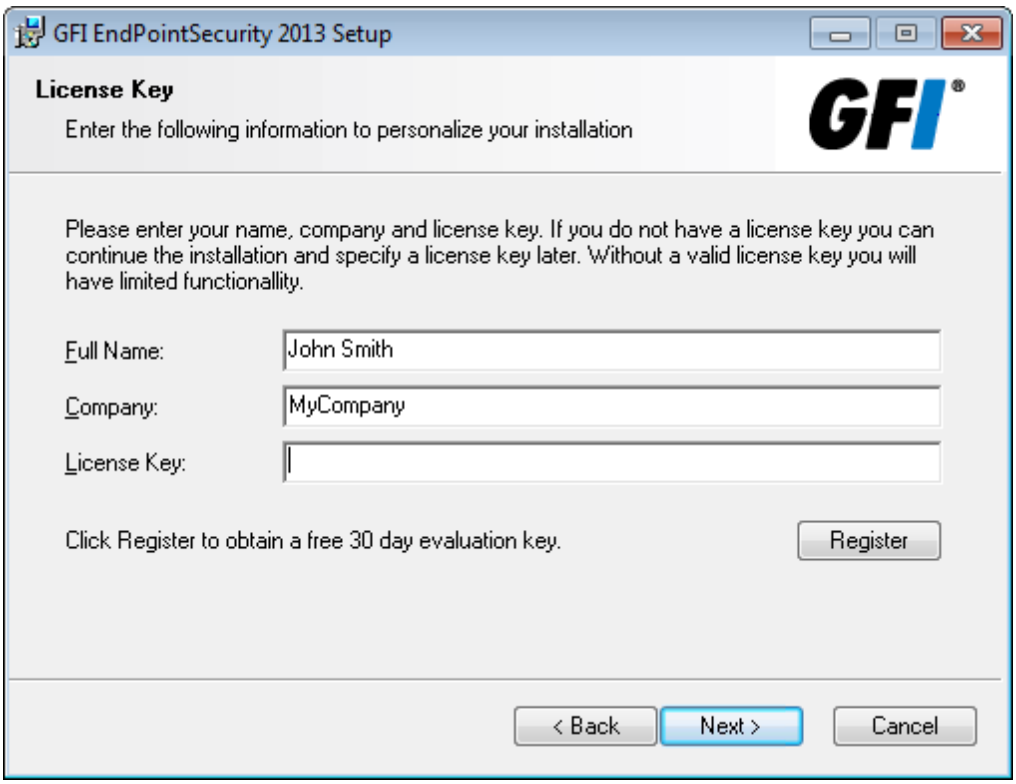
3. Clique em **Next** na tela inicial de boas-vindas.

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



Screenshot 2: 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 3: 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.

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 7: 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**.
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 8: 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 9: 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 4: Navegar na interface de usuário do GFI EndPointSecurity

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

Seção	Descrição
	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.
	Sub-tabs Acessar mais definições e/ou informações sobre a guia selecionada da seção 1.
	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.
	Right Pane Defina as opções de configuração selecionadas do painel esquerdo. Disponível somente para algumas guias.

2.6 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.

Esta seção contém as seguintes informações:

» Pré-condições de teste

» Caso de teste

» Voltar às configurações padrão

2.6.1 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.

2.6.2 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:

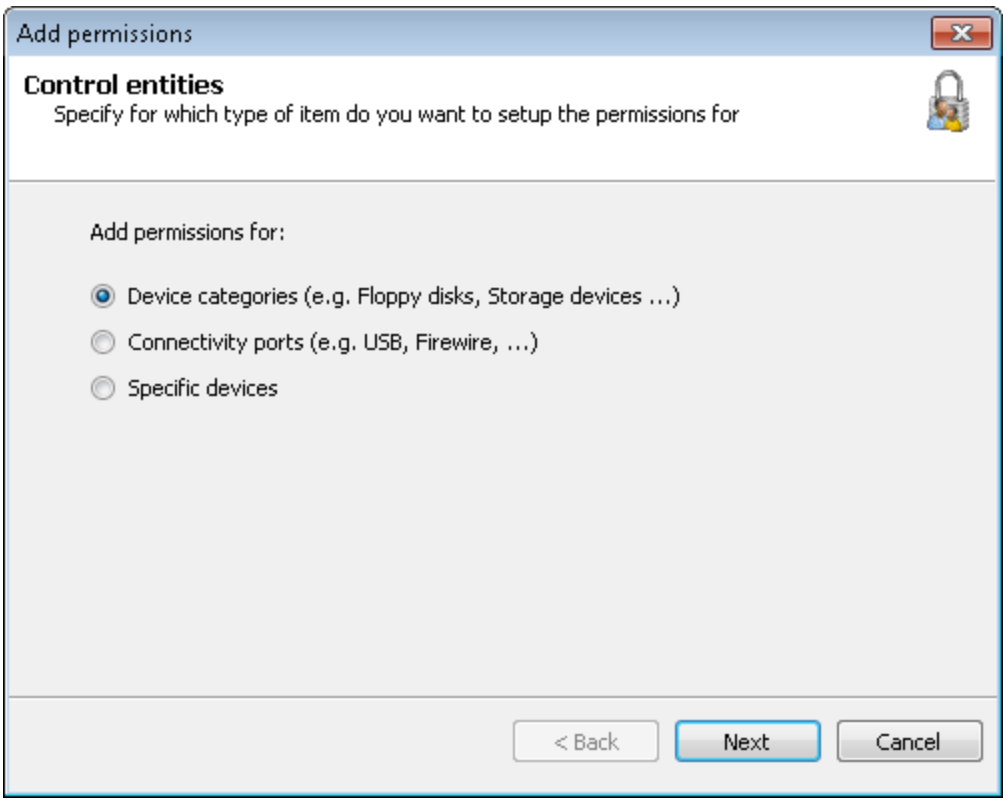
1. Efetue logon no computador local como usuário sem privilégios administrativos.
2. Insira o CD/DVD na unidade de CD/DVD.

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

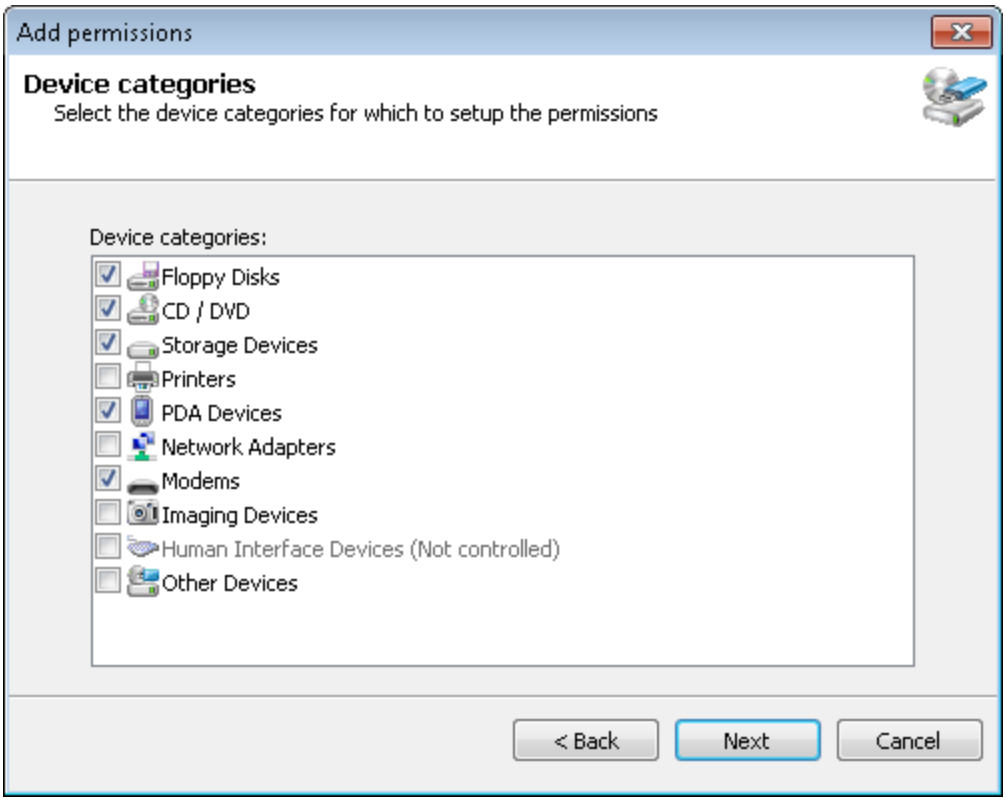
Para atribuir permissões de acesso ao dispositivo de CD/DVD ao usuário sem privilégios administrativos:

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**.



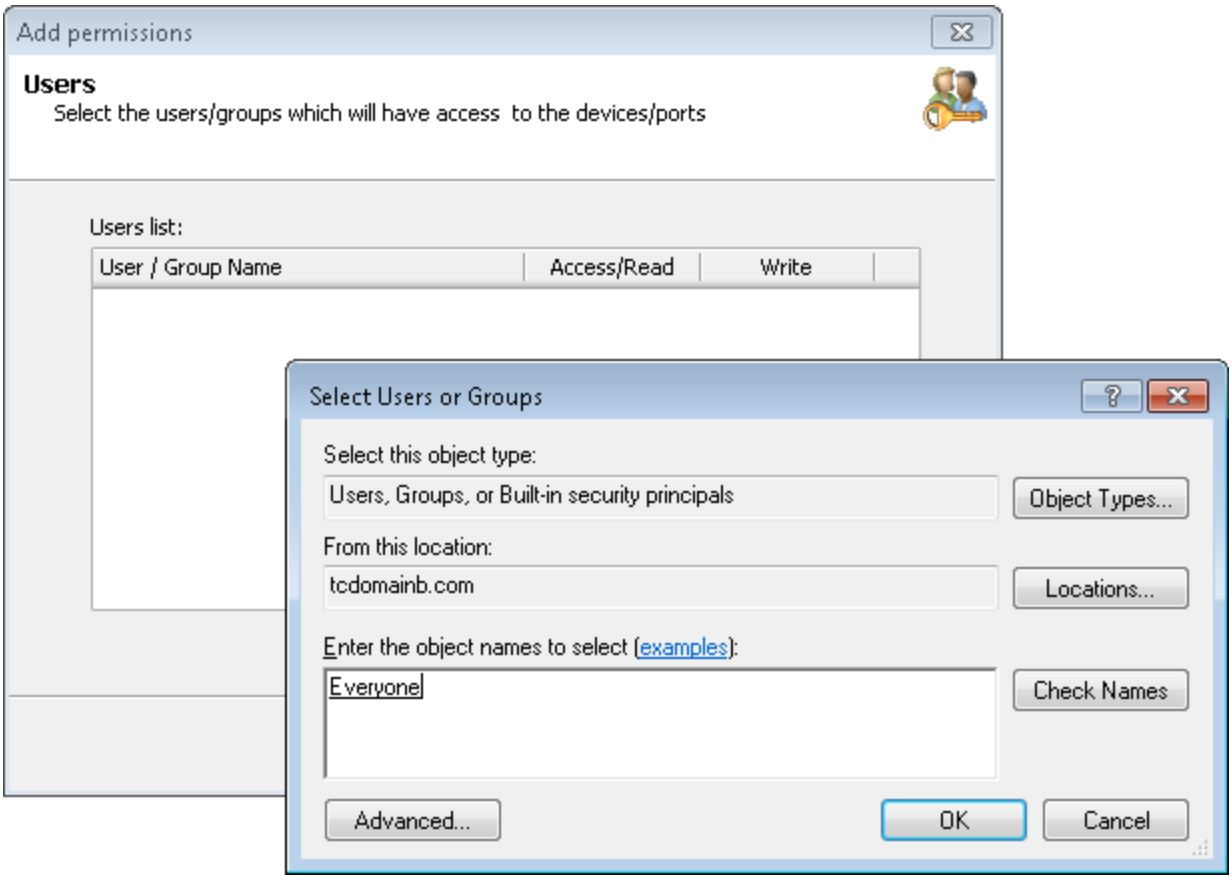
Screenshot 5: Selecionar entidades de controle

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



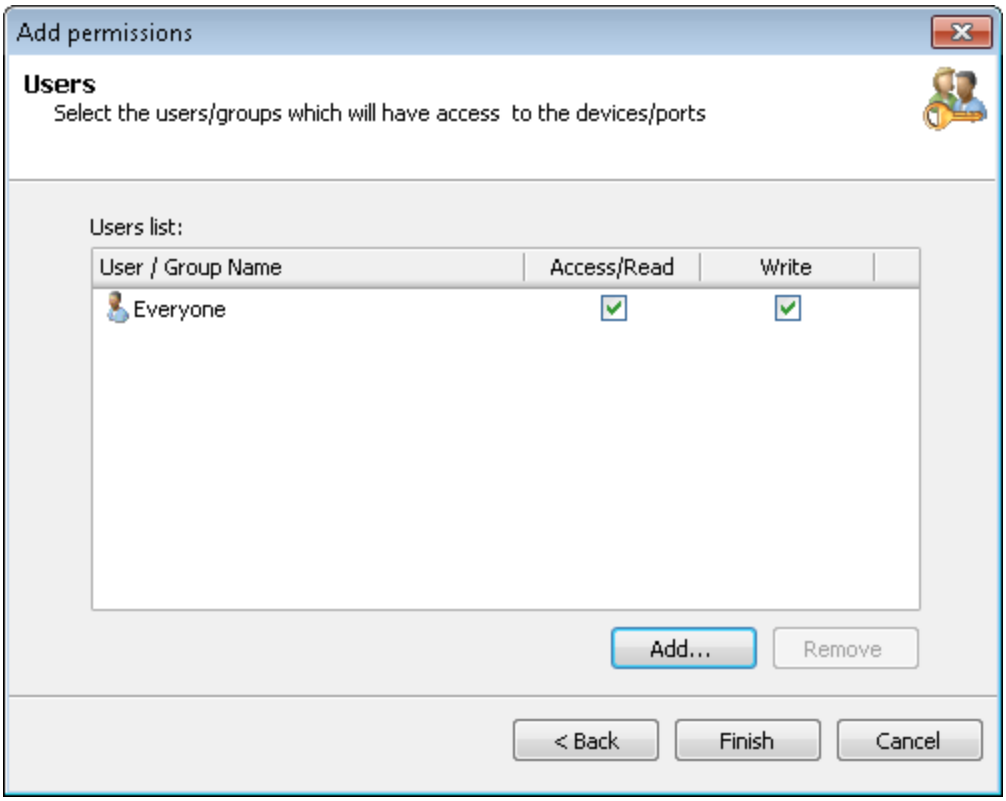
Screenshot 6: Selecionar categorias de dispositivo para atribuir permissões

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



Screenshot 7: 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 8: 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.

2.6.3 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.

3 Obter resultados

Este capítulo fornece instruções detalhadas sobre como bloquear dispositivos não autorizados da rede e tornar os pontos de extremidade seguros usando o GFI EndPointSecurity. Este capítulo ajuda a obter os resultados positivos de conformidade legal, garantindo que a sua rede esteja protegida usando os métodos e as técnicas de detecção de vulnerabilidade mais atualizados.

Tópicos neste capítulo

3.1 Prevenir vazamentos de dados e infecções de malware

A maioria dos roubos de dados ocorre internamente por funcionários transferindo manualmente dados para dispositivos de armazenamento removíveis. Usar dispositivos de armazenamento removíveis não autorizados pode expor a rede a um maior risco de infecções de malware. O GFI EndPointSecurity permite controlar de forma abrangente o acesso a dispositivos de armazenamento portáteis com esforço administrativo mínimo. O acesso temporário pode ser garantido a usuários finais de um dispositivo em um computador específico durante um período de tempo em particular.

1. Implantar agentes em computadores que necessitam de proteção

Os agentes do GFI EndPointSecurity são usados para proteger computadores na rede. Os agentes podem ser implantados manualmente, após a instalação de agentes em computadores específicos ou automaticamente ao instalar agentes em cada novo ponto de extremidade descoberto na rede. Consulte as seguintes seções para obter informações sobre:

- Adicionar computadores manualmente
- Adicionar computadores automaticamente
- Configurar as credenciais de logon.

2. Criar uma política de proteção para bloquear armazenamento removível

Os agentes protegem computadores com base em configurações de uma política de segurança atribuída. É possível criar tantas políticas de segurança quanto necessário e cada política pode conter diferentes configurações para diferentes níveis de autorização. Consulte as seguintes seções para obter informações sobre:

- Criar políticas de proteção
- Atribuir políticas de proteção
- Implantar políticas imediatamente
- Agendar a implantação de políticas
- Implantar políticas por meio do Active Directory
- Verificar a implantação de políticas de proteção.

3. Definir as configurações de políticas de proteção

Configure a política de proteção para bloquear dispositivos de armazenamento removíveis. Esta situação evita que usuários finais usem dispositivos que permitem transferir dados de e para um computador. Consulte as seguintes seções para obter informações sobre:

- Configurar categorias de dispositivos controladas
- Configurar permissões de acesso para categorias de dispositivos
- Configurar permissões de acesso para dispositivos específicos
- Configurar prioridades para permissões
- Ver permissões de acesso
- Configurar a lista de exclusão do dispositivo.

4. Configurar alertas de notificação em caso de tentativas de violações da política de segurança

O GFI EndPointSecurity pode enviar notificações a um destinatário individual ou a um grupo de destinatários quando um usuário final tenta violar uma política de segurança. Isto permite tomar as medidas necessárias de imediato e acabar com o uso não autorizado de dispositivos de armazenamento removíveis. Consulte as seguintes seções para obter informações sobre:

- Configurar alertas
- Configurar opções de alertas
- Configurar a conta de administrador de alertas
- Configurar destinatários de alertas
- Configurar grupos de destinatários de alertas.

5. Configurar acesso temporário ao uso genuíno de dispositivos de armazenamento removíveis

Se uma política de proteção de bloqueio estiver ativa, o GFI EndPointSecurity ainda permite o acesso temporário a um dispositivo para transferir genuinamente dados para e de um computador. Consulte as seguintes seções para obter informações sobre:

- Como funciona o GFI EndPointSecurity – acesso temporário
- Configurar usuários avançados
- Configurar os privilégios de acesso temporário
- Configurar a lista de permissão do dispositivo
- Configurar mensagens do usuário.

3.2 Automatizar a proteção de rede

Após a configuração do GFI EndPointSecurity, é possível proteger automaticamente novos computadores que são detectados em redes acessíveis. Isto pode ser conseguido especificando o(s) domínio(s) e/ou grupo(s) de trabalho que deve(m) ser verificado(s) em novos computadores e, em caso de detecção de um, o GFI EndPointSecurity instala um agente automaticamente e atribui a política padrão ao mesmo. As políticas podem ser alteradas a partir da guia Configuration > subguia Computers.

1. Descobrir automaticamente dispositivos na rede

O GFI EndPointSecurity permite adicionar automaticamente novos computadores que estão conectados à rede. Isto permite verificar um domínio ou um grupo de trabalho especificado e adicionar os computadores que se encontram no mesmo. Consulte as seguintes seções para obter informações sobre:

- Executar uma verificação de dispositivos
- Analisar resultados de verificação de dispositivos
- Adicionar dispositivos descobertos ao banco de dados.

2. Implantar agentes nos novos dispositivos descobertos

O GFI EndPointSecurity pode ser configurado para instalar automaticamente agentes em novos computadores que são adicionados ao banco de dados. Deve ser instalado um agente em cada computador que necessita de proteção. Consulte as seguintes seções para obter informações sobre:

- Adicionar computadores automaticamente
- Configurar opções avançadas
- Configurar as credenciais de logon.

3. (Opcional) Configurar a política de proteção que está atribuída aos dispositivos descobertos recentemente

Se uma política de proteção não for configurada para implantação, crie uma política que possa ser atribuída a novos agentes que estão sendo instalados nos computadores descobertos. A política padrão deve ser atribuída a um novo agente, mas pode ser alterada a partir da guia Configuration > subguia Computers. As configurações de segurança e o comportamento do dispositivo são impostos pela política. Consulte a seção a seguir para obter informações sobre:

- Personalizar políticas de proteção
- Configurar uma política como política padrão.

4. Atribuir políticas de proteção automaticamente

Configure o GFI EndPointSecurity para implantar automaticamente políticas de proteção em novos agentes. Consulte as seguintes seções para obter informações sobre:

- Agendar a implantação de políticas
- Implantar políticas por meio do Active Directory
- Verificar a implantação de políticas de proteção.

5. Monitorar a atividade dos dispositivos

O GFI EndPointSecurity permite manter uma trilha de auditoria dos logs de atividades gerados por agentes implantados em computadores de rede (o log de eventos deve estar habilitado). As guias Status e Activity permitem ver status e informações estatísticas sobre pontos de extremidade, agentes e GFI EndPointSecurity. Consulte as seguintes seções para obter informações sobre:

- Configurar o log de eventos
- Ver a atividade de uso dos dispositivos
- Ver estatísticas de uso dos dispositivos.

3.3 Monitorar a atividade de rede a partir de uma localização central

Os agentes geram logs de atividades que são armazenados em um banco de dados do SQL Server. O GFI EndPointSecurity mantém uma trilha de auditoria desses logs e fornece as informações em um conjunto de exibições do painel. As extensivas exibições do painel do GFI EndPointSecurity permitem monitorar a atividade de rede em tempo real, permitindo ao administrador tomar medidas imediatas quando é detectado um risco de segurança. Configure o GFI EndPointSecurity para gerar e enviar periodicamente (diariamente/semanalmente/mensalmente) relatórios para a equipe de gerenciamento e de TI para uma análise completa dos status de segurança do ponto de extremidade.

1. Analisar a atividade em toda a rede

As subguias fornecidas nas guias Status e Activity permitem monitorar a atividade de rede a partir de uma localização central. Estas guias fornecem uma avaliação de risco, estatísticas, status, logs de atividades e informações de implantação usando gráficos e tabelas. Consulte as seguintes seções para obter informações sobre:

- Analisar detalhes de avaliação do risco
- Analisar estatísticas
- Analisar informações de status
- Analisar detalhes de implantação do agente
- Analisar logs de atividades.

2. Gerar relatórios com base em logs de atividades gerados por agentes na rede

O GFI EndPointSecurity contém uma lista extensa de relatórios que podem ser usados tal como estão ou mesmo modificados para se adequarem ainda mais a suas exigências em termos de relatórios. O ReportPack contém relatórios técnicos para equipe de TI, bem como relatórios executivos para fins de gerenciamento. Consulte as seguintes seções para obter informações sobre:

- Usar oGFI EndPointSecurity ReportPack
- Gerar relatórios resumidos.

3. Realizar a manutenção do back-end do banco de dados

O GFI EndPointSecurity armazena logs de eventos em um banco de dados do SQL Server. Em uma rede grande com muita atividade, o tamanho do banco de dados pode aumentar exponencialmente e o desempenho de leitura/gravação entre o GFI EndPointSecurity e o banco de dados pode degradar-se. Recomenda-se a configuração das definições de retenção do log para excluir automaticamente eventos antigos ou indesejados ou até mesmo criar um novo banco de dados quando o atual alcançar um tamanho específico. Consulte as seguintes seções para obter informações sobre:

- Realizar a manutenção do back-end do banco de dados
- Usar uma instância existente do SQL Server.

4 Adicionar computadores de destino

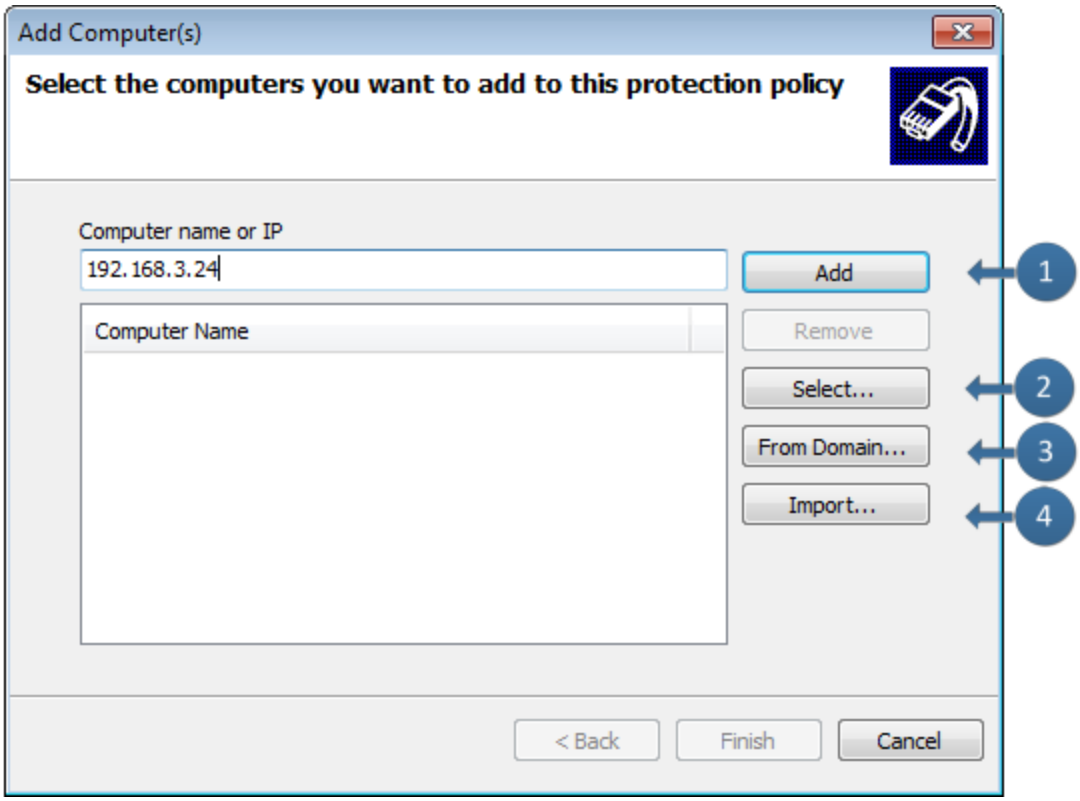
O GFI EndPointSecurity permite especificar os computadores nos quais deseja implantar agentes e políticas de proteção.

Tópicos neste capítulo

4.1 Adicionar computadores manualmente

Para adicionar manualmente um computador de destino:

1. Clique na guia **Configuration > Computers**.
2. Em **Common tasks**, clique em **Add computer(s)...**



Screenshot 9: Adicionar computadores manualmente

3. A tabela abaixo descreve as opções disponíveis da caixa de diálogo **Add Computer(s)**:

Table 10: Opções da caixa de diálogo Add Computer(s)

Opção	Descrição
1	Digite o nome/IP do computador de destino para adicionar e clique em **Add**. Repita esta etapa para cada computador de destino que deseja adicionar a esta política de proteção.
2	Clique em **Select...**. Na caixa de diálogo **Select Computers**, selecione o domínio/grupo de trabalho relevante a partir da lista suspensa e clique em **Search**. Habilite o(s) computador(es) necessário(s) e clique em **OK**.

Opção	Descrição
3	Clique em **From Domain…**. Especifique o(s) computador(es) necessário(s) a partir do domínio/grupo de trabalho em que o GFI EndPointSecurity reside.
4	Clique em **Import...**. Procure a localização do arquivo de texto que contém uma lista de computadores a ser importada. **Obs.** Especifique SOMENTE um nome/IP de computador por linha.

4. Clique em **Finish**.

4.2 Adicionar computadores automaticamente

O GFI EndPointSecurity permite buscar e adicionar novos computadores quando estes estão conectados a sua rede em intervalos específicos de tempo. Isto permite adicionar automaticamente computadores assim que estes são detectados na rede. Por meio dos recursos de Auto Discovery, é possível configurar:

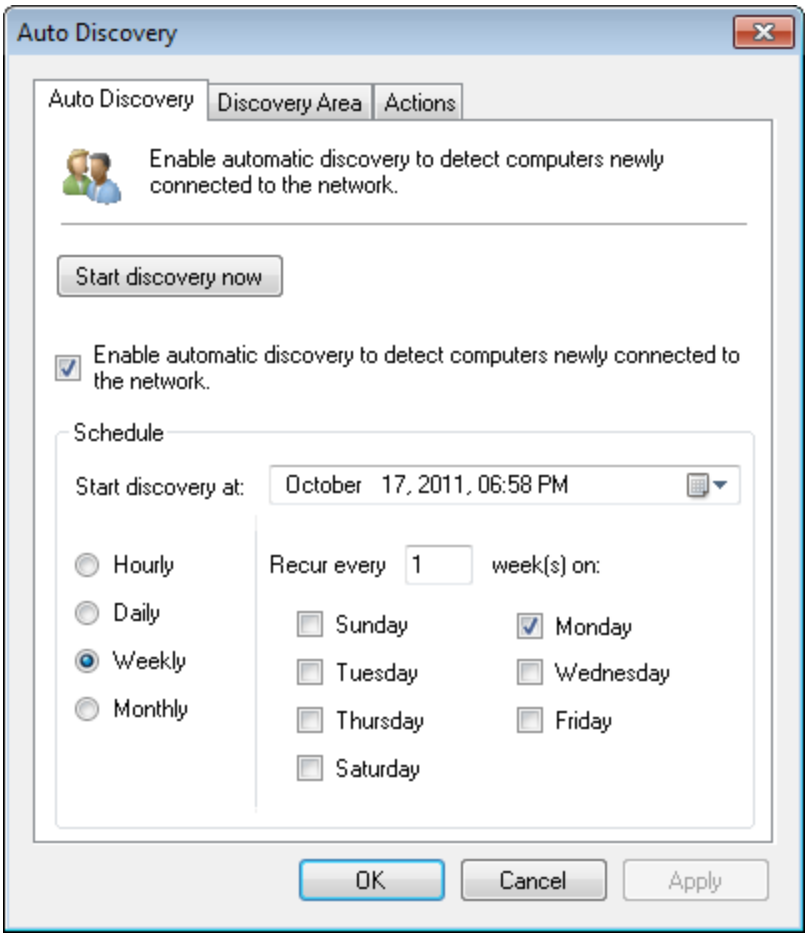
- A frequência e o agendamento das buscas
- O domínio/grupo de trabalho da descoberta a verificar
- A política atribuída aos novos computadores de destino descobertos e às credenciais de logon.

Por padrão:

- As configurações da descoberta automática são definidas para verificar o domínio/grupo de trabalho atual (domínio/grupo de trabalho no qual oGFI EndPointSecurity reside)
- As configurações de instalação do agente estão definidas para atribuir a política de proteção **General Control** (política de proteção padrão de envio) nos computadores descobertos recentemente.

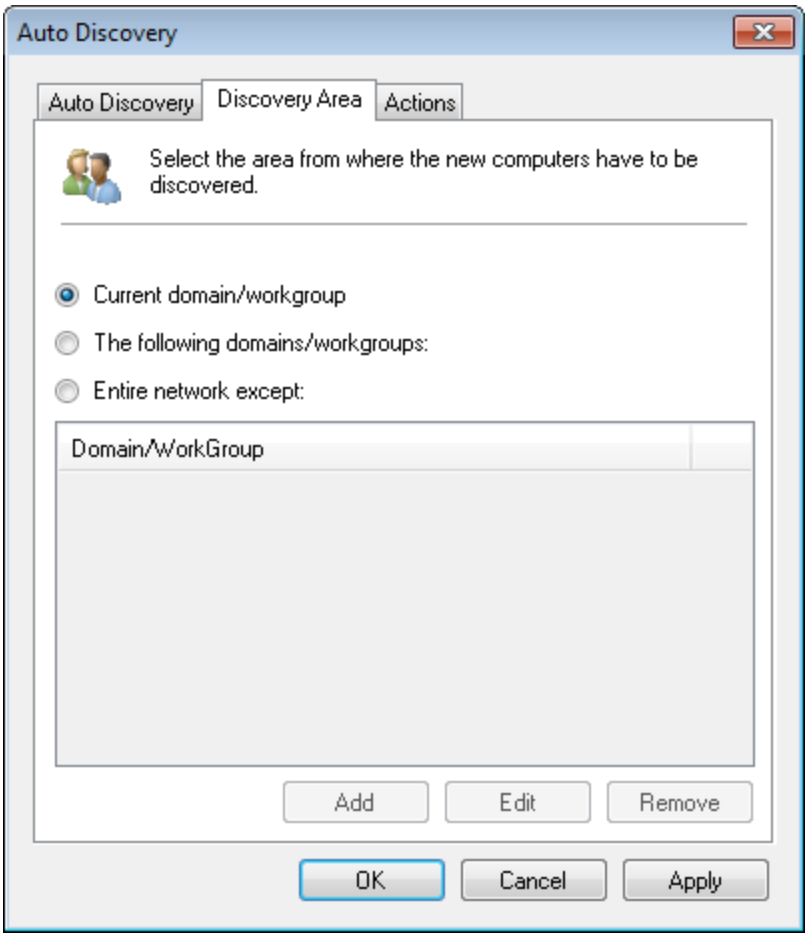
Para definir as configurações da descoberta automática:

1. Clique na guia **Configuration** > **Computers**.
2. A partir de **Common tasks**, clique em **Auto discovery settings…**



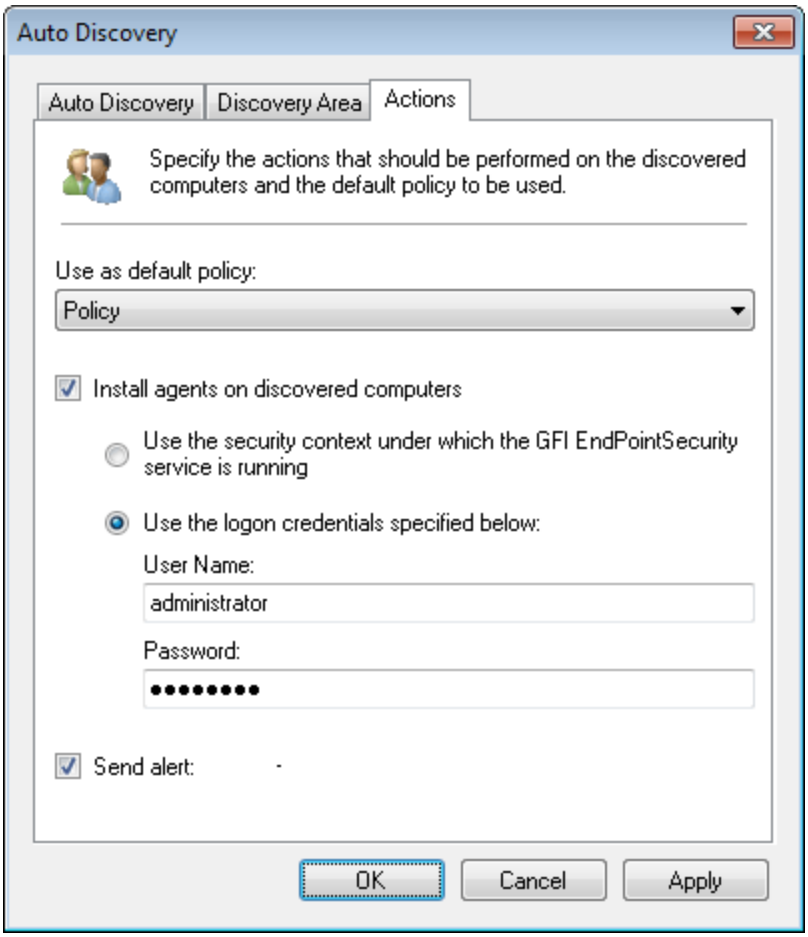
Screenshot 10: Opções de descoberta automática - Guia Auto Discovery

3. Clique em **Start discovery now** para executar a descoberta automática imediatamente.
4. Marque/desmarque **Enable automatic discovery to detect computers newly connected to the network**, para habilitar/desabilitar a descoberta automática.
5. Na seção **Schedule**, selecione a data de início e defina a frequência das pesquisas em Horária, Diária, Semanal, Mensal.



Screenshot 11: Opções da descoberta automática - Guia Discovery Area

6. Clique na guia **Discovery Area** e selecione a área a ser abrangida pela descoberta automática. Para **The following domains/workgroups** e **Entire network except**, clique em **Add** e digite no nome do domínio/grupo de trabalho.



Screenshot 12: Opções de descoberta automática - Guia Actions

7. Clique na guia **Actions** e, a partir do menu suspenso **Use as default policy**, selecione a política que deseja atribuir aos computadores descobertos recentemente.
8. Marque/desmarque **Install agents on discovered computers** para habilitar/desabilitar a implantação automática do agente. Clique em **Yes** para confirmar a habilitação da proteção automática.
9. Selecione o modo de logon que o GFI EndPointSecurity usa para efetuar logon no(s) computador (es) e implantar agentes/políticas de proteção. Por padrão, o GFI EndPointSecurity está configurado para usar as credenciais de logon da conta do usuário já com sessão iniciada a partir da qual o GFI EndPointSecurity está sendo executado.
10. Marque/desmarque **Send alert** para habilitar/desabilitar opções de alertas. Para obter mais informações, consulte Configurar opções de alertas (página 130).
11. Clique em **Apply** e em **OK**.

4.3 Configurar as credenciais de logon

O GFI EndPointSecurity exige o logon nos computadores de destino de forma a:

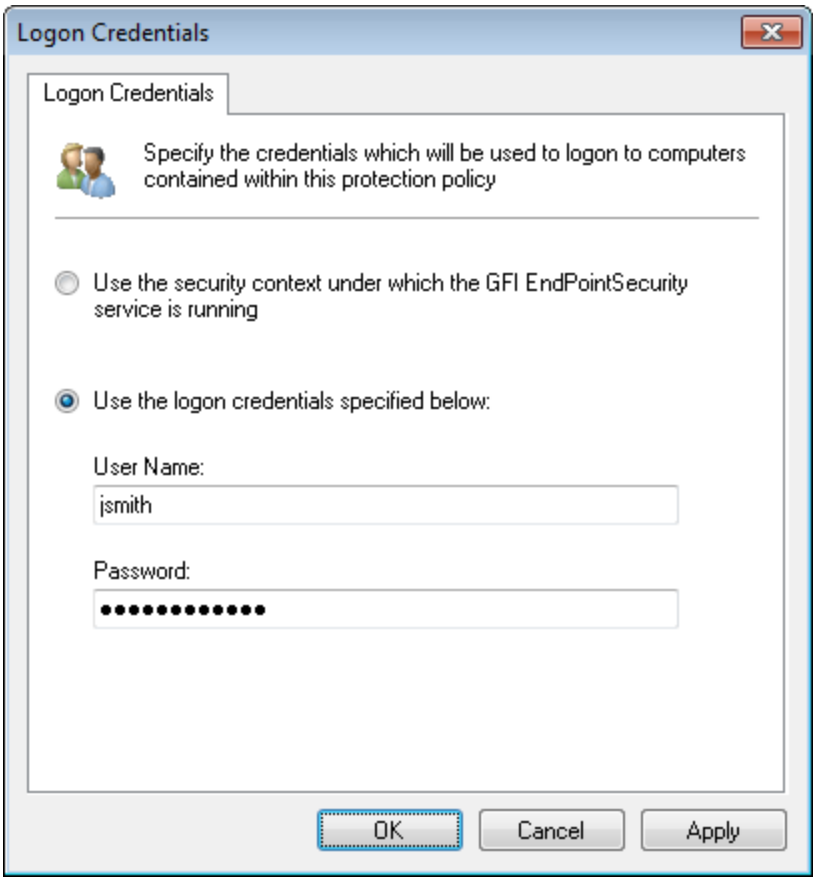
- Implantar agentes e atualizações às políticas de proteção
- Controlar o status de proteção de todos os computadores de destino.

Esta ação requer que o GFI EndPointSecurity seja executado em uma conta que possui privilégios administrativos sobre seus computadores de destino de rede (exemplo: uma conta de administrador de domínio).

Para especificar as credenciais de logon para um computador de destino:

1. Clique na guia **Configuration > Computers**.
2. Clique com o botão direito do mouse em um computador a partir da lista e clique em **Set logon credentials...**.

> **Obs.**
>
> Se desejar configurar vários computadores para o logon usando as mesmas credenciais, realce os computadores necessários, clique com o botão direito do mouse em um deles e clique em **Set logon credentials...**. Alternativamente, clique em **Set logon credentials...** a partir de **Actions**.



Screenshot 13: Opções da caixa de diálogo Logon Credentials

3. A tabela abaixo descreve as opções disponíveis de credenciais de logon:

Table 11: Opções de credenciais de logon

Opção	Descrição
Use the security context under which GFI EndPointSecurity service is running	Use as mesmas credenciais que estão executando o GFI EndPointSecurity.
Use the logon credentials specified below	Especifique credenciais alternativas para usar ao efetuar o logon em computadores de destino remoto. **Obs.** Especifique credenciais que possuem privilégios administrativos sobre destinos de verificação.

4. Clique em **Apply** e em **OK**.

> **Obs.**
>
> Por padrão, o GFI EndPointSecurity é configurado para usar as credenciais de logon da conta de usuário com a sessão iniciada no momento, executando o GFI EndPointSecurity.

5 Gerenciar políticas de proteção

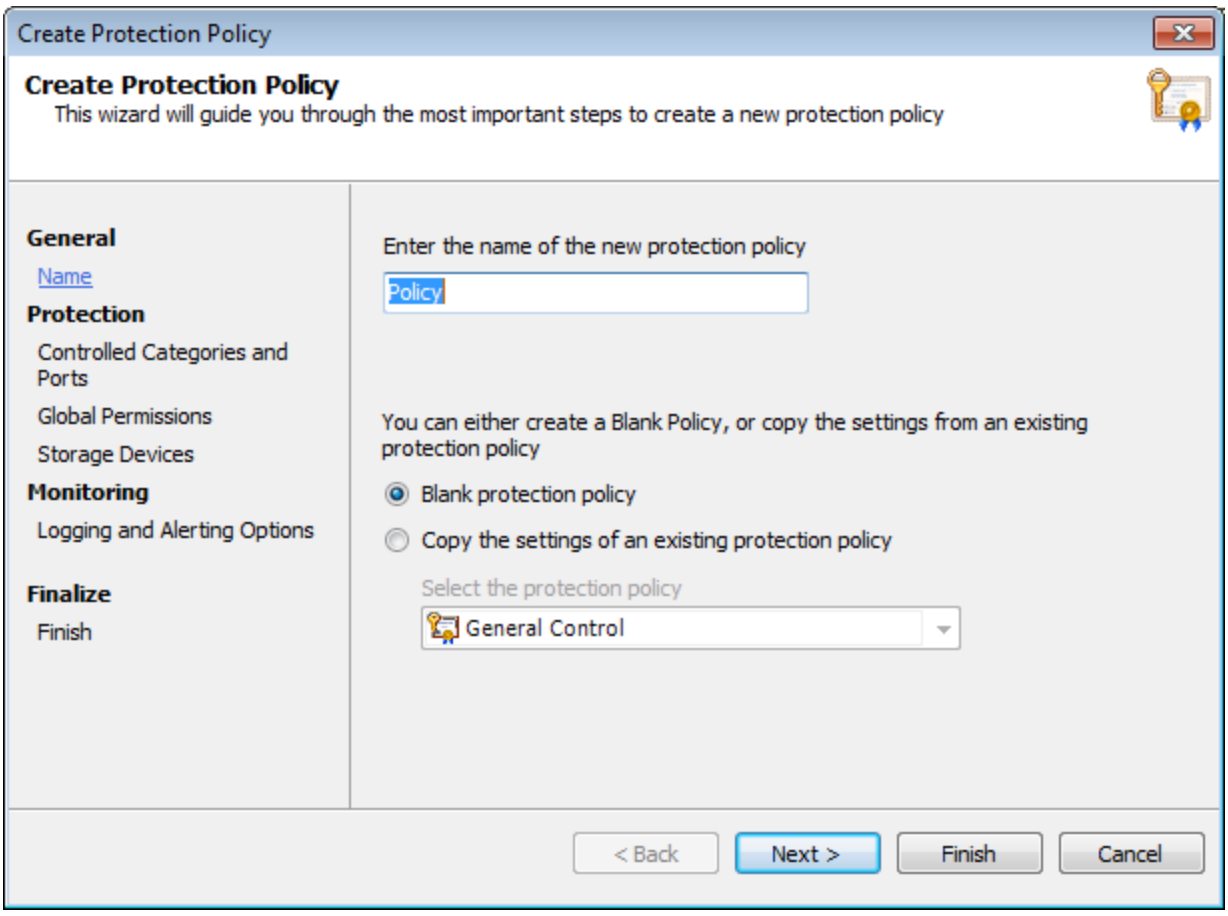
Este capítulo descreve como implantar políticas de proteção criadas recentemente e agendá-las. Antes da implantação você também poderá modificar as configurações de sua política de proteção.
Tópicos neste capítulo

5.1 Criar uma nova política de proteção

O GFI EndPointSecurity funciona com uma política de proteção padrão para que o software esteja operacional após a instalação. É possível criar mais políticas de proteção para se adequarem às políticas de segurança de acesso a dispositivos da empresa.

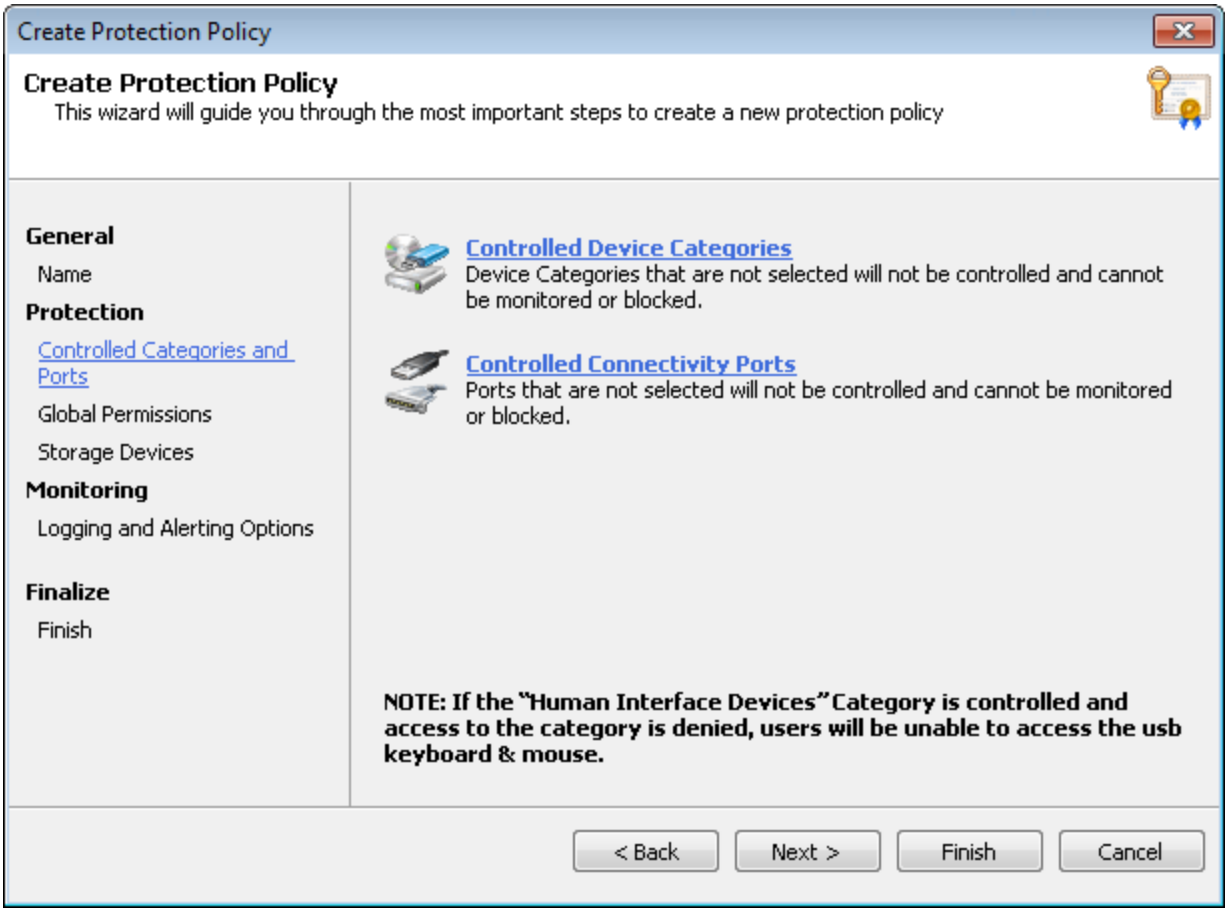
Para criar uma nova política de proteção:

1. Clique na guia **Configuration > Protection Policies**.
2. A partir de **Common tasks**, clique em **Create new protection policy…**



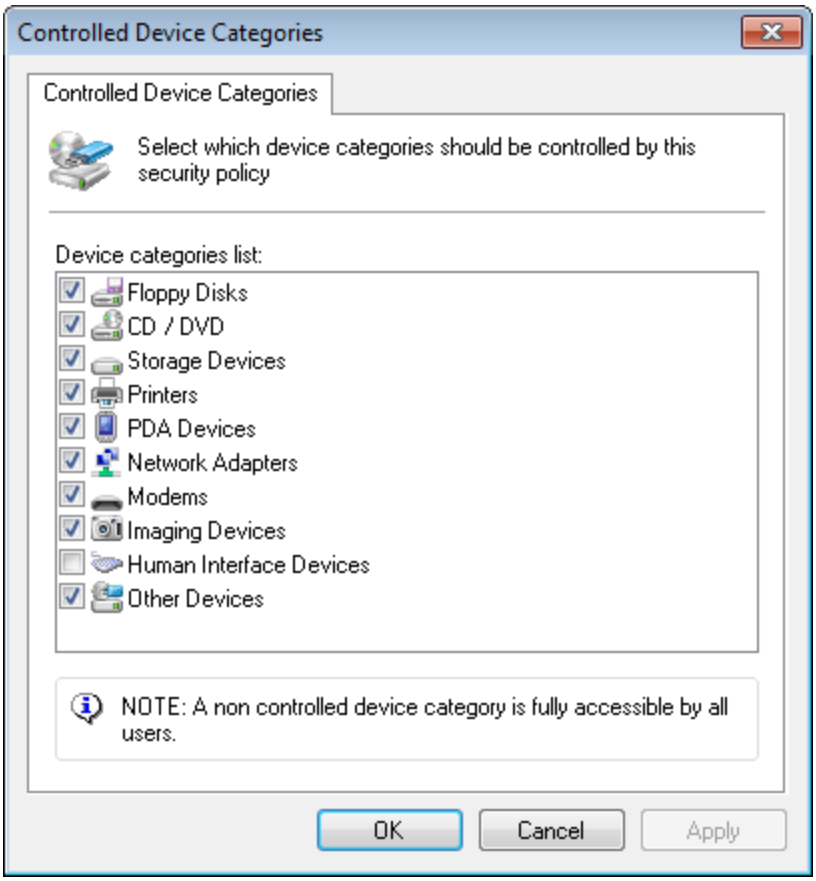
Screenshot 14: Criar uma nova política - Configurações de General

3. Digite um nome exclusivo para a nova política de proteção.
4. Selecione se deseja criar uma política em branco ou copiar as configurações de uma política já existente. Clique em **Next**. Na área de configurações, selecione a opção de herança das configurações necessária a partir de:



Screenshot 15: Criar uma nova política - Configurações de Controlled Categories and Ports

5. Clique em **Controlled Device Categories**.

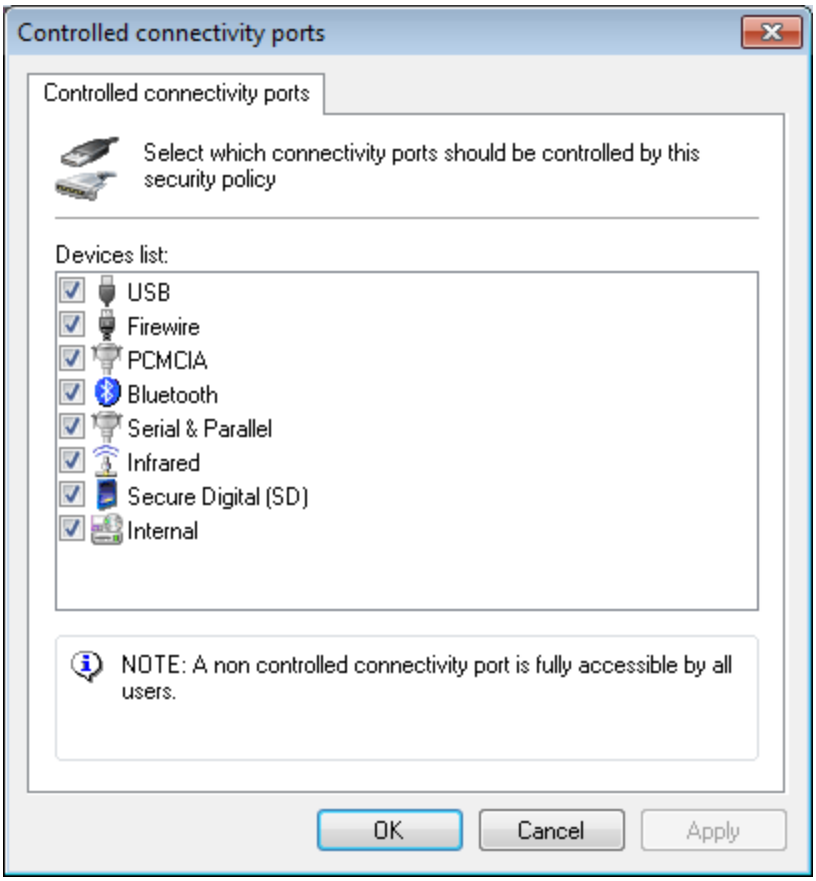


Screenshot 16: Opções de Controlled Device Categories

6. A partir da caixa de diálogo **Controlled Device Categories**, selecione as categorias necessárias do dispositivo que deseja controlar por meio desta nova política. Clique em **OK** para fechar a caixa de diálogo **Controlled Device Categories** e retornar ao assistente.

> **Importante**
>
> Se os dispositivos de interface humana estiverem habilitados e o acesso for negado, os usuários não poderão usar teclados e mouses USB conectados a computadores de destino protegidos por esta política.

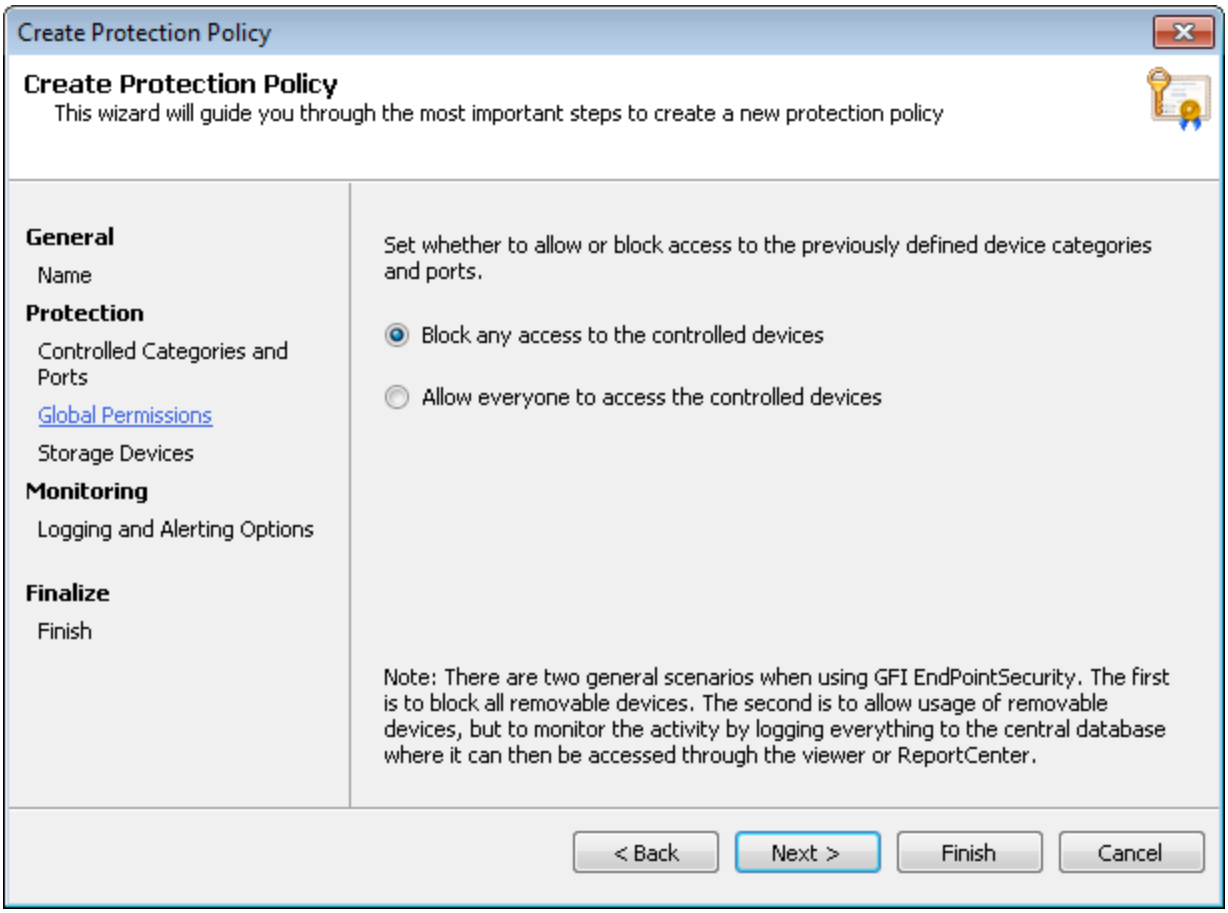
7. Clique em **Controlled Connectivity Ports**.



Screenshot 17: Opções de Controlled connectivity ports

8. A partir da caixa de diálogo **Controlled connectivity ports**, selecione as portas de conectividade necessárias que deseja controlar por meio desta nova política. Clique em **OK** para fechar a caixa de diálogo **Controlled connectivity ports** e retornar ao assistente.

9. Clique em **Next**.



Screenshot 18: Criar uma nova política - Configurações de Global Permissions

10. A partir da caixa de diálogo **Global Permissions**, selecione as permissões de acesso globais necessárias:

- **Block any access to the controlled devices** – para bloquear o acesso a todos os dispositivos/portas selecionados.
- **Allow everyone to access the controlled devices** – para permitir o acesso a todos os dispositivos/portas selecionados. Se esta opção for selecionada, o monitoramento da atividade continuará sendo realizado nos computadores de destino abrangidos pela política de proteção.

11. Clique em **Next**.

12. Clique em **File-Type Filter** e adicione os tipos de arquivos a bloquear/permitir por meio desta política.

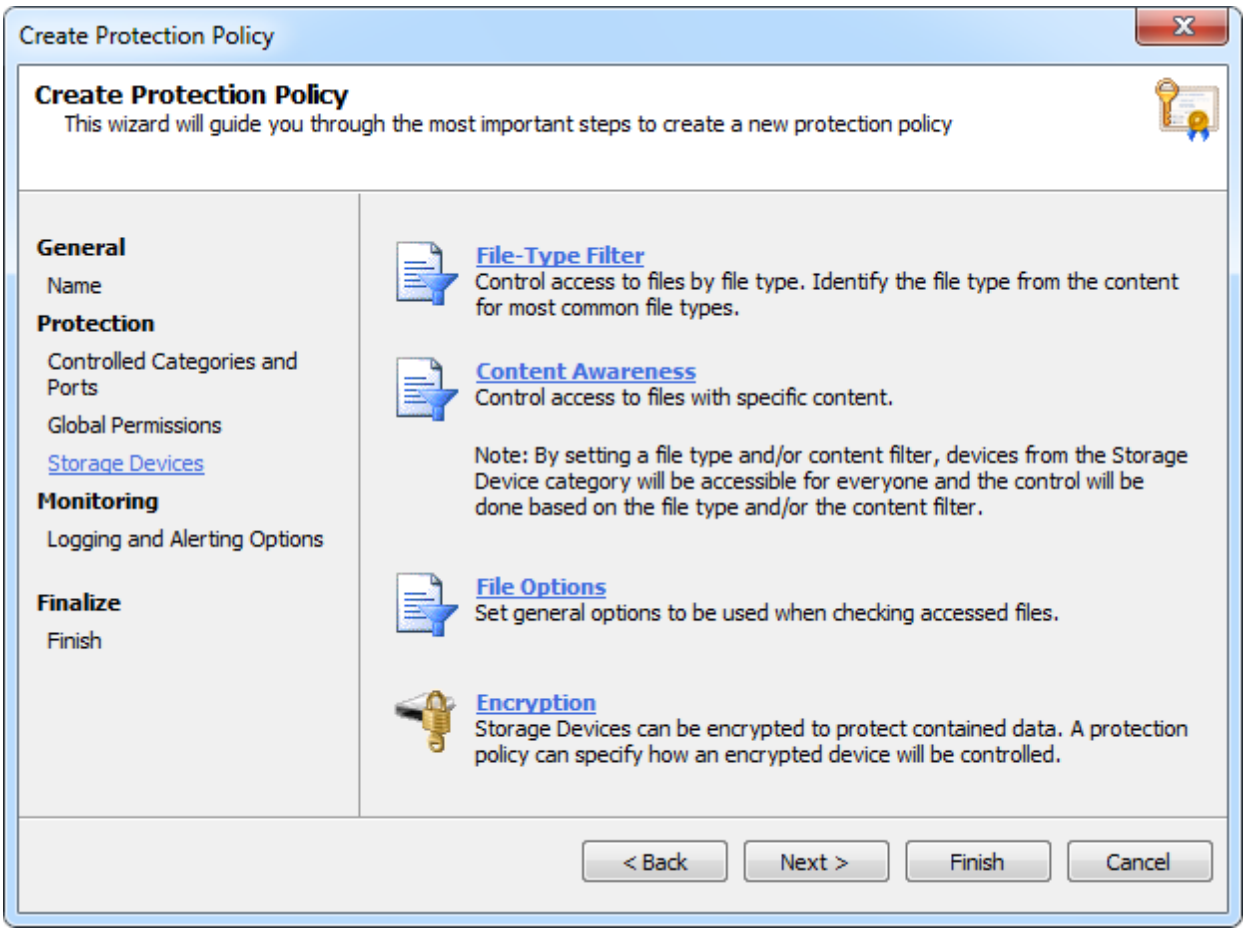
Obs.

O GFI EndPointSecurity permite restringir o acesso com base em tipos de arquivos. Possui também a capacidade de identificar o conteúdo real da maioria dos tipos de arquivos comuns (exemplo: arquivos .DOC ou .XLS) e tomar as medidas necessárias aplicáveis ao tipo de arquivo verdadeiro. Esta opção torna-se ainda mais útil quando as extensões de arquivos são manipuladas de forma mal-intencionada. Para obter mais informações, consulte Configurar filtros do tipo de arquivo (página 82).

13. Clique em **OK** para fechar a caixa de diálogo **File-Type Filter** e regressar ao assistente.
14. Clique em **Encryption** e habilite/configure o mecanismo de criptografia preferido.

> **Obs.**
>
> Além disso, o GFI EndPointSecurity pode também permitir ou bloquear os usuários e/ou grupos de usuários do Active Directory (AD) relativamente ao acesso a tipos de arquivos específicos armazenados em dispositivos que estão criptografados com o BitLocker To Go. Estas restrições são aplicadas quando os dispositivos criptografados são conectados a computadores de destino abrangidos pela política de proteção. Para obter mais informações, consulte Configurar criptografia de segurança (página 89).

15. Clique em **OK** para fechar a caixa de diálogo **Encryption** e regressar ao assistente.
16. Clique em **Next**.



17. A partir de **Storage Devices**, selecione as opções necessárias que deseja controlar a partir das guias descritas abaixo:

Table 12: Configurações da descoberta automática

Guia	Descrição
File-Type Filter	O GFI EndPointSecurity permite especificar as restrições por tipo de arquivo em arquivos, tais como .DOC ou .XLS, sendo copiados para/de dispositivos permitidos. É possível aplicar estas restrições aos usuários e/ou grupos de usuários do Active Directory (AD).

Guia	Descrição
Content Awareness	O GFI EndPointSecurity permite especificar as restrições do conteúdo do arquivo para uma política de proteção em particular. O recurso de conscientização do conteúdo verifica os arquivos que transitam os pontos de extremidade por meio de dispositivos removíveis e este identifica conteúdo baseado em expressões regulares pré-configuradas e personalizadas e em arquivos do dicionário. Por padrão, o módulo procura detalhes confidenciais seguros tais como números de previdência social e números de contas primárias, bem como informações relacionadas com empresas, tais como nomes de doenças, medicamentos, químicos perigosos e também linguagem trivial e termos étnicos/racistas. » É possível configurar o conteúdo verificando como uma política global de uma forma semelhante ao módulo de verificação de arquivos.
File Options	O GFI EndPointSecurity permite especificar as opções necessárias para bloquear ou permitir arquivos com base no tamanho. O GFI EndPointSecurity permite também ignorar arquivos de grande dimensão ao verificar o tipo e o conteúdo do arquivo, bem como os arquivos armazenados.
Encryption	O GFI EndPointSecurity permite configurar definições que se adaptam especificamente a dispositivos criptografados. Este permite também criptografar dispositivos que ainda não estejam protegidos.

Obs.

Para obter mais informações, consulte Para obter mais informações, consulte Personalizar políticas de proteção (página 58).

18. Configure as opções de logon e de alertas para esta política e clique em **Next**.

Obs.

Para obter mais informações, consulte Configurar o log de eventos e Configurar alertas.

19. Revise a página de resumo para obter informações sobre sua política e clique em **Finish**.

5.2 Atribuir uma política de proteção

A etapa seguinte é interligar o conjunto relevante de permissões de acesso ao dispositivo e da porta de conectividade a cada computador de destino. É possível fazê-lo atribuindo políticas de proteção a computadores de destino.

Obs.

Pode ser atribuída somente uma política de proteção aos computadores de destino de cada vez.

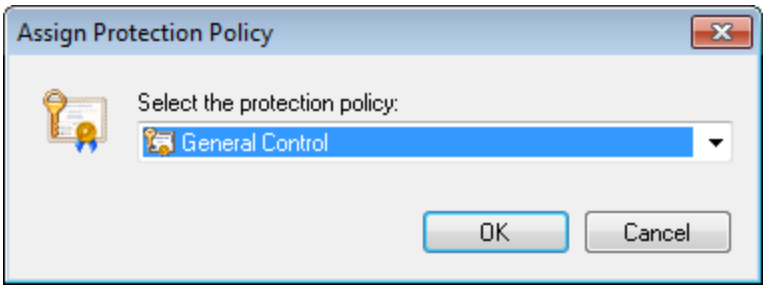
Para atribuir uma política de proteção a um computador de destino:

1. A partir do console de gerenciamento do GFI EndPointSecurity, selecione **Configuration**.
2. Clique em **Computers**.
3. Assinale o(s) computador(es) de destino necessário(s).

Obs.

Se atribuir a mesma política a mais do que um computador de destino, selecione todos os computadores de destino necessários e, em seguida, especifique a política de proteção para o conjunto selecionado de computadores de destino.

4. A partir do painel esquerdo, clique no hyperlink **Assign Protection Policy** na seção **Actions**.



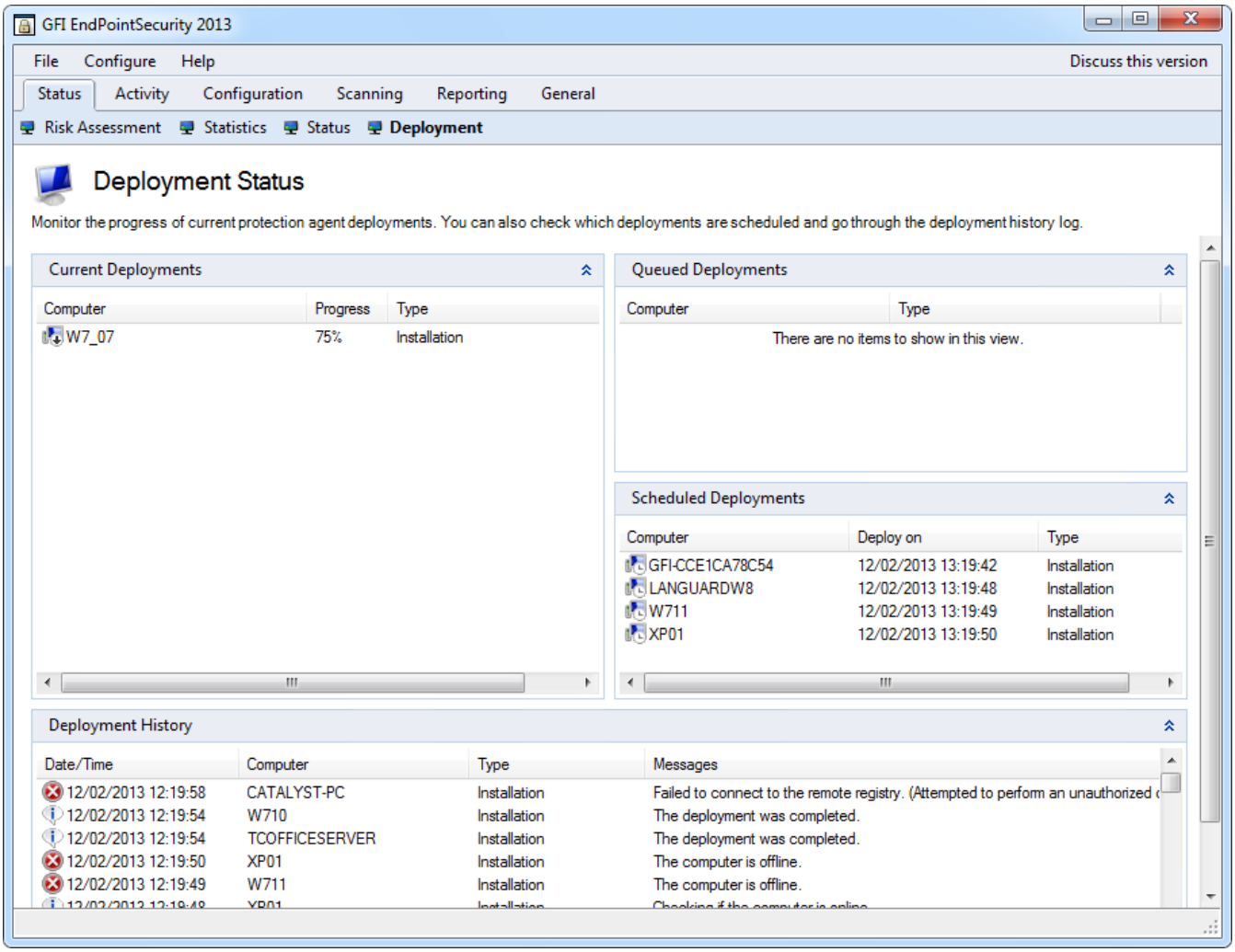
Screenshot 19: Opções de Assign Protection Policy

5. Na caixa de diálogo **Assign Protection Policy** selecione a política de proteção necessária a partir da lista suspensa e clique em **OK**.

5.2.1 Implantar imediatamente

Para implantar imediatamente uma política de proteção nos computadores de destino:

1. Clique na guia **Configuration** > subguia **Computers**.
2. Assinale o(s) computador(es) de destino necessário(s). Se for necessária mais do que uma implantação, é possível assinalar todos os computadores de destino necessários de uma vez e, em seguida, implantar as políticas de proteção no conjunto selecionado de computadores de destino.
3. A partir de **Actions**, clique em **Deploy now…**. A exibição deve mudar automaticamente para **Status > Deployment**.

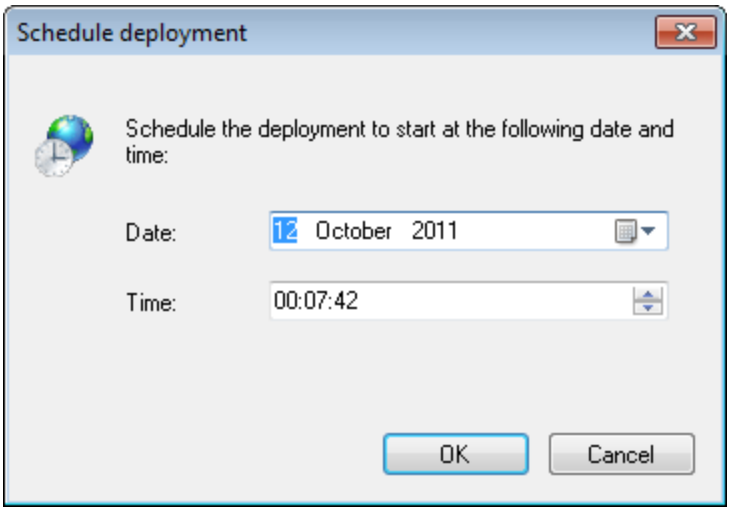


Screenshot 20: Implantar uma política imediatamente - Subguia Deployment

5.2.2 Implantação da política agendada

Para agendar a implantação de uma política de proteção:

1. Clique na guia **Configuration > Computers**.
2. Assinale o(s) computador(es) de destino necessário(s). Se for necessária mais do que uma implantação, é possível assinalar todos os computadores de destino necessários de uma vez e, em seguida, implantar as políticas no conjunto selecionado de computadores de destino.
3. A partir de **Actions**, clique em **Schedule deployment…**.



Screenshot 21: Opções de Schedule deployment

4. A partir da caixa de diálogo **Schedule deployment**, selecione a data e hora da implantação e clique em **OK**.

> **Obs.**
>
> Se o 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.

5.2.3 Implantar políticas por meio do Active Directory

É possível criar um pacote do instalador do Windows (arquivo de instalação .msi) que você pode implantar por meio das Políticas de grupo do Active Directory nos computadores de destino em seu domínio.

Para criar um pacote do instalador do Windows:

1. Clique na guia **Configuration > Protection Policies**.
2. A partir do painel esquerdo, selecione a política de proteção para a qual deseja criar o pacote do instalador do Windows.
3. A partir do painel direito, clique em **Deploy through Active Directory** na seção **Deployment**.
4. Digite o **File name** do arquivo .msi e navegue para selecionar o caminho de destino.
5. Clique em **Save**.

> **Obs.**
>
> Para obter informações sobre como implantar software usando as Políticas de grupo do Active Directory no Microsoft Windows Server 2003 e no Microsoft Windows Server 2008, consulte http://support.microsoft.com/kb/816102.

5.3 Verificar a implantação de políticas de proteção

Assim que uma política de proteção seja implantada, recomenda-se que se verifique se os computadores de destino ficaram afetados pela política. Verifique se a implantação foi bem-sucedida

a partir de:

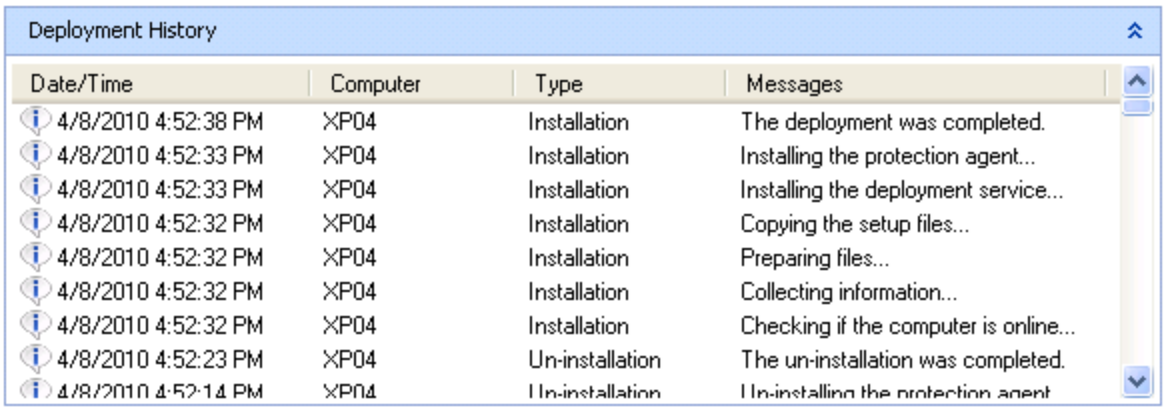
- Área de histórico de implantação
- Área do status dos agentes

5.3.1 Histórico de implantações

Use as informações exibidas na área Deployment History para determinar se a implantação para cada computador de destino foi concluída com êxito ou se foram encontrados erros.

Para exibir o histórico de implantações:

1. Clique em **Status> Deployment**.



Screenshot 22: Área Deployment History

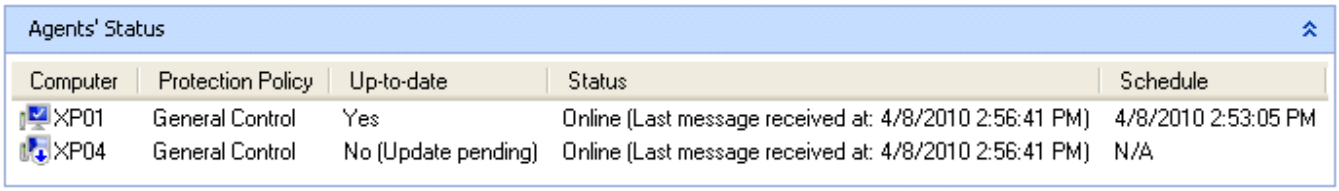
2. A partir de **Deployment History**, confirme se a conclusão da atualização no computador local foi bem-sucedida. Para obter mais informações, consulte Vista do status de implantação (página 120).

5.3.2 Status dos agentes

Use as informações exibidas na área Agents' Status para determinar o status de todas as operações de implantação realizadas em seus computadores de destino de rede.

Para visualizar os status dos agentes:

3. Clique em **Status> Agents**.



Screenshot 23: Área de Agents' Status

4. A partir de **Agents' Status**, confirme a atribuição com êxito da política de proteção correta para o (s) computador(es) de destino e se essa implantação do agente se encontra atualizada.

> **Obs.**
>
> Cada agente envia o seu status online para a instalação do GFI EndPointSecurity principal em intervalos regulares. Se estes dados não forem recebidos pela instalação principal, o agente é considerado offline.

Obs.

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.

Para obter mais informações sobre a área de status dos agentes, consulte a seção Vista do status dos agentes no capítulo Monitorar status.

6 Personalizar políticas de proteção

Este capítulo fornece informações relacionadas com a modificação das configurações de suas políticas de proteção pré-configuradas. Isto permite ajustar as configurações por tempo, uma vez que vai descobrindo novos obstáculos à segurança e possíveis vulnerabilidades.

Tópicos neste capítulo

6.1 Configurar categorias de dispositivos controladas

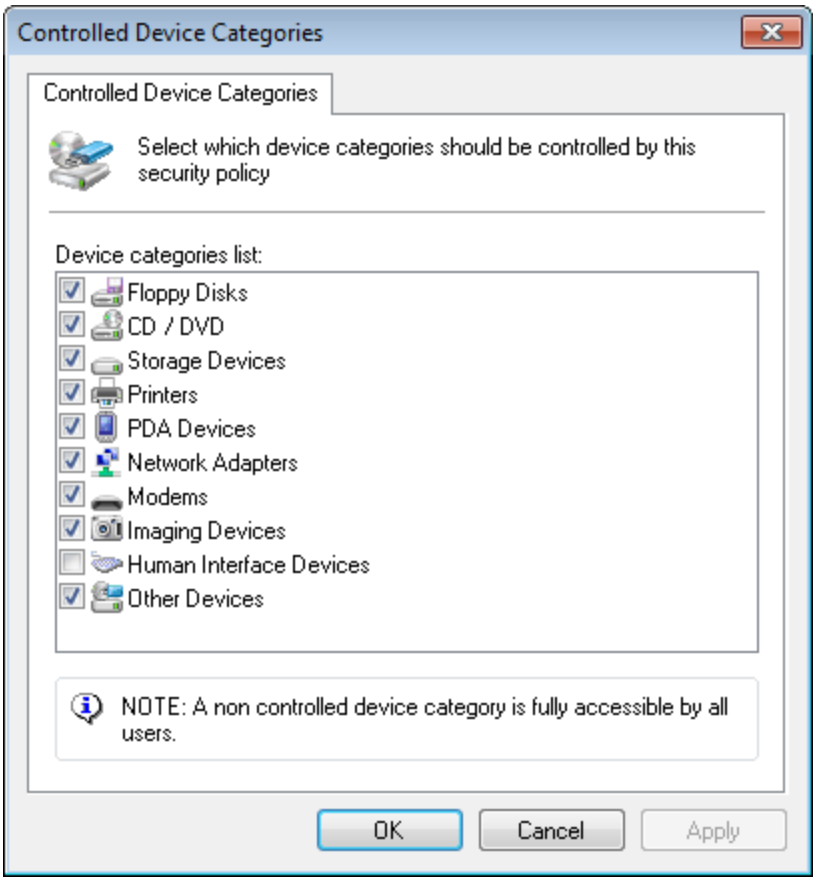
O GFI EndPointSecurity permite selecionar quais as categorias de dispositivos suportadas que devem ser controladas ou não pela política de proteção. É possível fazê-lo em uma base de política por política.

Obs.

Os dispositivos não especificados serão totalmente acessíveis a partir dos computadores de destino abrangidos pela política de proteção. Como resultado, o GFI EndPointSecurity não pode monitorar e bloquear dispositivos que pertençam a uma categoria que não seja controlada pela política de proteção.

Para configurar dispositivos controlados por uma política de proteção:

1. Clique na guia **Configuration > Protection Policies**.
2. Em **Protection Policies > Security**, selecione a política de proteção a configurar.
3. Clique em **Security**.
4. A partir de **Common tasks**, clique em **Edit controlled device categories…**.



Screenshot 24: Opções de Controlled Device Categories

5. Na caixa de diálogo **Controlled Device Categories** marque/desmarque as categorias de dispositivo necessárias que serão controladas pela política de proteção e clique em **OK**.

Importante

Se habilitar Human Interface Devices e negar o acesso a esses dispositivos, os usuários não poderão usar os teclados e mouses USB conectados a computadores de destino protegidos por esta política.

Para implantar atualizações de políticas de proteção em computadores de destino especificados na política:

1. Clique na guia **Configuration** > **Computers**.
2. A partir de **Common tasks**, clique em **Deploy to all computers**….

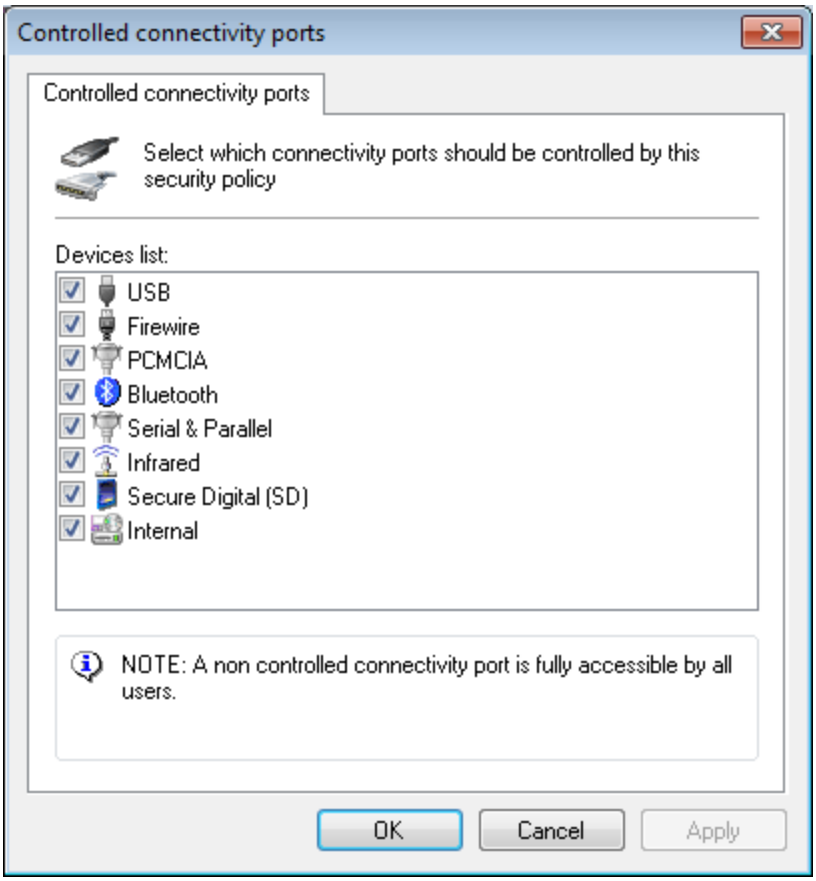
6.2 Configurar portas de conectividade controladas

O GFI EndPointSecurity permite selecionar quais as portas de conectividade suportadas que devem ser controladas ou não pela política de proteção. É possível fazê-lo em uma base de política por política.

> **Obs.**
>
> As portas não especificadas serão totalmente acessíveis a partir dos computadores de destino abrangidos pela política de proteção. Como resultado, o GFI EndPointSecurity não pode monitorar e bloquear dispositivos conectados a uma porta que não seja controlada pela política de proteção.

Para configurar quais as portas que serão controladas por uma política de proteção específica:

1. Clique na guia **Configuration > Protection Policies**.
2. Em **Protection Policies > Security**, selecione a política de proteção a configurar.
3. Clique em **Security**.
4. A partir de **Common tasks**, clique em **Edit controlled ports**….



Screenshot 25: Opções de Controlled connectivity ports

5. A partir da caixa de diálogo **Controlled connectivity ports**, marque/desmarque as portas de conectividade necessárias que serão controladas pela política de proteção e clique em **OK**.

Para implantar atualizações de políticas de proteção em computadores de destino especificados na política:

1. Clique na guia **Configuration** > **Computers**.
2. A partir de **Common tasks**, clique em **Deploy to all computers…**.

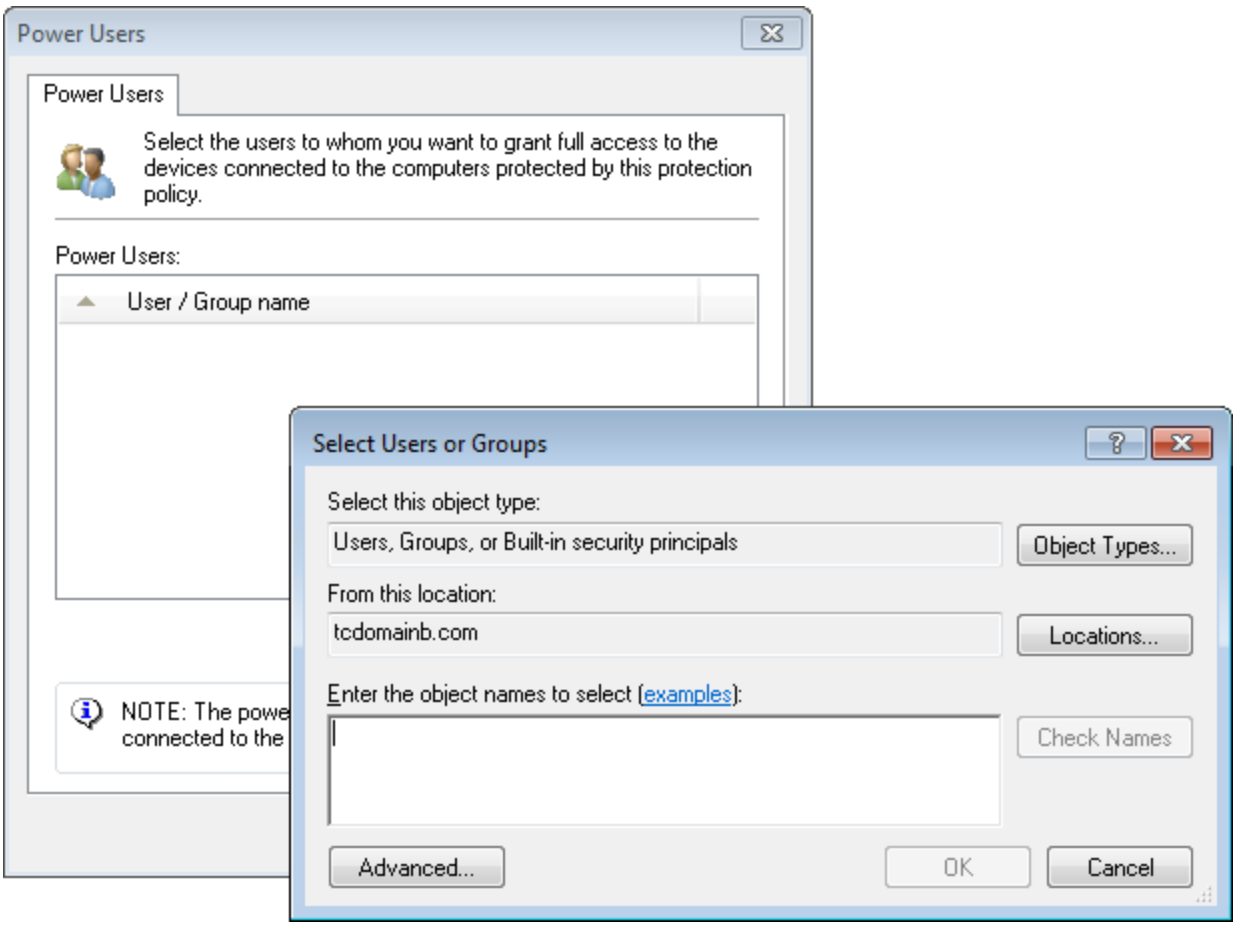
6.3 Configurar usuários avançados

O GFI EndPointSecurity permite especificar usuários e/ou grupos de usuários do Active Directory (AD) como usuários avançados. É automaticamente fornecido aos usuários avançados acesso completo a dispositivos conectados a qualquer computador de destino abrangido por uma política de proteção. É possível definir conjuntos de usuários avançados em uma base de política por política.

É necessário ter cuidado ao usar este recurso, uma vez que especificar incorretamente um usuário como um usuário avançado fará com que esse usuário substitua todas as restrições da política de proteção relevante.

Para especificar os usuários avançados de uma política de proteção:

1. Clique na guia **Configuration > Protection Policies**.
2. Em **Protection Policies > Security**, selecione a política de proteção a configurar.
3. A partir do painel direito, clique em **Power users** na seção **Security**.



Screenshot 26: Opções de usuários avançados

4. Na caixa de diálogo Power Users:

- **Opção 1**: Clique em **Add…** para especificar o(s) usuário(s)/grupo(s) que será(ão) designado(s) como usuário(s) avançado(s) para esta política de proteção e clique em **OK**.
- **Opção 2**: Assinale o(s) usuário(s)/grupo(s) e clique em **Remove** para diminuir níveis dos usuários avançados e clique em **OK**.

Para implantar atualizações de políticas de proteção em computadores de destino especificados na política:

1. Clique na guia **Configuration** > **Computers**.
2. A partir de **Common tasks**, clique em **Deploy to all computers…**.

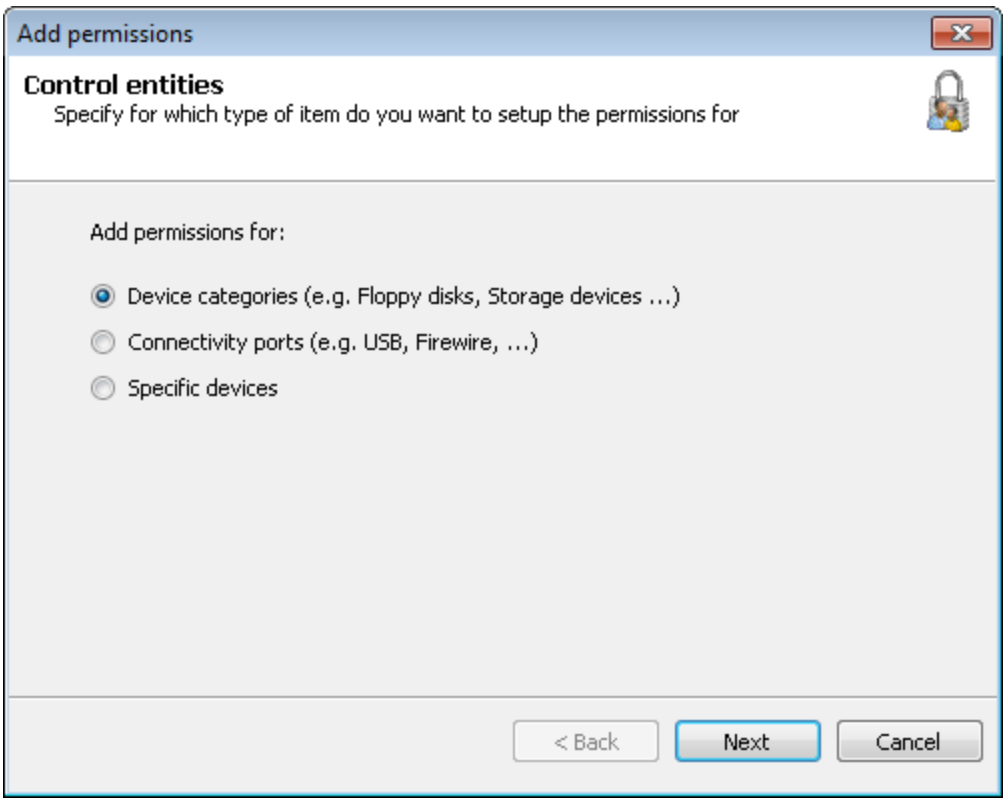
6.4 Configurar permissões de acesso para categorias de dispositivos

O GFI EndPointSecurity permite definir permissões por categorias de dispositivo para os usuários e/ou grupos de usuários do Active Directory (AD). É possível fazê-lo em uma base de política por política.

Quando uma categoria de dispositivo não está definida para ser controlada por uma política de segurança em particular, a entrada relevante é desabilitada. Para obter mais informações, consulte Configurar categorias de dispositivos controladas (página 58).

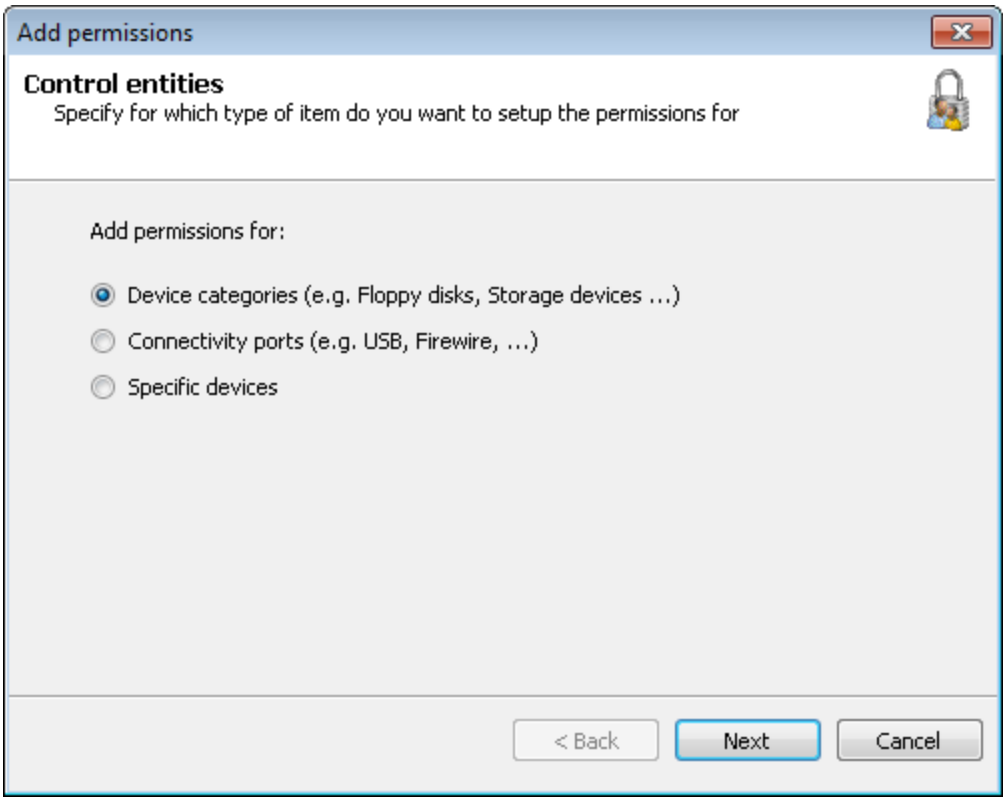
Para configurar as permissões de acesso a categorias de dispositivo para usuários em uma política de proteção:

1. Clique na guia **Configuration > Protection Policies**.
2. Em **Protection Policies > Security**, selecione a política de proteção a configurar.
3. A partir de **Common tasks**, clique em **Add permission(s)…**.



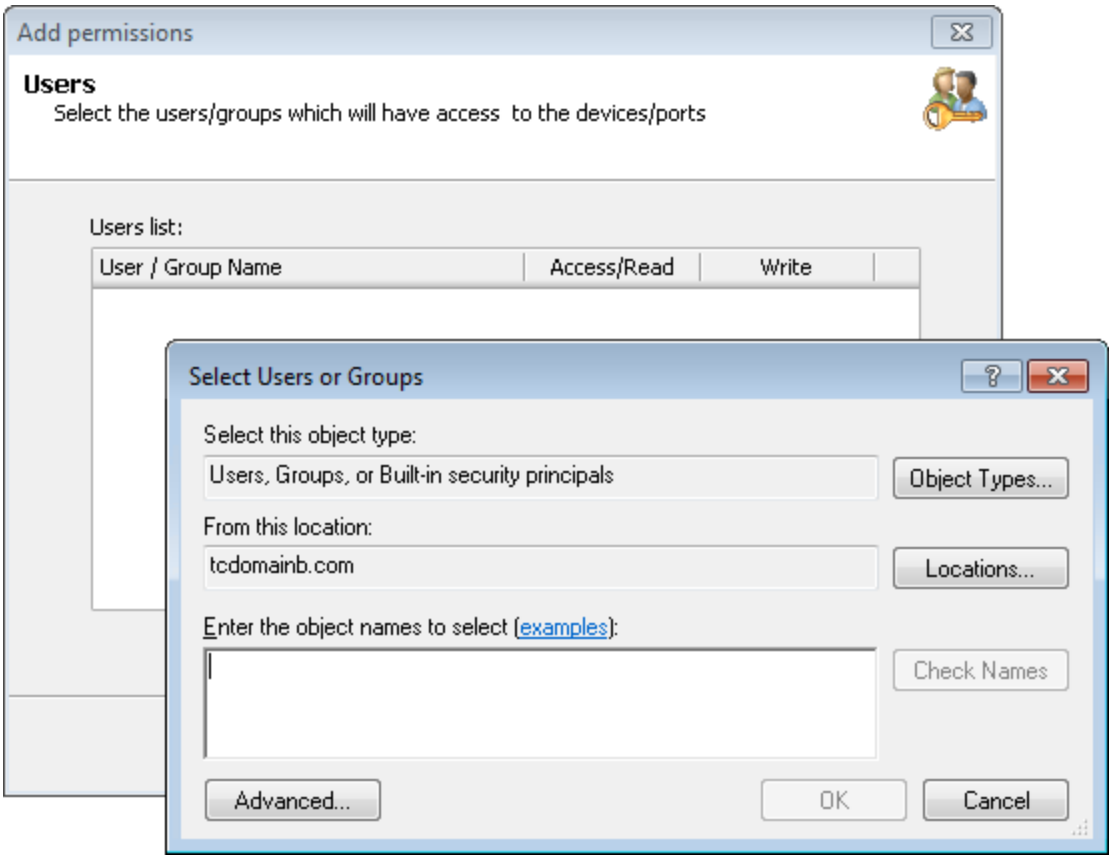
Screenshot 27: Opções de Add permissions - Control entities

4. Na caixa de diálogo **Add permissions**, selecione **Device categories** e clique em **Next**.



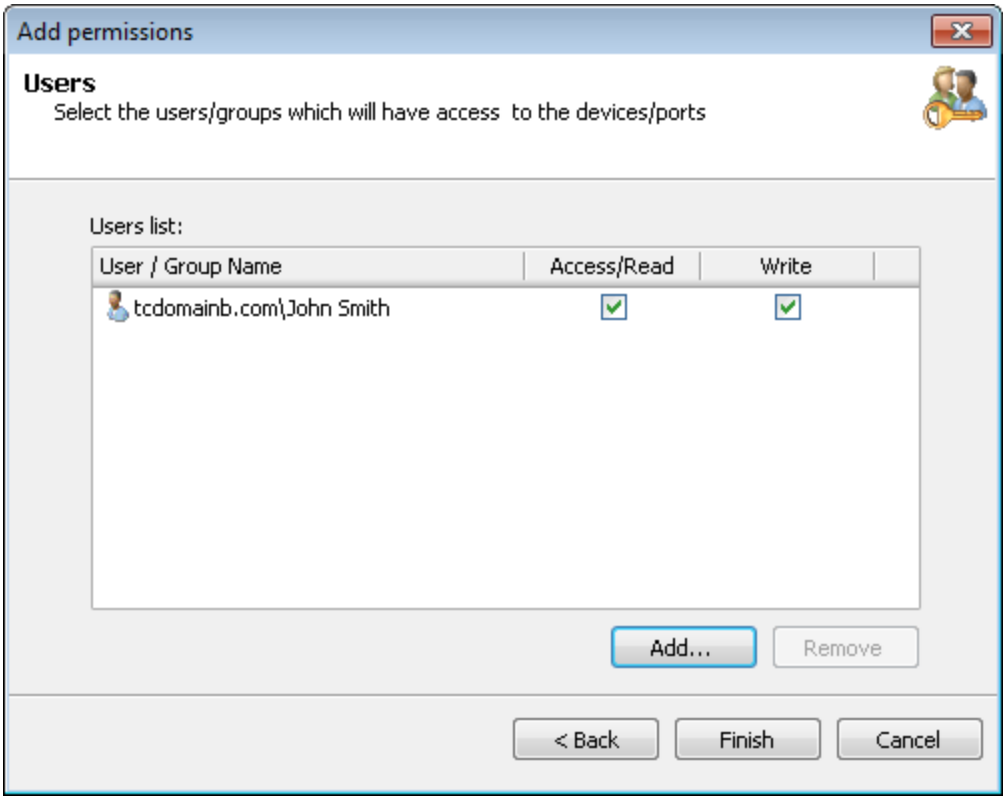
Screenshot 28: Opções de Add permissions - Device categories

5. Habilite ou desabilite as categorias do dispositivo necessárias para as quais deseja configurar permissões e clique em **Next**.



Screenshot 29: Opções de Add permissions - Users

6. Clique em **Add…** para especificar o(s) usuário(s)/grupo(s) que terá(ão) acesso às categorias do dispositivo especificadas nesta política de proteção e clique em **OK**.



Screenshot 30: Opções de Add permissions - Users

7. Habilite ou desabilite as permissões de Access/Read e Write para cada usuário/grupo que especificou e clique em **Finish**.

Para implantar atualizações de políticas de proteção em computadores de destino especificados na política:

1. Clique na guia **Configuration** > **Computers**.
2. A partir de **Common tasks**, clique em **Deploy to all computers…**.

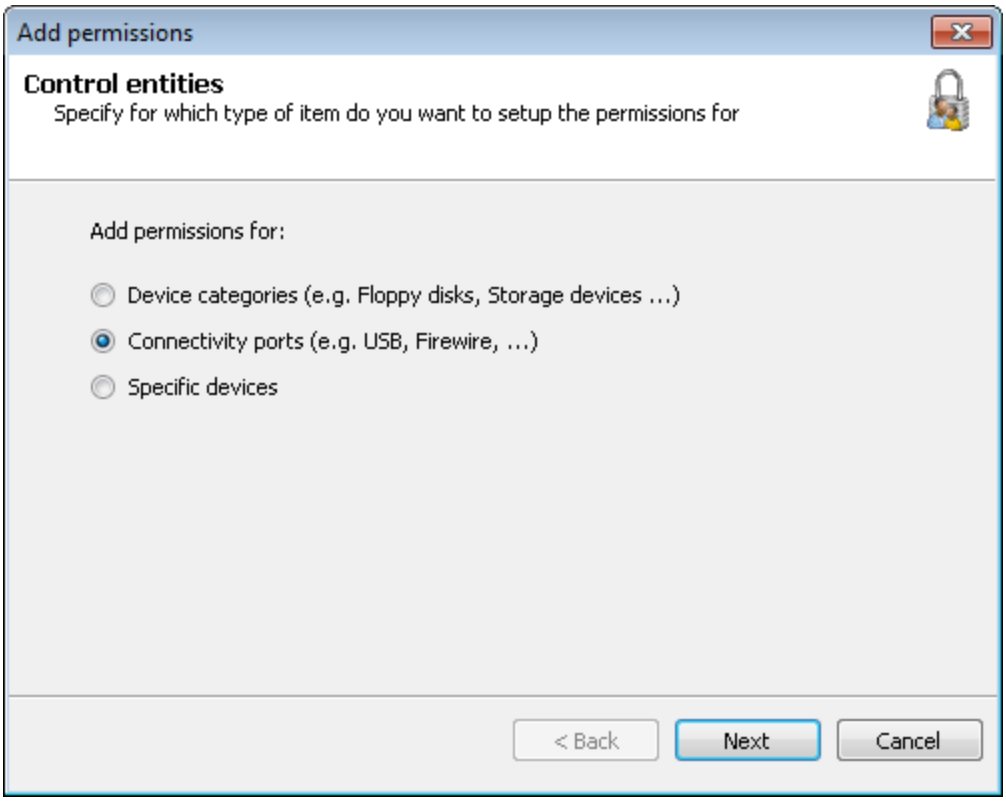
6.5 Configurar permissões de acesso para portas de conectividade

O GFI EndPointSecurity fornece a possibilidade de definir permissões por portas de conectividade para os usuários e/ou grupos de usuários do Active Directory (AD). É possível fazê-lo em uma base de política por política.

Quando uma porta de conectividade não é definida para ser controlada por uma política de proteção, a permissão relevante é desabilitada. Para obter mais informações, consulte Configurar portas de conectividade controladas (página 60).

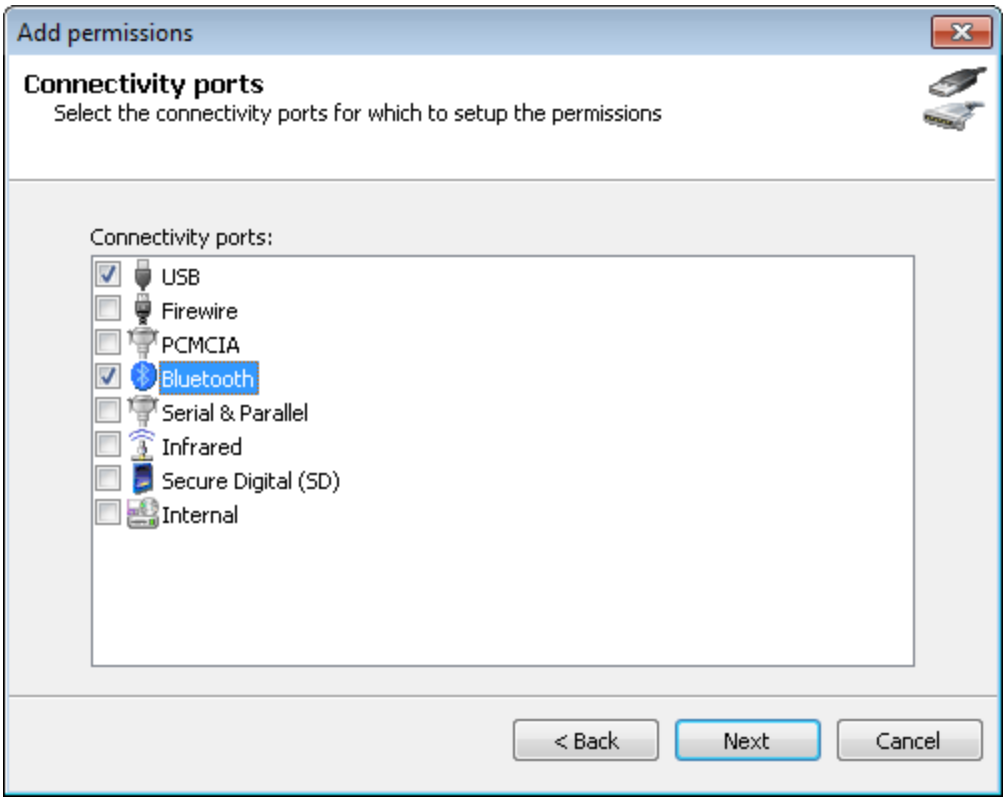
Para configurar as permissões de uso da porta de conectividade para usuários abrangidos por uma determinada política de proteção:

1. Clique na guia **Configuration > Protection Policies**.
2. Em **Protection Policies > Security**, selecione a política de proteção a configurar.
3. Clique em **Security** > **Set Permissions**.
4. A partir de **Common tasks**, clique em **Add permission(s)…**.



Screenshot 31: Opções de Add permissions - Control entities

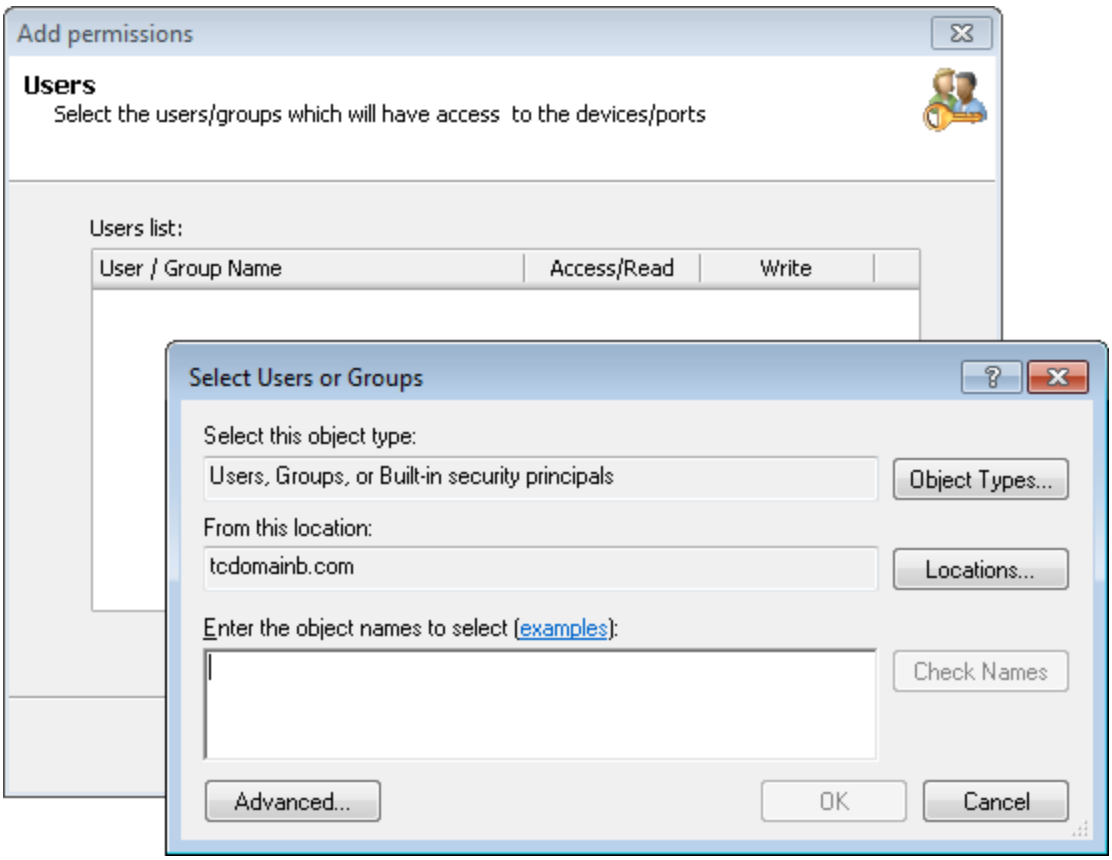
5. Na caixa de diálogo **Add permissions** selecione **Connectivity ports** e clique em **Next**.



Screenshot 32: Opções de Add permissions - Connectivity ports

6. Habilite ou desabilite as portas de conectividade necessárias para as quais deseja configurar permissões e clique em **Next**.

7. Clique em **Add...** para especificar o(s) usuário(s)/grupo(s) que terá(ão) acesso às portas de conectividade especificadas nesta política de proteção e clique em **OK**.



Screenshot 33: Opções de Add permissions - Users

8. Habilite ou desabilite as permissões de Access/Read para cada usuário/grupo que especificou e clique em **Finish**.

Para implantar atualizações de políticas de proteção em computadores de destino especificados na política:

1. Clique na guia **Configuration** > **Computers**.
2. A partir de **Common tasks**, clique em **Deploy to all computers...**.

6.6 Configurar permissões de acesso para dispositivos específicos

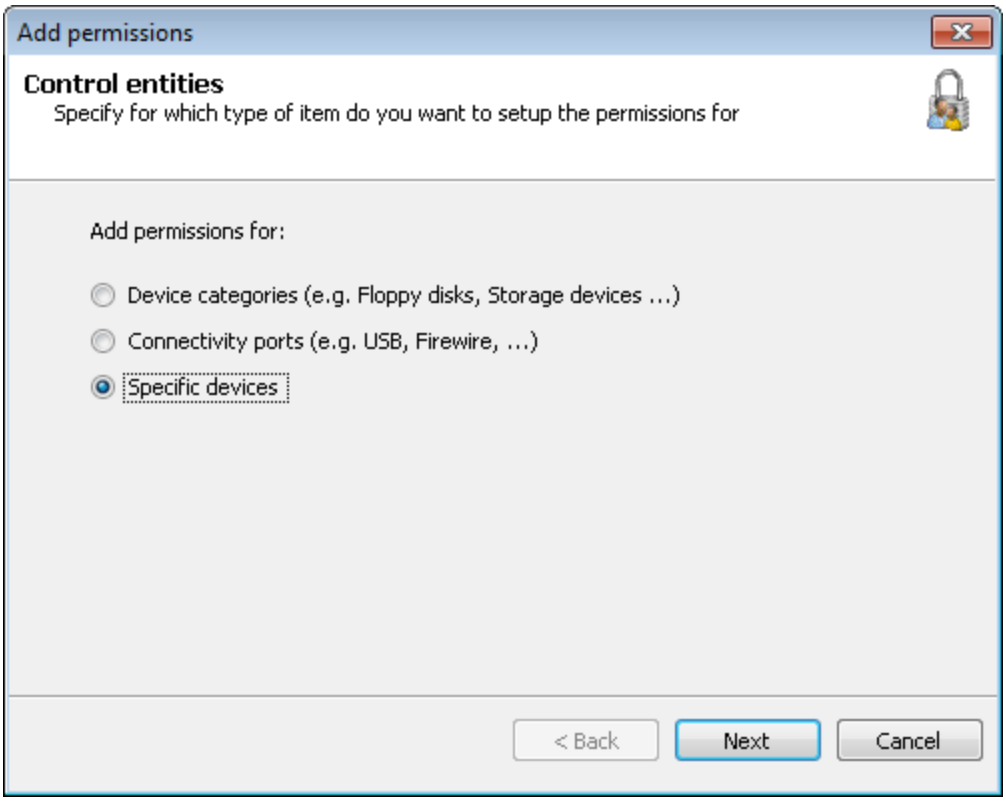
O GFI EndPointSecurity permite definir permissões por dispositivos específicos para os usuários e/ou grupos de usuários do Active Directory (AD). É possível fazê-lo em uma base de política por política.

Por exemplo, é possível atribuir permissões somente de leitura a uma pen drive USB aprovada de uma empresa específica. As tentativas para usar outras pen drives USB não aprovas serão bloqueadas.

> **Obs.**
>
> Para uma lista atualizada de dispositivos conectados no momento aos computadores de destino, execute uma verificação do dispositivo e adicione os dispositivos descobertos ao banco de dados de dispositivos antes de configurar as permissões de acesso para dispositivos específicos. Para obter mais informações, consulte Descobrir dispositivos (página 101).

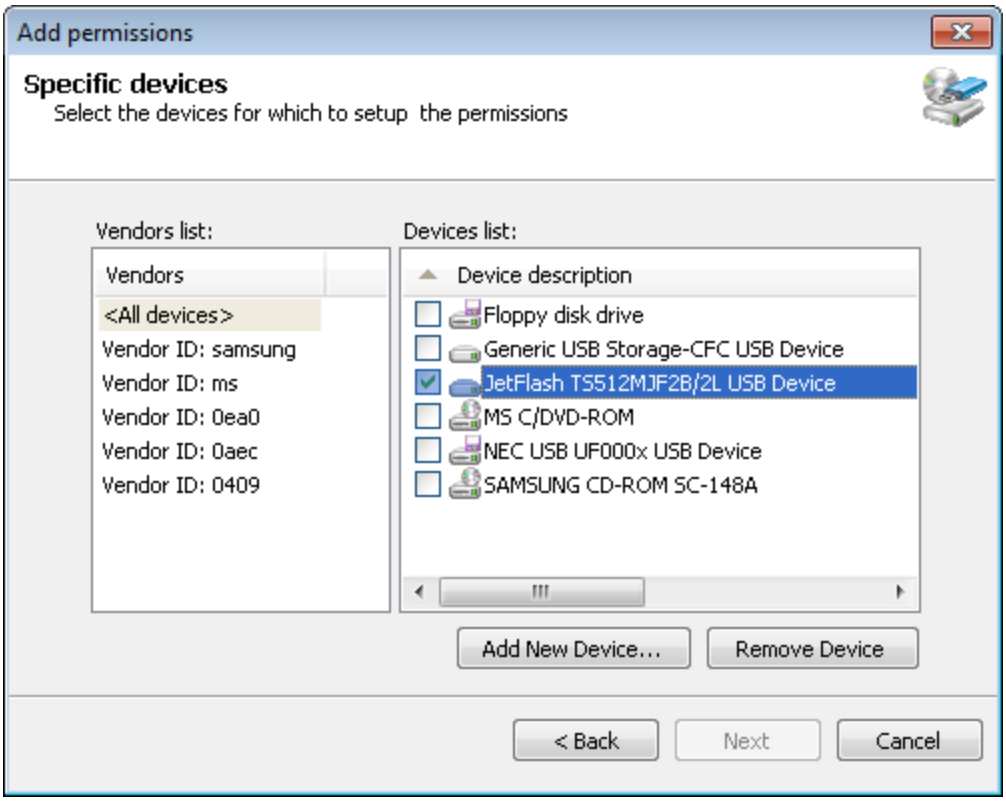
Para configurar as permissões de acesso a dispositivos específicos para usuários em uma política de proteção:

1. Clique na guia **Configuration > Protection Policies**.
2. Em **Protection Policies > Security**, selecione a política de proteção a configurar.
3. Clique no subnó **Security**.
4. A partir do painel esquerdo, clique em **Add permission(s)...** na seção **Common tasks**.



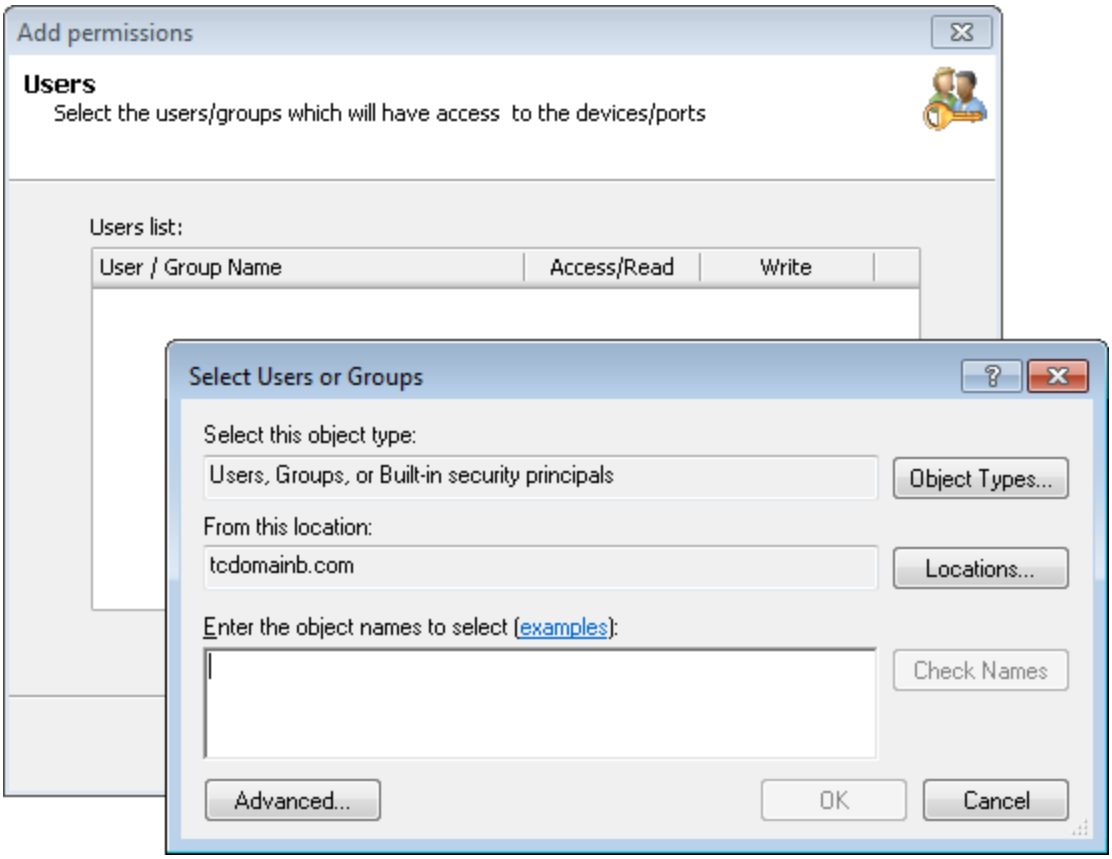
Screenshot 34: Opções de Add permissions - Control entities

5. Na caixa de diálogo **Add permissions**, selecione **Specific devices** e clique em **Next**.



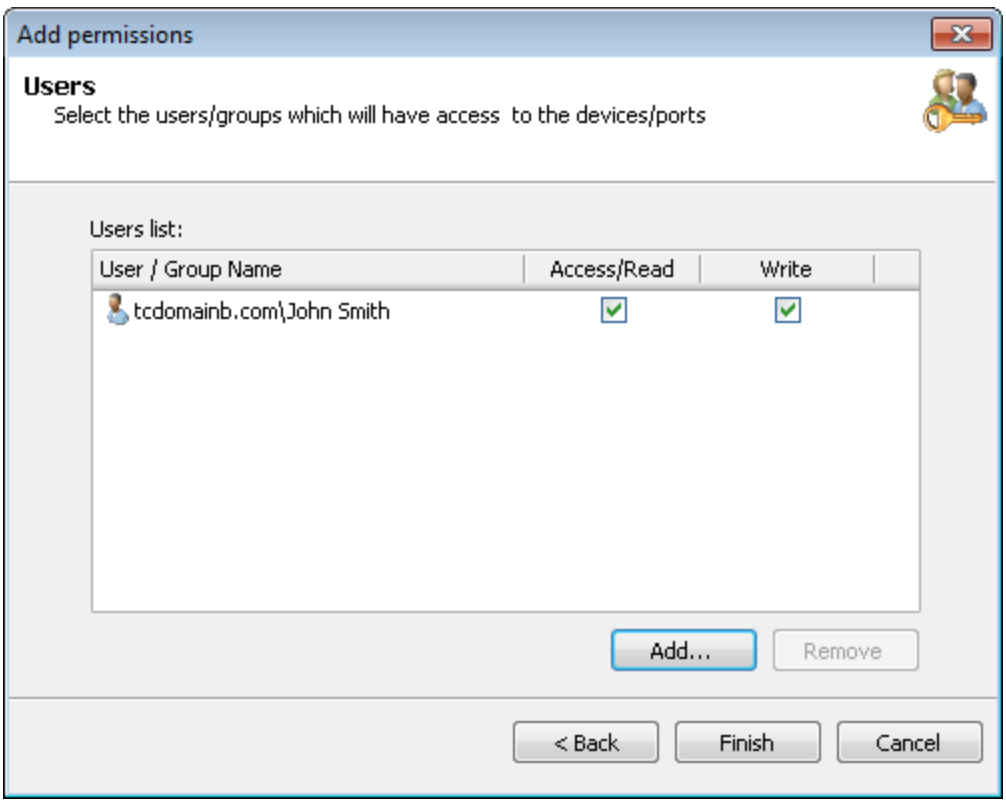
Screenshot 35: Opções de Add permissions - Specific devices

6. Habilite ou desabilite os dispositivos necessários a partir da lista Devices, para os quais deseja configurar permissões e clique em **Next**. Se um dispositivo necessário não se encontrar na lista, clique em **Add New Device**... para especificar os detalhes do dispositivo para o qual deseja configurar permissões e clique em **OK**.



Screenshot 36: Opções de Add permissions - Users

7. Clique em **Add...** para especificar o(s) usuário(s)/grupo(s) que terá(ão) acesso aos dispositivos específicos, especificados nesta política de proteção e clique em **OK**.



Screenshot 37: Opções de Add permissions - Users

8. Habilite ou desabilite as permissões de Access/Read e Write para cada usuário/grupo que especificou e clique em **Finish**.

Para implantar atualizações de políticas de proteção em computadores de destino especificados na política:

1. Clique na guia **Configuration** > **Computers**.
2. A partir de **Common tasks**, clique em **Deploy to all computers...**.

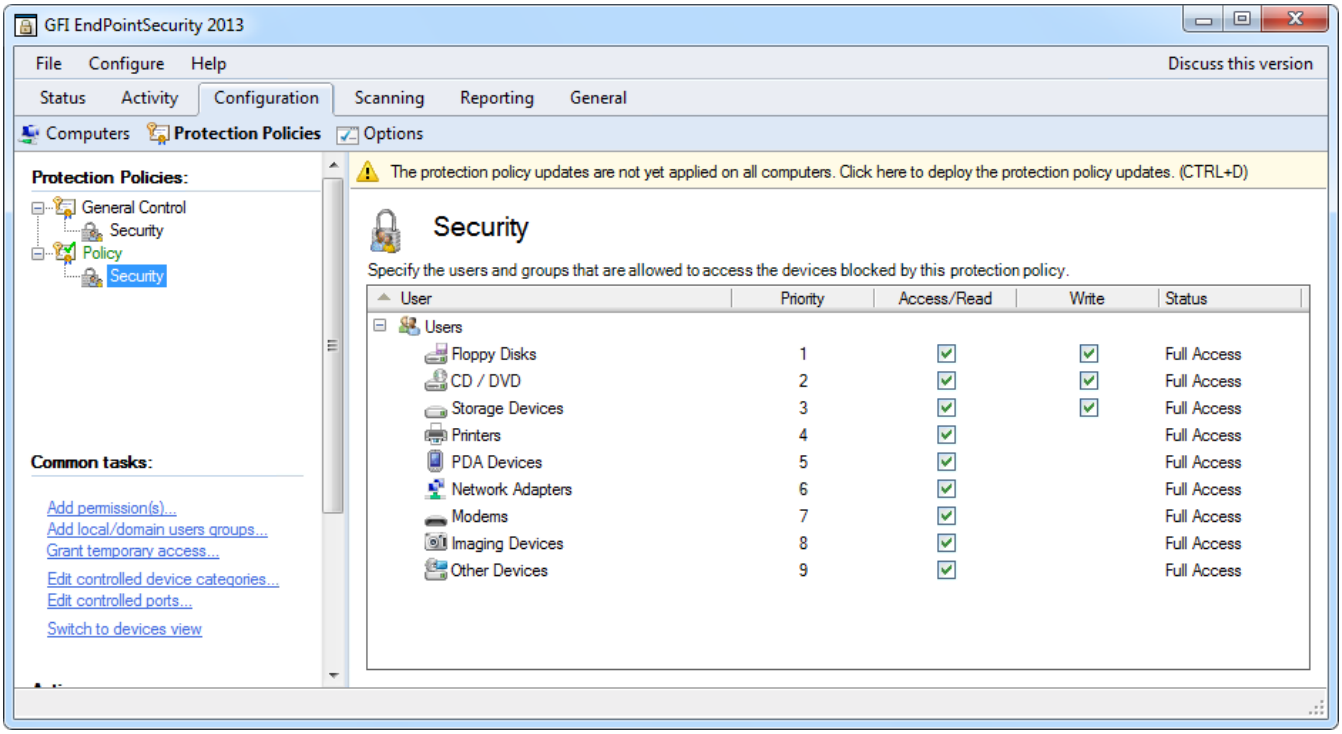
6.7 Ver permissões de acesso

O GFI EndPointSecurity permite ver todas as permissões atribuídas aos usuários e/ou grupos de usuários do Active Directory (AD). É possível fazê-lo em uma base de política por política.

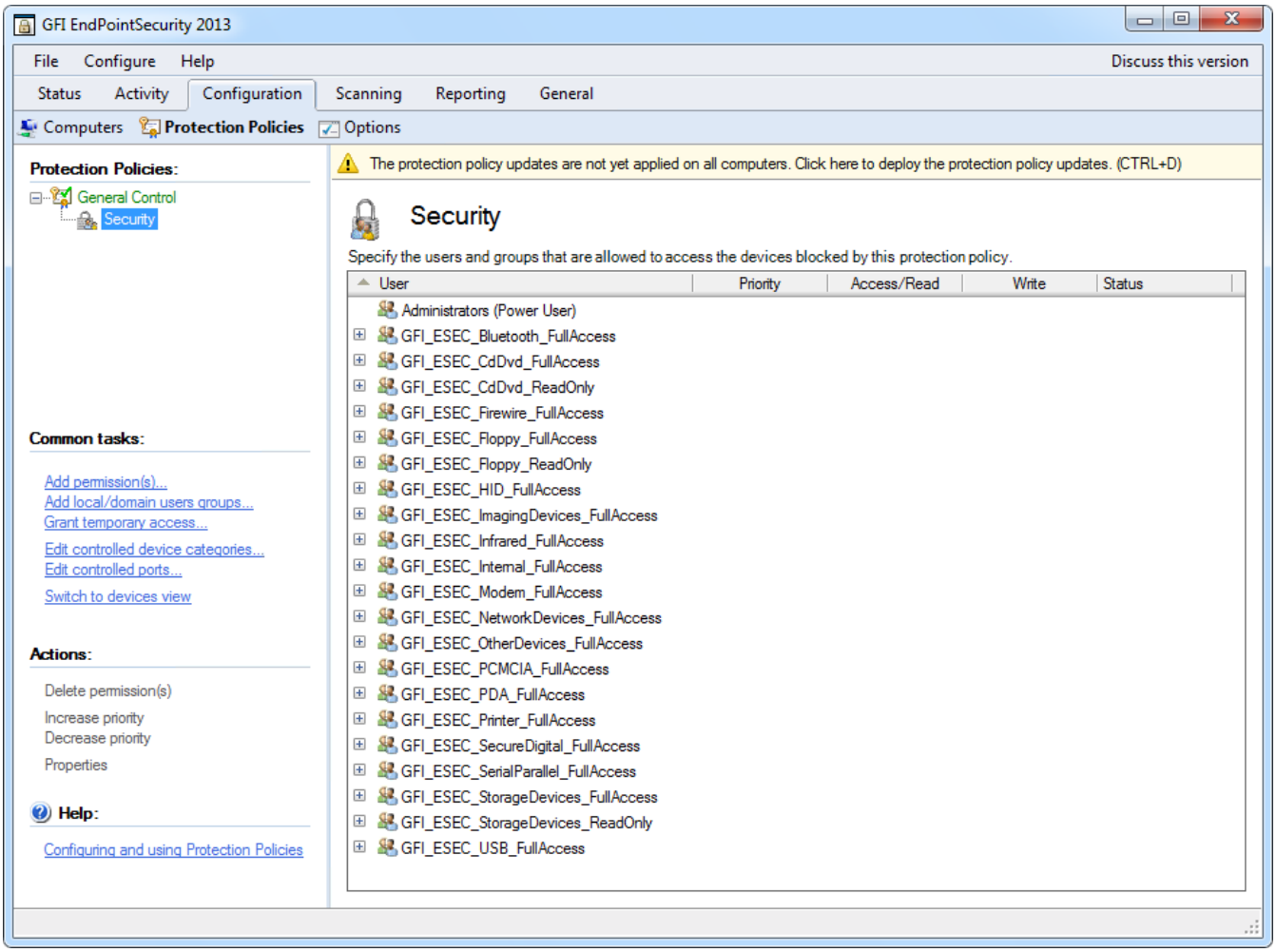
Quando uma categoria de dispositivo ou uma porta de conexão não é definida para ser controlada por uma política de segurança em particular, a permissão relevante é desabilitada. Para obter mais informações, consulte Configurar categorias de dispositivos controladas ou Configurar portas de conectividade controladas.

Para ver todas as permissões atribuídas a usuários em uma política de proteção:

1. Clique na guia **Configuration > Protection Policies**.
2. Em **Protection Policies > Security**, selecione a política de proteção a configurar.
3. Clique em **Security**. No painel direito é possível ver todas as permissões definidas para esta política de proteção.



Screenshot 38: Subguia Protection Policies - vista dos dispositivos



Screenshot 39: Subguia Protection Policies - vista dos usuários

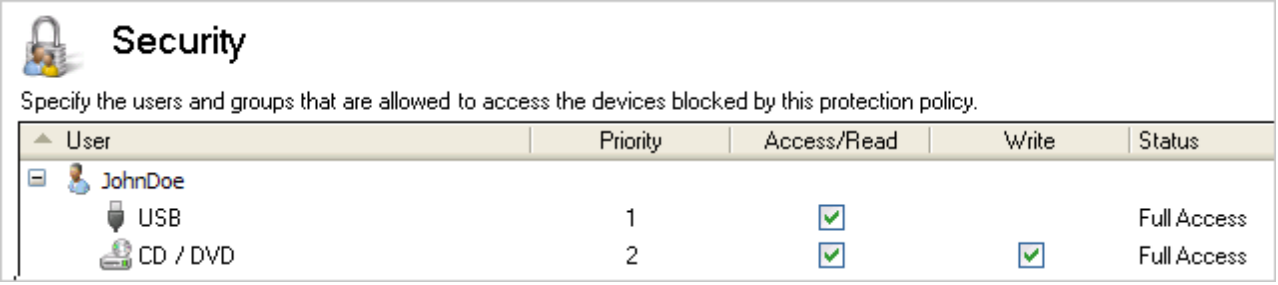
4. A partir do painel esquerdo, clique em **Switch to devices view** ou **Switch to users view** na seção **Common tasks** para alternar o agrupamento de permissões por dispositivos/portas ou usuários.

> **Obs.**
>
> Na vista dos usuários, é possível ver também os usuários avançados especificados na política.

6.8 Configurar prioridades para permissões

O GFI EndPointSecurity permite atribuir prioridades a quaisquer permissões atribuídas aos usuários e/ou grupos de usuários do Active Directory (AD). É possível fazê-lo em uma base de política por política e em uma base de usuário por usuário.

Por exemplo, para certo usuário especificado em uma determinada política de proteção, é possível decidir dar prioridade 1 às permissões da porta USB e prioridade 2 às permissões da unidade de CD/DVD. Isto significa que se o usuário se conectar a uma unidade de CD/DVD externa por meio da porta USB ao computador de destino, as permissões para a porta USB terão precedência relativamente às permissões da unidade de CD/DVD.



Screenshot 40: Subguia Protection Policies - Área Security

Para dar prioridade a permissões atribuídas a usuários em uma política de proteção:

1. Clique na guia **Configuration > Protection Policies**.
2. Em **Protection Policies > Security**, selecione a política de proteção a configurar.
3. Clique no subnó **Security**.
4. A partir do painel esquerdo, clique em **Switch to users view** na seção **Common tasks** para alternar o agrupamento de permissões por usuários.
5. Clique com o botão direito do mouse na seção **Security** e selecione **Expand all**.
6. Assinale o dispositivo ou porta necessário(a).
7. A partir do painel esquerdo, clique em **Increase priority** ou **Decrease priority** na seção **Actions**.

Para implantar atualizações de políticas de proteção em computadores de destino especificados na política:

1. Clique na guia **Configuration** > **Computers**.
2. A partir de **Common tasks**, clique em **Deploy to all computers**….

6.9 Configurar a lista de exclusão do dispositivo

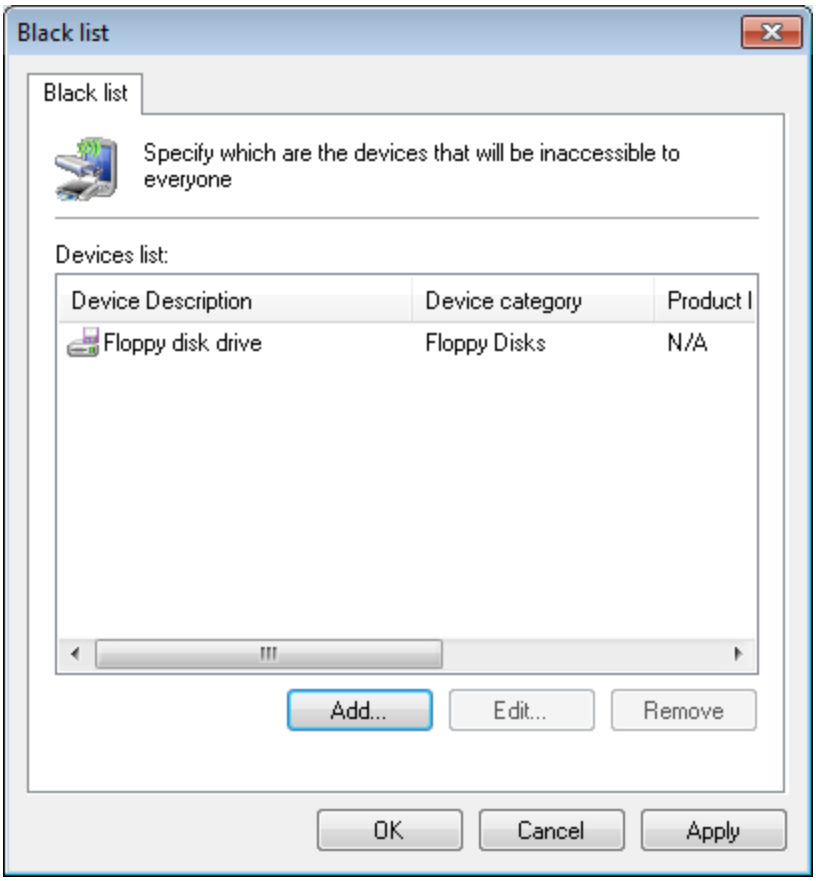
O GFI EndPointSecurity permite especificar que dispositivo(s) pode(m) tornar-se inacessíveis para todos. A lista de exclusão é granular, por isso é também possível adicionar à lista de exclusão um dispositivo específico com um número de série específico. É possível fazê-lo em uma base de política por política.

Para uma lista atualizada de dispositivos conectados no momento aos computadores de destino, execute uma verificação do dispositivo e adicione os dispositivos descobertos ao banco de dados dos dispositivos antes de configurar os dispositivos presentes na lista de exclusão. Para obter mais informações, consulte Descobrir dispositivos (página 101).

> **Obs.**
>
> Os usuários avançados substituirão dispositivos presentes na lista de exclusão e, assim, serão capazes de acessar dispositivos presentes na lista de exclusão.

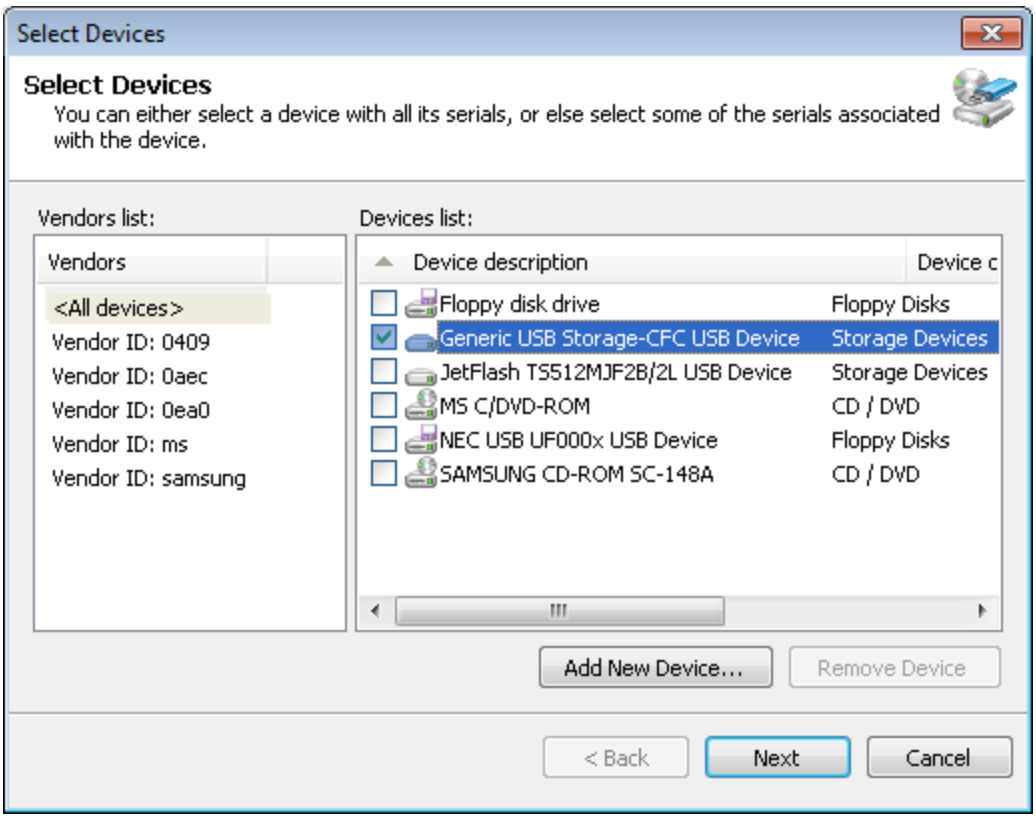
Para adicionar dispositivos à lista de exclusão de uma política de proteção específica:

1. Clique na guia **Configuration > Protection Policies**.
2. Em **Protection Policies > Security**, selecione a política de proteção a configurar.
3. A partir do painel direito, clique em **Devices Blacklist** na seção **General Control**.



Screenshot 41: Opções de Black list

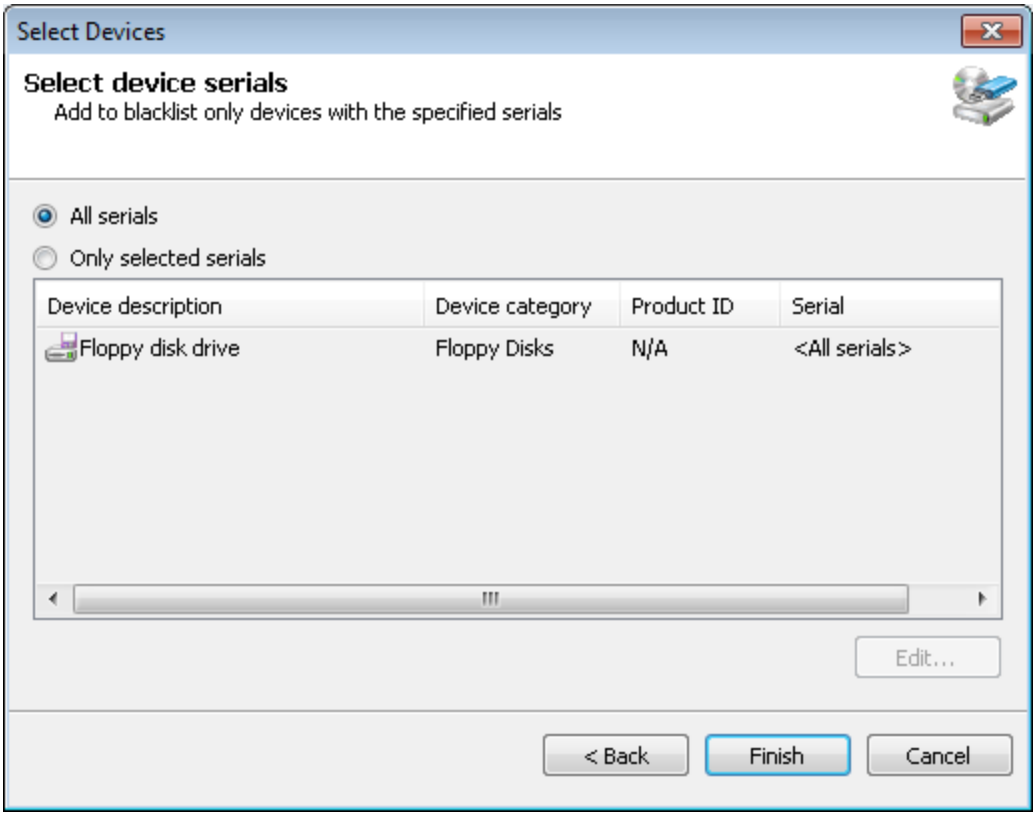
4. Na caixa de diálogo **Black list**, clique em **Add…** para selecionar dispositivos a adicionar à lista de exclusão.



Screenshot 42: Opções de Select Devices

5. Na caixa de diálogo **Select Devices** habilite ou desabilite os dispositivos para adicionar à lista de exclusão a partir da lista Devices e clique em **Next**.

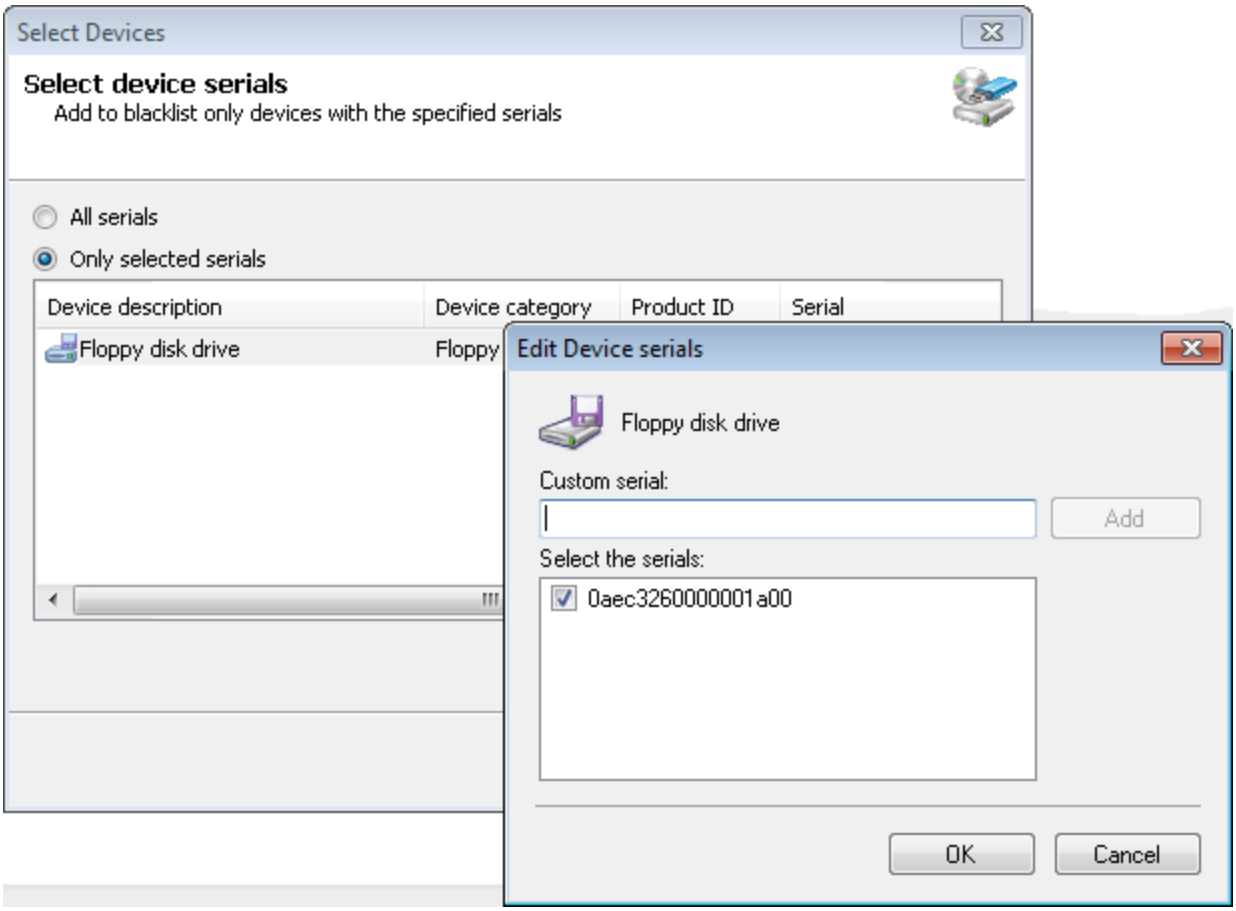
> **Obs.**
>
> Se um dispositivo necessário não se encontrar na lista, clique em **Add New Device…** para especificar os detalhes do dispositivo que deseja adicionar à lista de exclusão e clique em **OK**.



Screenshot 43: Opções de Select Devices - Select device serials

6. Selecione a opção relacionada com os números de série necessários a partir de:

- **All serials** - para adicionar à lista de exclusão todos os números de série de um dispositivo específico. Clique em **Finish** e **OK**.
- **Only selected serials** - para especificar número(s) de série do dispositivo específico(s) a adicionar à lista de exclusão. Em seguida, assinale o dispositivo e clique em **Edit…** para especificar o(s) número(s) de série(s). Clique em **OK**, **Finish** e **OK**.



Screenshot 44: Opções de Select Devices - Edit Device serials

Para implantar atualizações de políticas de proteção em computadores de destino especificados na política:

1. Clique na guia **Configuration** > **Computers**.
2. A partir de **Common tasks**, clique em **Deploy to all computers**….

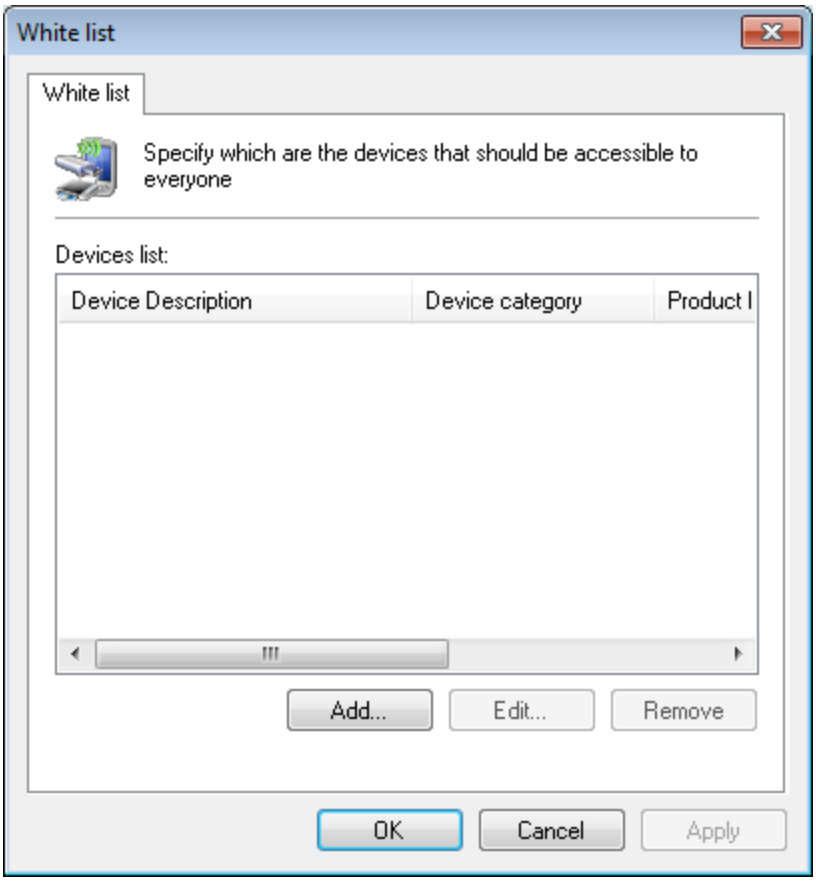
6.10 Configurar a lista de permissão do dispositivo

O GFI EndPointSecurity permite especificar o(s) dispositivo(s) que pode(m) ser acessado(s) por todos. A lista de permissão é granular, por isso também é possível adicionar à lista de permissão um dispositivo específico com um número de série específico. É possível fazê-lo em uma base de política por política.

Para uma lista atualizada de dispositivos conectados no momento aos computadores de destino, execute uma verificação do dispositivo e adicione os dispositivos descobertos ao banco de dados de dispositivos antes de configurar os dispositivos presentes na lista de permissão. Para obter mais informações, consulte Descobrir dispositivos (página 101).

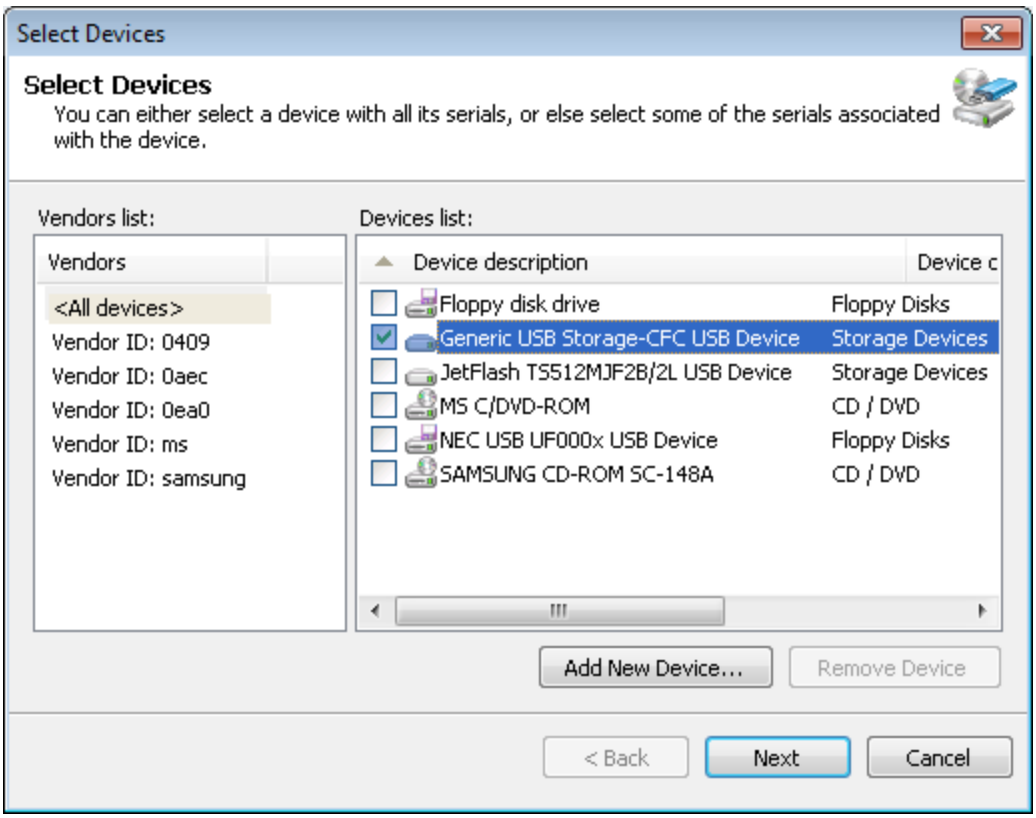
Para adicionar dispositivos da lista de permissão a uma política de proteção:

1. Clique na guia **Configuration > Protection Policies**.
2. Em **Protection Policies > Security**, selecione a política de proteção a configurar.
3. A partir do painel direito, clique em **Devices WhiteList** na seção **General Control**.



Screenshot 45: Opções da lista de permissão

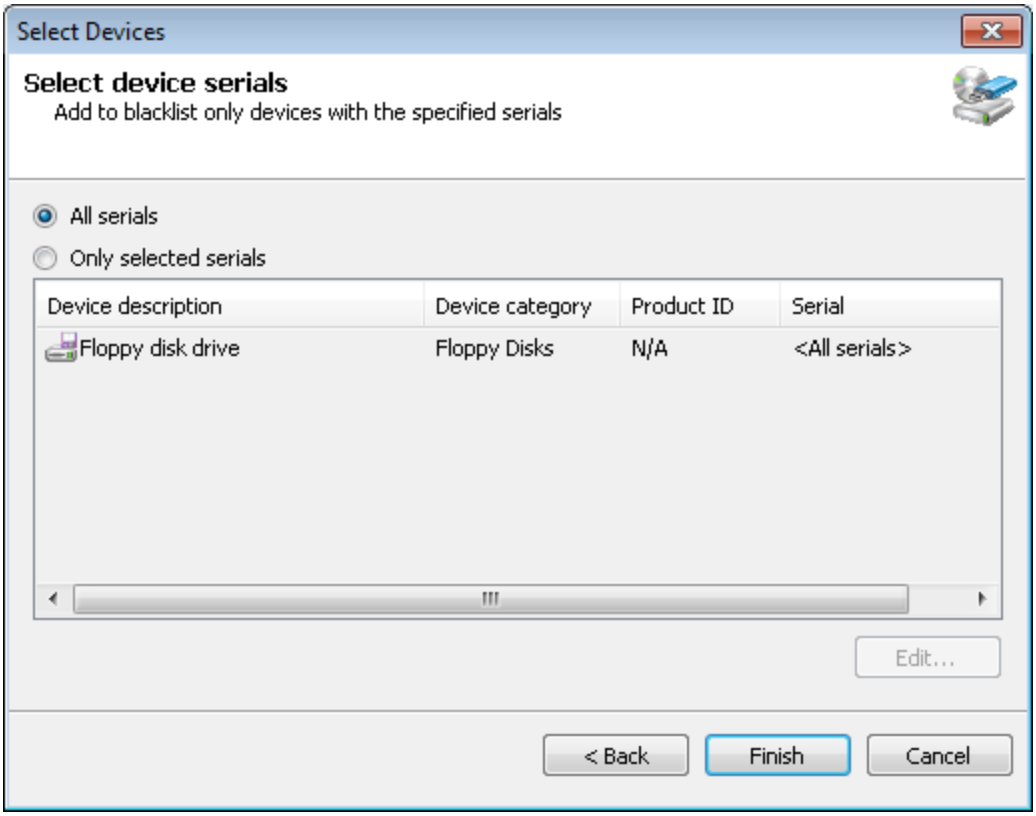
4. Na caixa de diálogo **White list**, clique em **Add…** para selecionar dispositivos a adicionar à lista de permissão.



Screenshot 46: Opções de Select Devices

5. Na caixa de diálogo **Select Devices** habilite ou desabilite os dispositivos para adicionar à lista de permissão a partir da lista Devices e clique em **Next**.

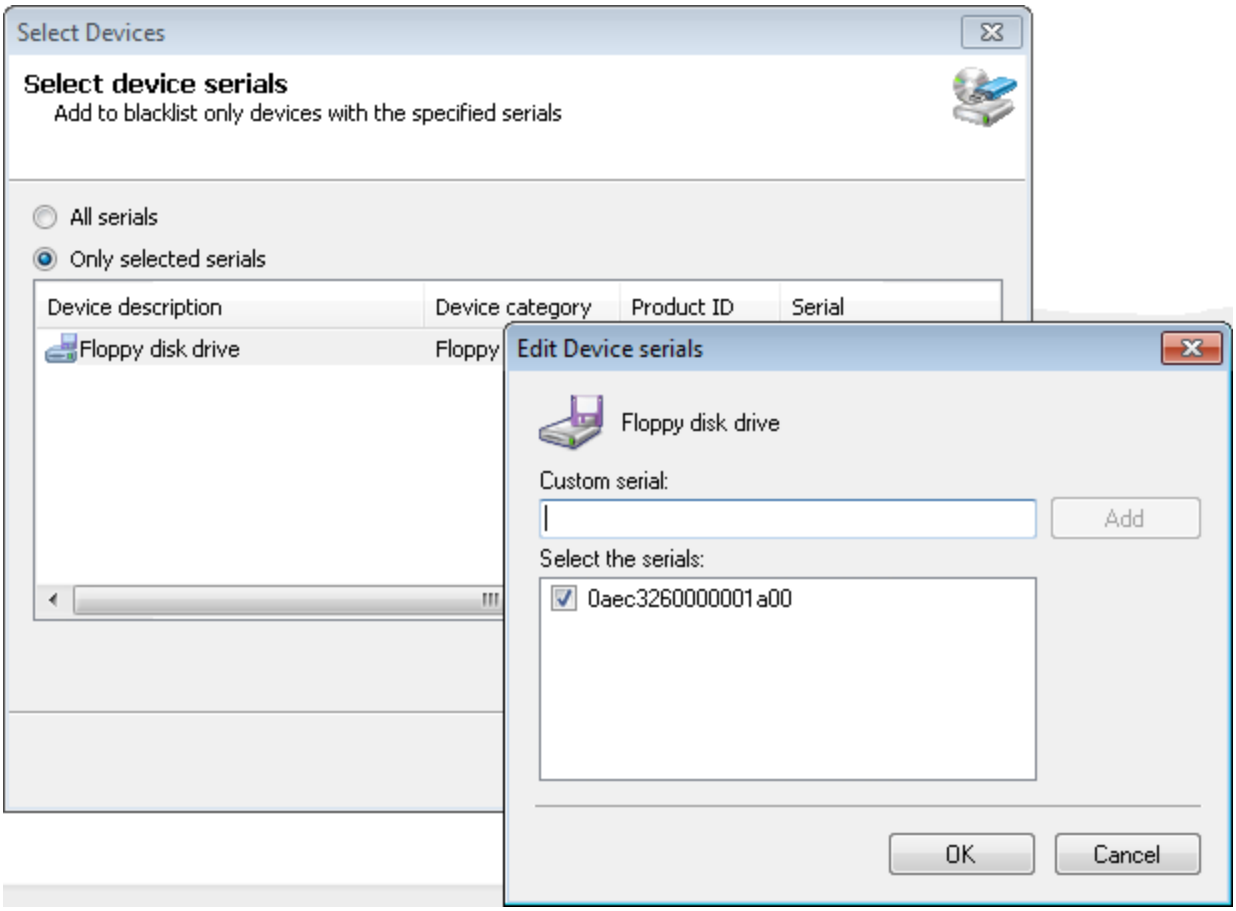
> **Obs.**
>
> Se um dispositivo necessário não se encontrar na lista, clique em **Add New Device…** para especificar os detalhes do dispositivo que deseja adicionar à lista de permissão e clique em **OK**.



Screenshot 47: Opções de Select Devices - Select device serials

6. Selecione a opção relacionada com os números de série necessários a partir de:

- **All serials** – para adicionar à lista de permissão todos os números de série de um dispositivo específico. Clique em **Finish** e **OK**.
- **Only selected serials** – para especificar que somente os números de série de dispositivos específicos são adicionados à lista de permissão. Em seguida, assinale o dispositivo e clique em **Edit…** para selecionar o(s) número(s) de série(s) na lista de permissão. Clique em **OK**, **Finish** e **OK**.



Screenshot 48: Opções de Select Devices - Edit Device serials

Para implantar atualizações de políticas de proteção em computadores de destino especificados na política:

1. Clique na guia **Configuration** > **Computers**.
2. A partir de **Common tasks**, clique em **Deploy to all computers…**.

6.11 Configurar os privilégios de acesso temporário

O GFI EndPointSecurity permite garantir acesso temporário aos usuários. Isto permite aos usuários acessar dispositivos e portas de conexão em computadores de destino protegidos por uma duração/janela de tempo especificada. É possível fazê-lo em uma base de política por política.

Quando o acesso temporário é fornecido, quaisquer permissões e configurações (por ex., filtros do tipo de arquivo) definidas na política de proteção aplicável ao computador de destino são temporariamente substituídas.

Para obter mais informações, consulte Como funciona o GFI EndPointSecurity - acesso temporário (página 18).

» Solicitar acesso temporário para um computador protegido

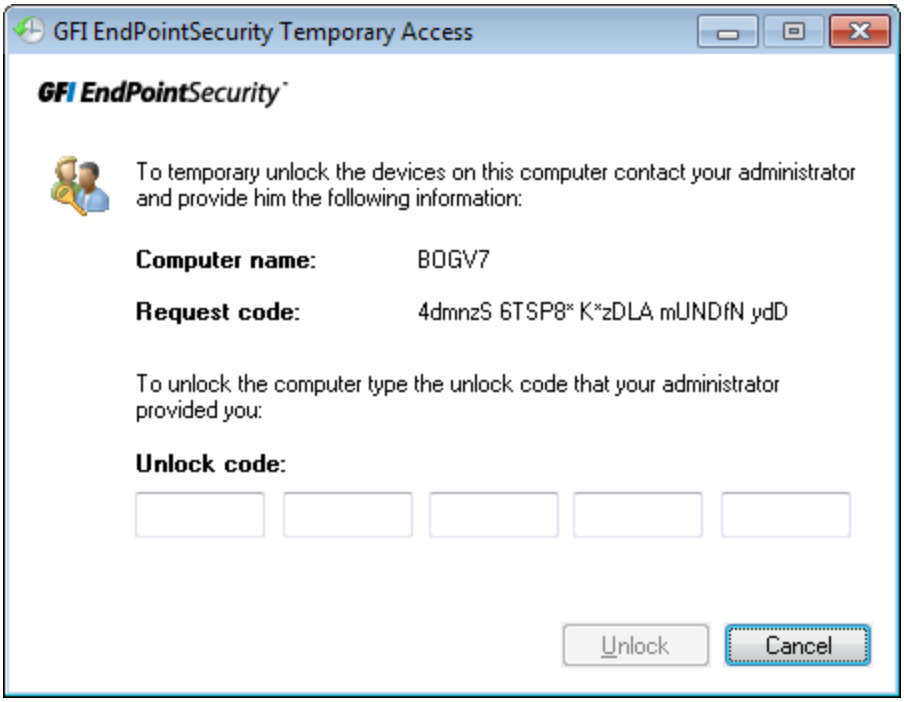
» Conceder acesso temporário a um computador protegido.

6.11.1 Solicitar acesso temporário para um computador protegido

Para gerar um código de solicitação: ferramenta:

Screenshot 49: Ícone Devices Temporary Access

1. A partir do **Control Panel** clique em **Devices Temporary Access**.



Screenshot 50: Ferramenta Temporary Access do GFI EndPointSecurity

2. Na caixa de diálogo **GFI EndPointSecurity Temporary Access** tome nota do **Request code** gerado. Comunique os detalhes seguintes a seu administrador de segurança:

- Código de solicitação
- Tipo de dispositivo/porta de conexão
- Quando solicitar acesso
- Durante quanto tempo necessita de acesso.

Mantenha a ferramenta Temporary Access do GFI EndPointSecurity aberta.

3. Quando o administrador enviar o código de desbloqueio, digite-o no campo **Unlock code**.

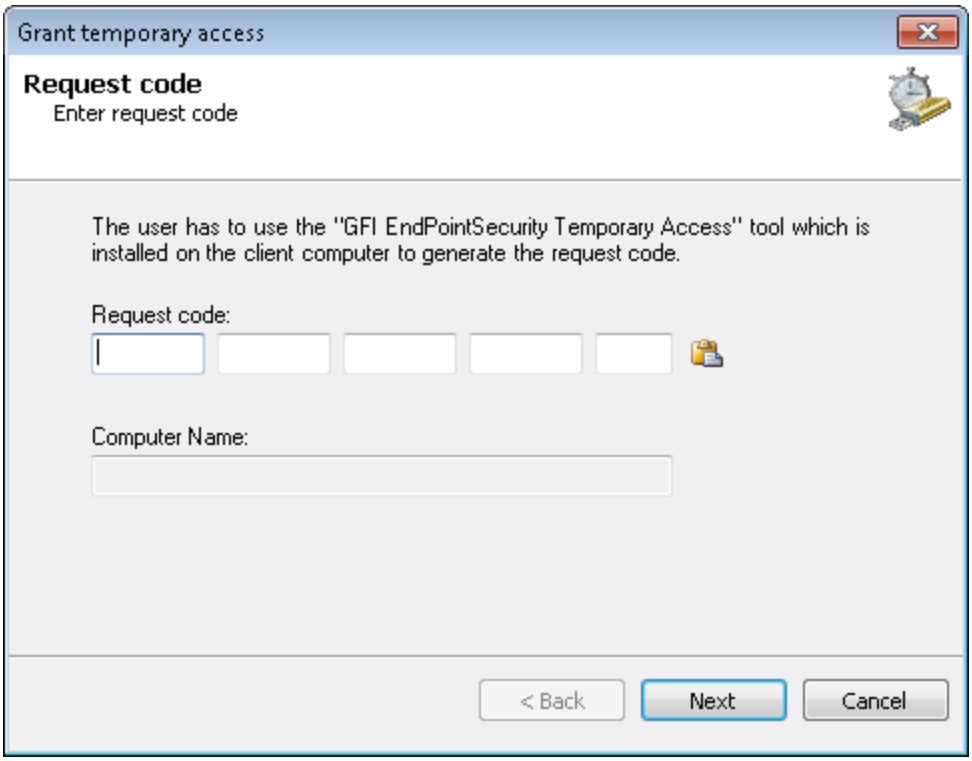
> **Obs.**
>
> Um código de desbloqueio digitado em um computador de destino protegido fora do período de validade especificado não ativará o acesso temporário.

4. Clique em **Unlock** para ativar o acesso temporário. Agora já pode acessar o dispositivo e/ou a porta de conexão necessário(a).

6.11.2 Conceder acesso temporário a um computador protegido

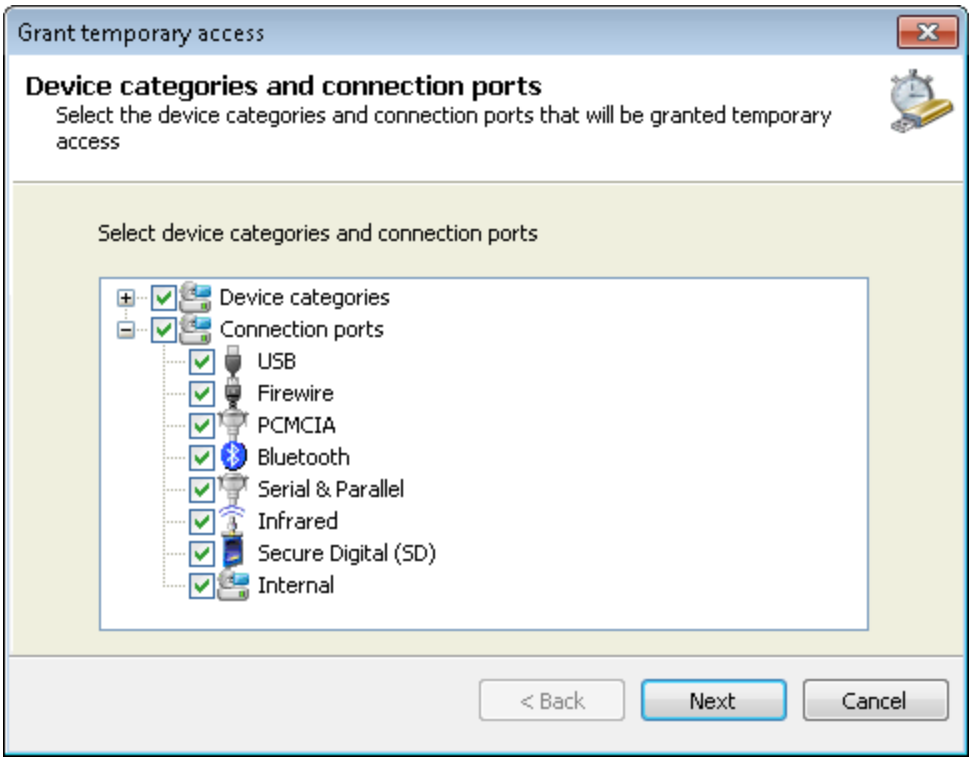
Para conceder acesso temporário:

1. A partir do console de gerenciamento do GFI EndPointSecurity, clique na guia **Configuration** > sub-guia **Protection Policies**.
2. A partir do painel esquerdo, selecione a política de proteção que inclui o computador ao qual é necessário conceder acesso temporário.
3. A partir do painel direito, clique em **Grant temporary access** na seção **Temporary Access**.



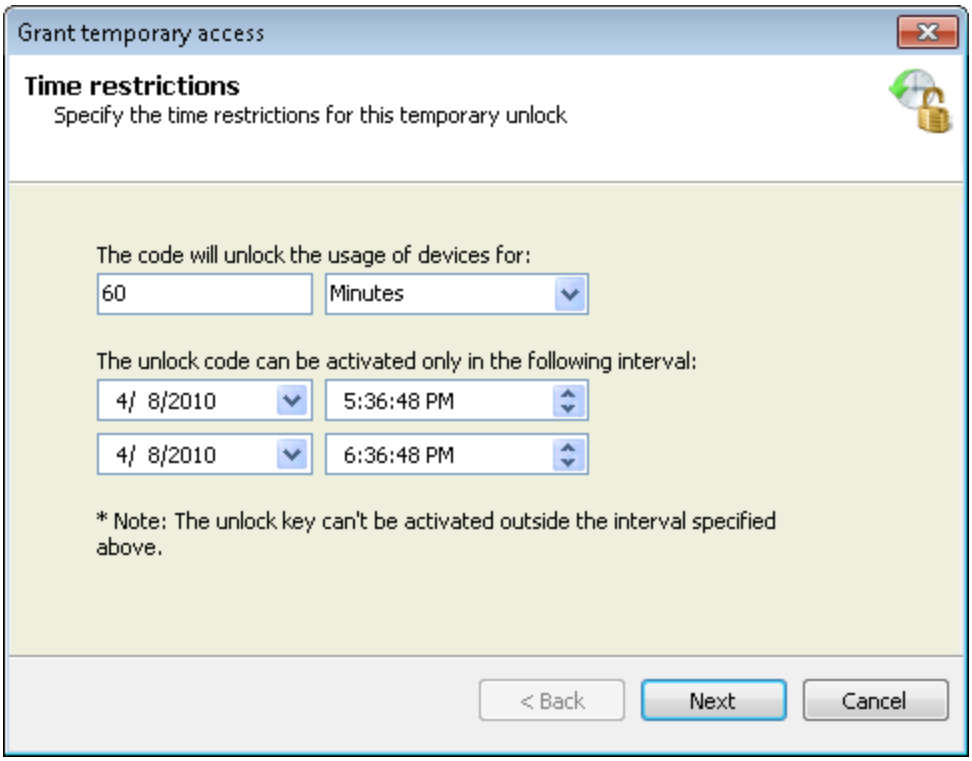
Screenshot 51: Opções de Grant temporary access - Request code

4. Na caixa de diálogo **Grant temporary access** digite o código de solicitação recebido do usuário, no campo **Request code**. O nome do computador a partir do qual o código de solicitação foi gerado é exibido no campo **Computer Name**. Clique em **Next**.



Screenshot 52: Opções de Grant temporary access - Device categories and connection ports

5. Na lista, habilite as categorias e/ou as portas de conexão dos dispositivos necessários aos quais irá conceder acesso temporário e clique em **Next**.



Screenshot 53: Opções de Grant temporary access - Time restrictions

6. Especifique a duração durante a qual o acesso é permitido e o período de validade do código de desbloqueio e clique em **Next**.

7. Tome nota do **Unlock code** gerado. Comunique o código ao usuário que está solicitando acesso temporário e clique em **Finish**.

6.12 Configurar filtros do tipo de arquivo

O GFI EndPointSecurity permite especificar as restrições por tipo de arquivo em arquivos, tais como .DOC ou .XLS, sendo copiados para/de dispositivos permitidos. É possível aplicar estas restrições aos usuários e/ou grupos de usuários do Active Directory (AD). É possível fazê-lo em uma base de política por política.

A filtragem é baseada nas verificações da extensão de arquivo e nas verificações da assinatura real do tipo de arquivo. A verificação da assinatura real do tipo de arquivo pode ser realizada nos seguintes tipos de arquivos:

AVI	BMP	CAB	CHM	DLL	DOC	EMF	EXE	GIF	HLP
HTM	JPE	JPEG	JPG	LNK	M4A	MDB	MP3	MPEG	MPG
MSG	MSI	OCX	P7M	PDF	PPT	RAR	RTF	SCR	SYS
TIF	TIFF	TXT	URL	WAV	XLS	ZIP	DOCX	XLSX	PPTX

Obs. 1

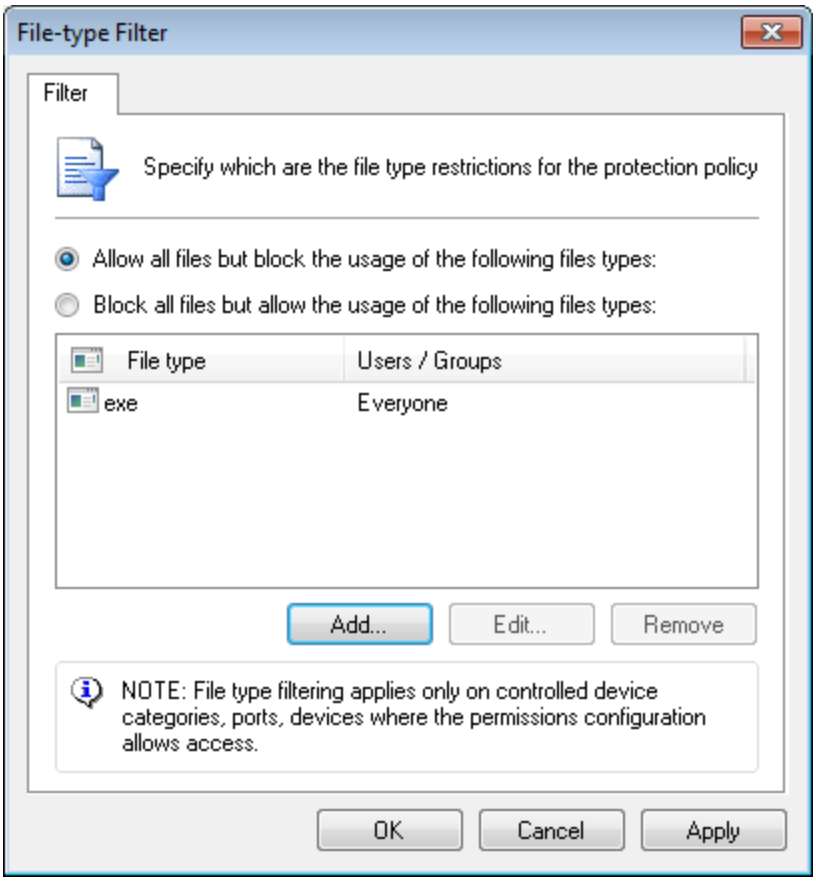
Para qualquer outro tipo de arquivo não especificado acima, a filtragem baseia-se somente na extensão de arquivo.

Obs. 2

A filtragem por tipo de arquivo se aplica somente a categorias e/ou portas de dispositivos para as quais as permissões foram definidas para permitir o acesso.

Para configurar as restrições do tipo de arquivo para usuários em uma política de proteção específica:

1. A partir do console de gerenciamento do GFI EndPointSecurity, clique na guia **Configuration > Protection Policies**.
2. A partir do painel esquerdo, selecione a política de proteção para a qual deseja especificar restrições de tipos de arquivos.
3. A partir do painel direito, clique em **File-type Filter** na seção **File control**.

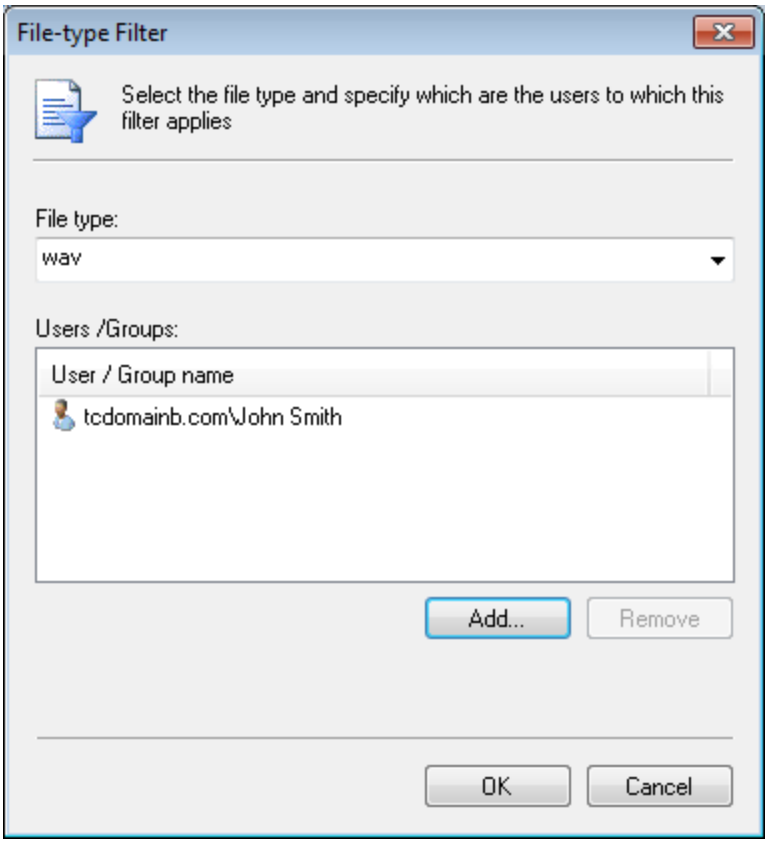


Screenshot 54: Opções de File-type Filter

4. Na caixa de diálogo File-type Filter, selecione a restrição a aplicar a esta política:

» Permite todos os arquivos, mas bloqueia o uso dos seguintes tipos de arquivos

» Bloqueia todos os arquivos, mas permite o uso dos seguintes tipos de arquivos.



Screenshot 55: Opções de usuário e filtro de tipo de arquivo

5. Clique em **Add…** e selecione ou digite o tipo de arquivo a partir da lista suspensa **File type**.
6. Clique em **Add…** para especificar os usuários/grupos que possuem permissão/estão bloqueados de acessar o tipo de arquivo especificado e clique em **OK**. Repita as duas subetapas anteriores para cada tipo de arquivo a restringir.
7. Clique em **OK** duas vezes.

Para implantar atualizações de políticas de proteção em computadores de destino especificados na política:

1. A partir do console de gerenciamento do GFI EndPointSecurity, clique na guia **Configuration** > sub-guia **Computers**.
2. A partir do painel esquerdo, clique em **Deploy to all computers…** na seção **Common tasks**.

6.13 Configurar conscientização do conteúdo

O GFI EndPointSecurity permite especificar as restrições do conteúdo do arquivo para uma política de proteção em particular. O recurso de conscientização do conteúdo verifica os arquivos que transitam os pontos de extremidade por meio de dispositivos removíveis e este identifica conteúdo baseado em expressões regulares pré-configuradas e personalizadas e em arquivos do dicionário. Por padrão, o módulo procura detalhes confidenciais seguros tais como números de previdência social e números de contas primárias, bem como informações relacionadas com empresas, tais como nomes de doenças, medicamentos, químicos perigosos e também linguagem trivial e termos étnicos/racistas.

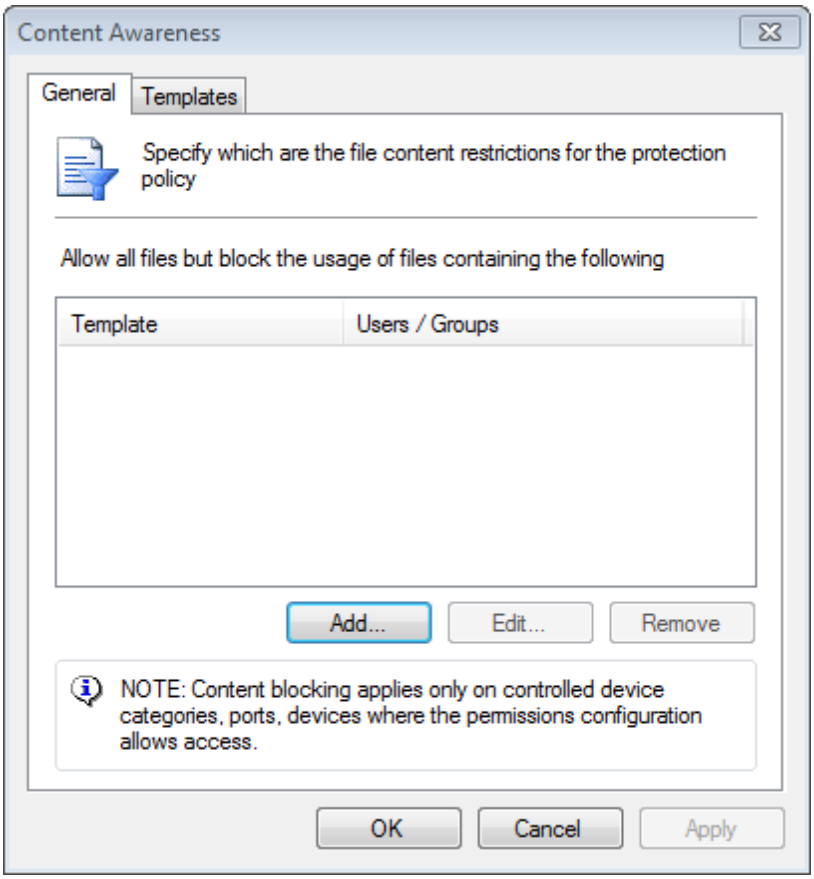
» É possível configurar o conteúdo verificando como uma política global de uma forma semelhante ao módulo de verificação de arquivos.

6.13.1 Gerenciar opções de conscientização do conteúdo

Para configurar as opções de conscientização do conteúdo para usuários

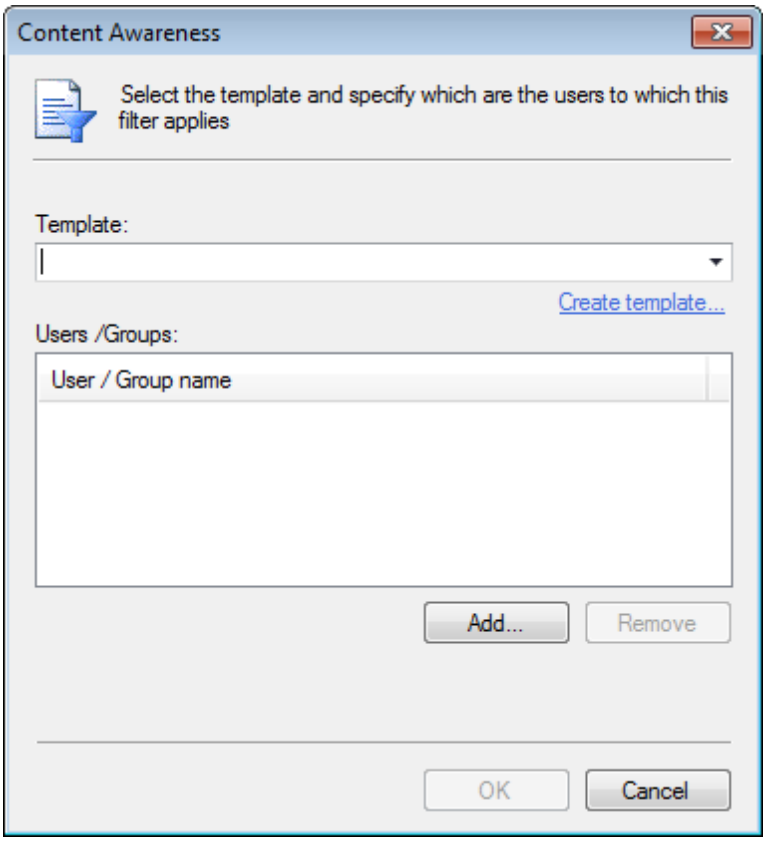
em uma política de proteção específica:

1. A partir do console de gerenciamento GFI EndPointSecurity, clique na guia **Configuration > Protection Policies**.
2. A partir do painel esquerdo, selecione a política de proteção para a qual deseja especificar restrições de conteúdo.
3. A partir do painel direito, clique em **Content awareness** na seção **File control**.



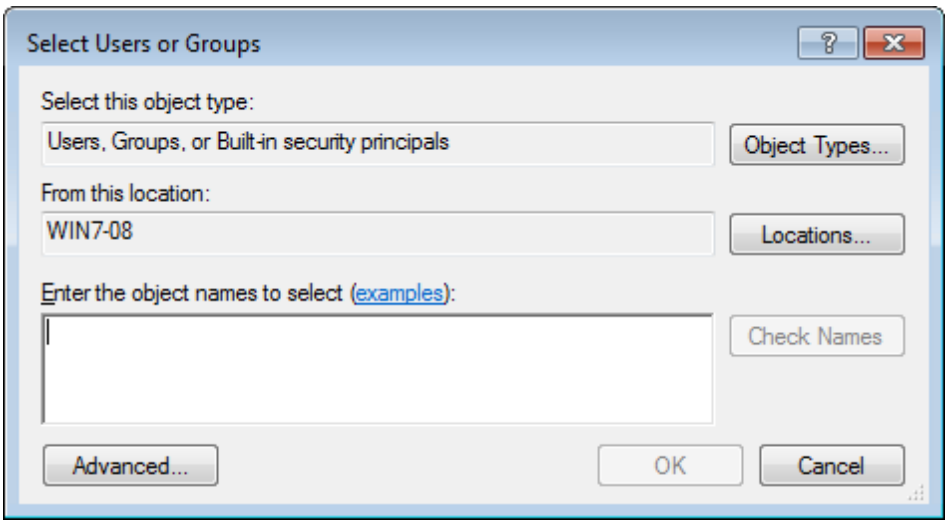
Screenshot 56: Opções de Content Awareness

4. Na caixa de diálogo Content Awareness, clique em **Add** para selecionar o modelo a aplicar nesta política:



Screenshot 57: Adicionar um novo modelo

5. Clique em **Add…** e selecione ou digite o modelo a partir da lista suspensa **Template**.
6. Clique em **Add…** para especificar o(s) usuário(s)/grupo(s) e clique em **OK**. Repita as duas subetapas anteriores para cada modelo que será aplicado.
7. Clique em **OK**.

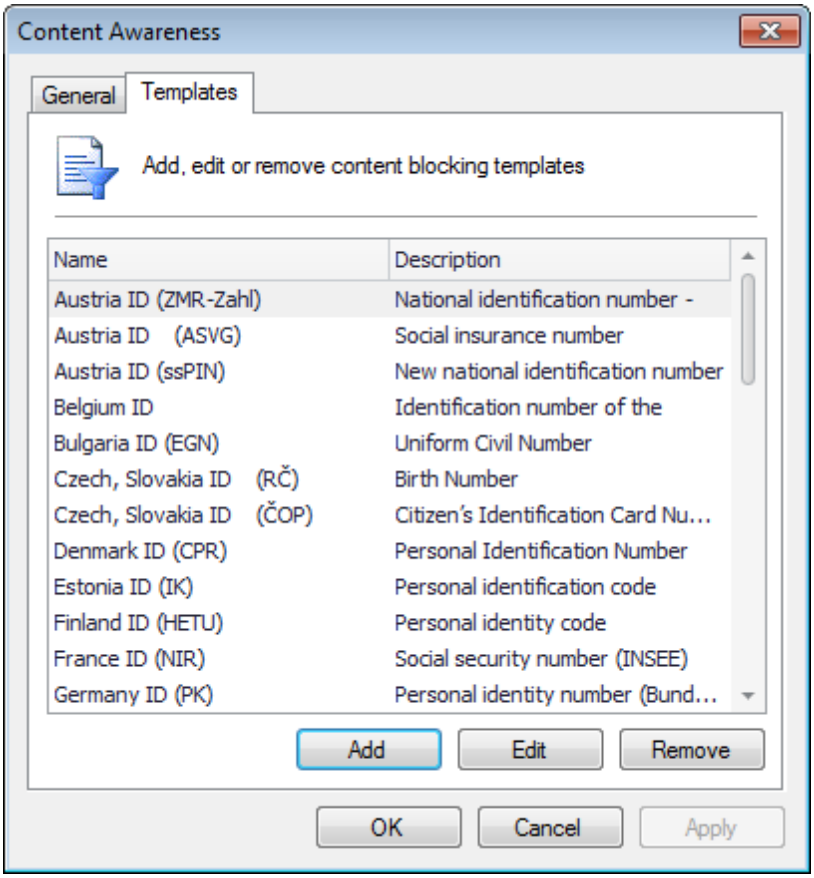


Screenshot 58: Selecionar usuários ou grupos

6.13.2 Gerenciar opções de modelos

Para adicionar, editar ou remover modelos predefinidos:

1. Clique em **Templates** e selecione um modelo a partir da lista **Template**.
2. Clique em **Add**, **Edit** ou **Remove** para alterar ou excluir modelos.

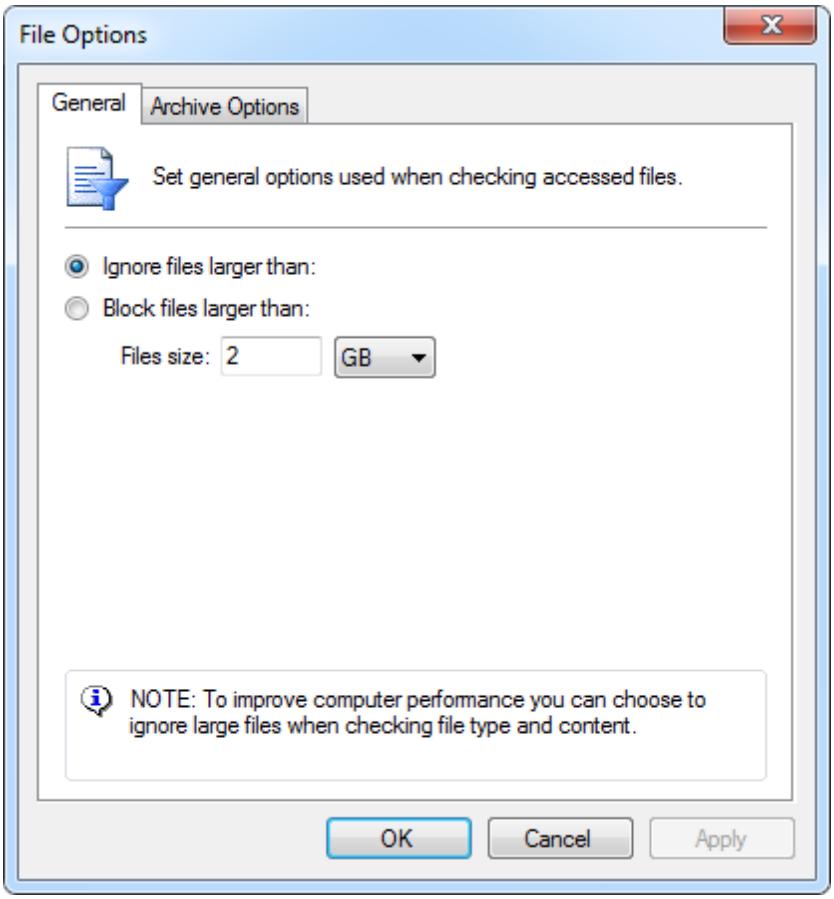


Screenshot 59: Gerenciar modelos

6.14 Configurar opções do arquivo

O GFI EndPointSecurity permite especificar as opções necessárias para bloquear ou permitir arquivos com base no tamanho. O GFI EndPointSecurity permite também ignorar arquivos de grande dimensão ao verificar o tipo e o conteúdo do arquivo, bem como os arquivos armazenados.

1. A partir do console de gerenciamento GFI EndPointSecurity, clique na guia **Configuration > Protection Policies**.
2. A partir do painel esquerdo, selecione a política de proteção para a qual deseja especificar restrições de opções do arquivo.
3. A partir do painel direito, clique em **File options** na seção **File control**.

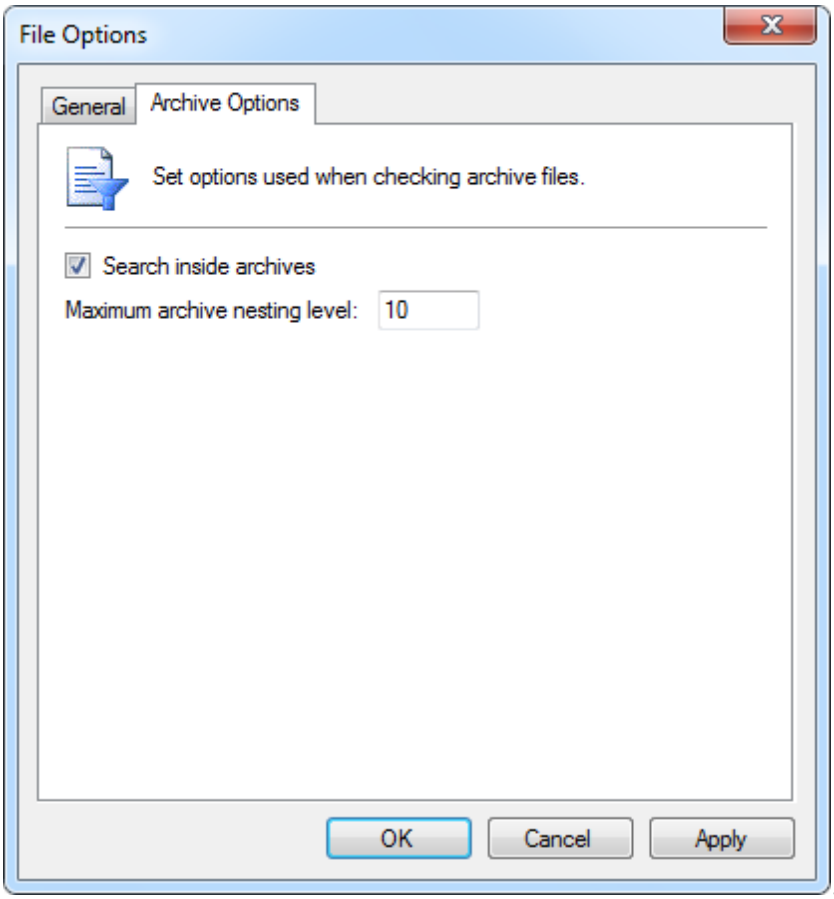


Screenshot 60: Opções de arquivo

4. Na caixa de diálogo File Options, selecione a partir das opções seguintes:

Table 13: Opções de arquivo - Opções do usuário

Opção	Descrição
Ignore files larger than:	Ignora arquivos maiores do que o tamanho especificado ao verificar arquivos acessados.
Block files larger than:	Bloqueia arquivos maiores do que o tamanho especificado ao verificar arquivos acessados.



Screenshot 61: Opções de usuário e filtro de tipo de arquivo

5. A partir da guia **Archive Options**, habilite/desabilite **Search inside archives** e especifique o nível de aninhamento do arquivo ao verificar arquivos do arquivo.
6. Clique em **OK**.

6.15 Configurar criptografia de segurança

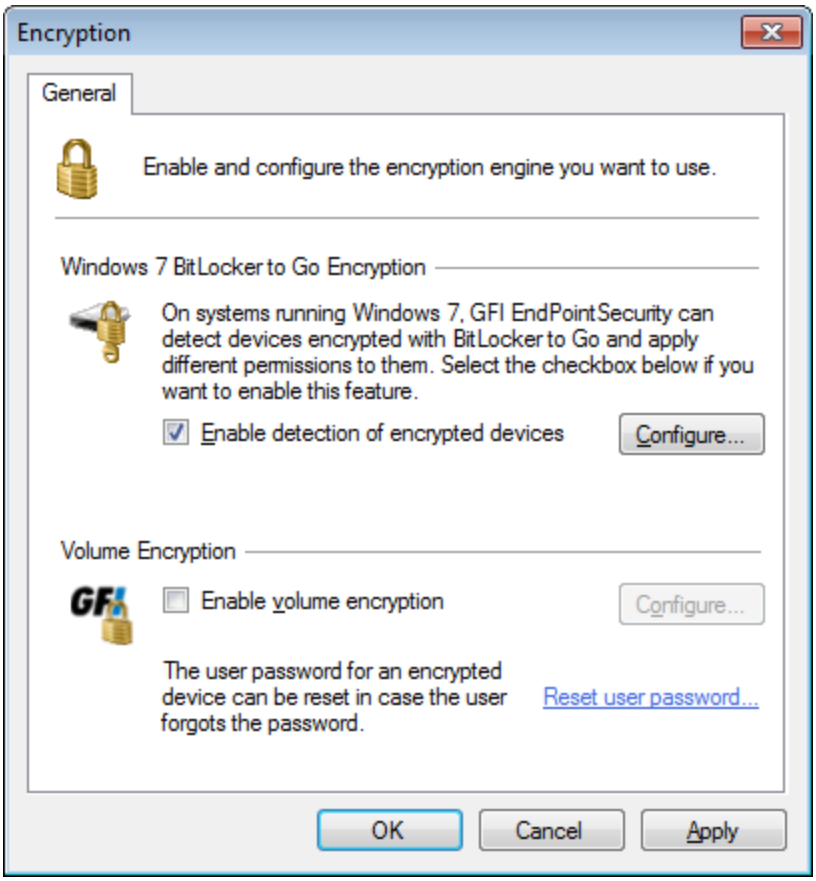
O GFI EndPointSecurity permite configurar definições que se adaptam especificamente a dispositivos criptografados. Este permite também criptografar dispositivos que ainda não estejam protegidos.

- Configurar os dispositivos BitLocker To Go da Microsoft
- Configurar a criptografia de volume

6.15.1 Configurar os dispositivos BitLocker To Go da Microsoft

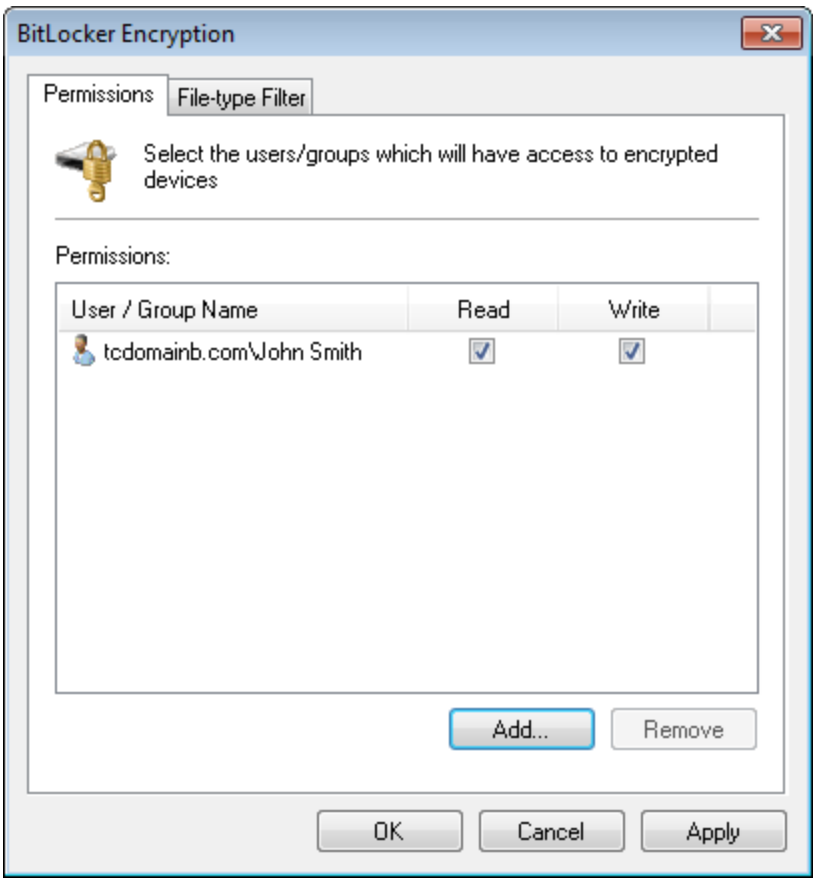
O GFI EndPointSecurity pode detectar dispositivos de armazenamento criptografados com o BitLocker To Go da Microsoft. Isto permite configurar diferentes permissões em tais dispositivos. Para habilitar a detecção do BitLocker To Go da Microsoft:

1. A partir do console de gerenciamento do GFI EndPointSecurity, clique na guia **Configuration > Protection Policies**.
2. A partir do painel esquerdo, selecione a política de proteção para a qual deseja aplicar a política de criptografia.
3. A partir do painel direito, clique em **Encryption** na seção **Security**.



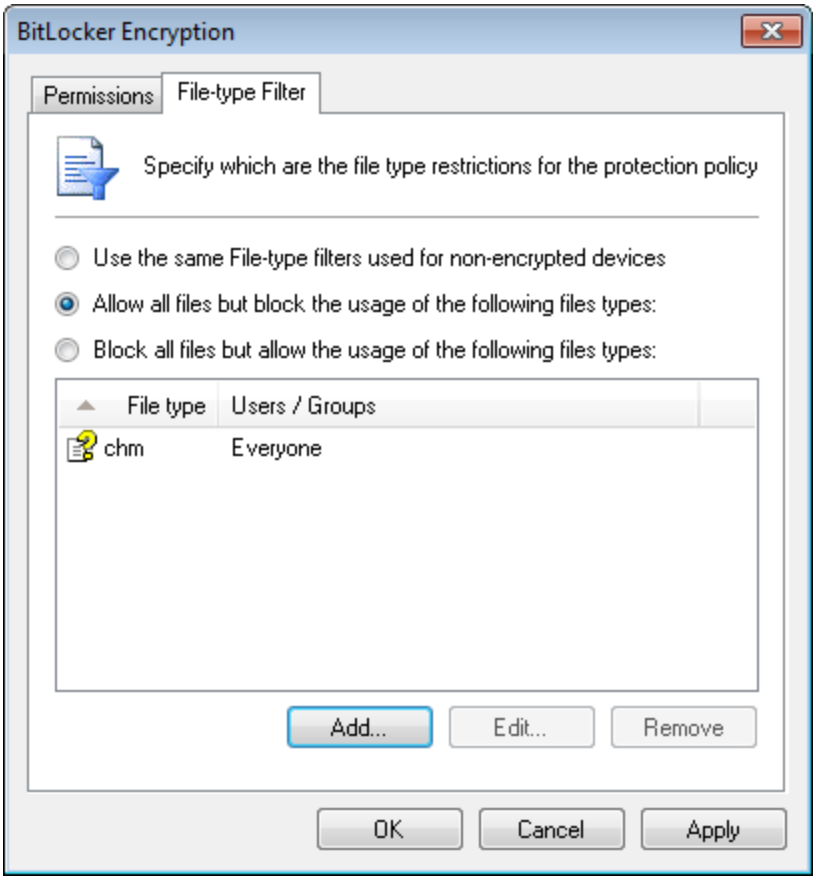
Screenshot 62: Opções de Encryption - Guia General

4. Selecione **Enable detection of encrypted devices** e clique em **Configure...**.



Screenshot 63: Opções de Encryption - Guia Permissions

5. Clique em **Add…** para especificar os usuários e grupos com acesso a dispositivos criptografados.



Screenshot 64: Opções de Encryption - Guia File-type Filter

6. Selecione a guia **File-type Filter** para configurar os tipos de arquivos a restringir.
7. Selecione a restrição a aplicar a esta política:

» Use os mesmos filtros de tipo de arquivo usados para dispositivos não criptografados

» Permite todos os arquivos, mas bloqueia o uso dos seguintes tipos de arquivos

» Bloqueia todos os arquivos, mas permite o uso dos seguintes tipos de arquivos.

8. Use os botões **Add**, **Edit** e **Remove** para gerenciar tipos de arquivos.
9. Clique em **OK**.

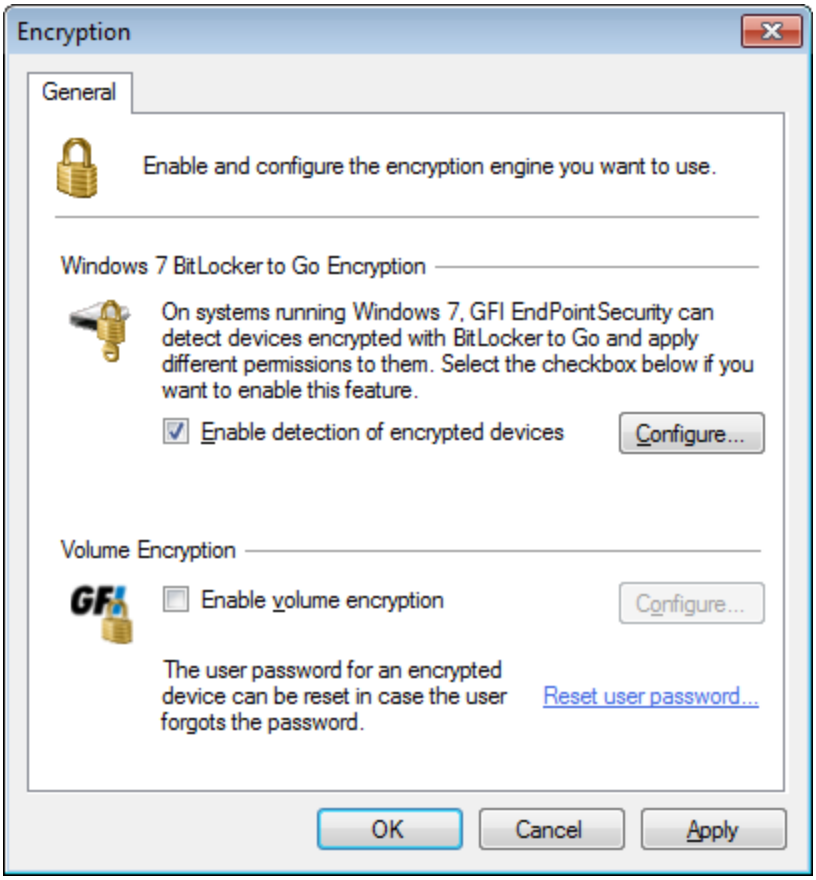
6.15.2 Configurar a criptografia de volume

A criptografia de volume permite criptografar os conteúdos de dispositivos USB usando a criptografia AES 256. Quando a criptografia de volume é reforçada, os usuários devem fornecer uma senha para criptografar ou acessar dados dos dispositivos de armazenamento. Para reforçar a criptografia de volume em agentes instalados:

Obs.

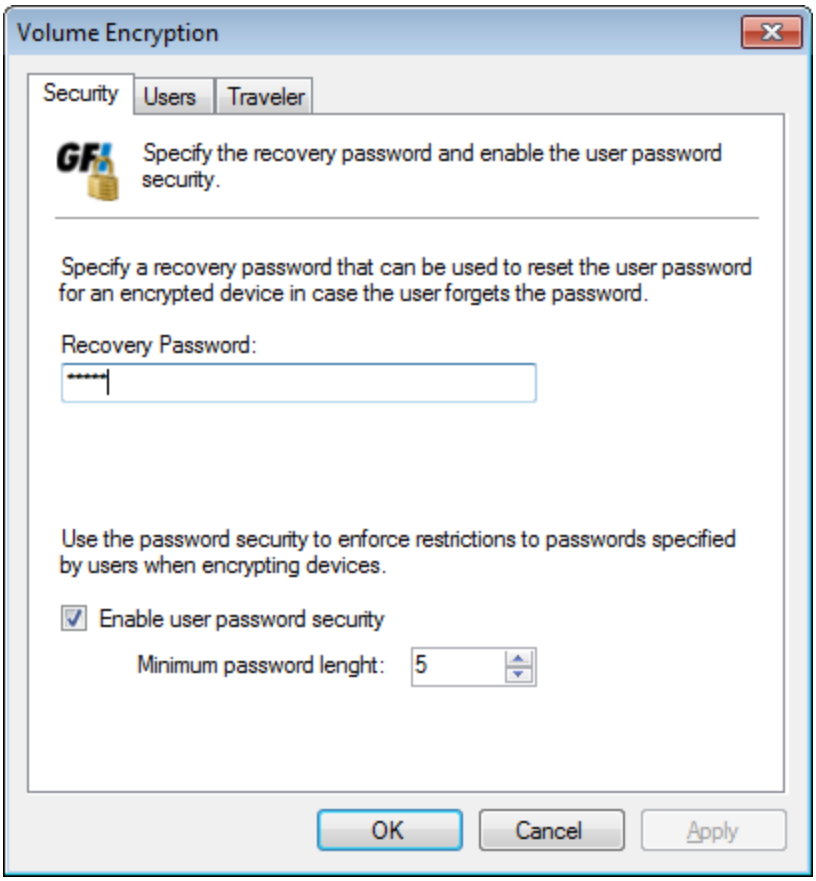
A criptografia a pedido é possível mesmo se não for forçada pelo administrador diretamente pelo usuário final, clicando na entrada **Encrypt...** a partir do menu de contexto de shell de uma unidade removível.

1. A partir do console de gerenciamento do GFI EndPointSecurity, clique na guia **Configuration > Protection Policies**.
2. A partir do painel esquerdo, selecione a política de proteção para a qual deseja aplicar a política de criptografia.
3. A partir do painel direito, clique em **Encryption** na seção **Security**.



Screenshot 65: Opções de Encryption - Guia General

4. Selecione **Enable volume encryption**. Clique em **Configure**. Clique em **Reset user password** para redefinir a senha de criptografia para um usuário específico.

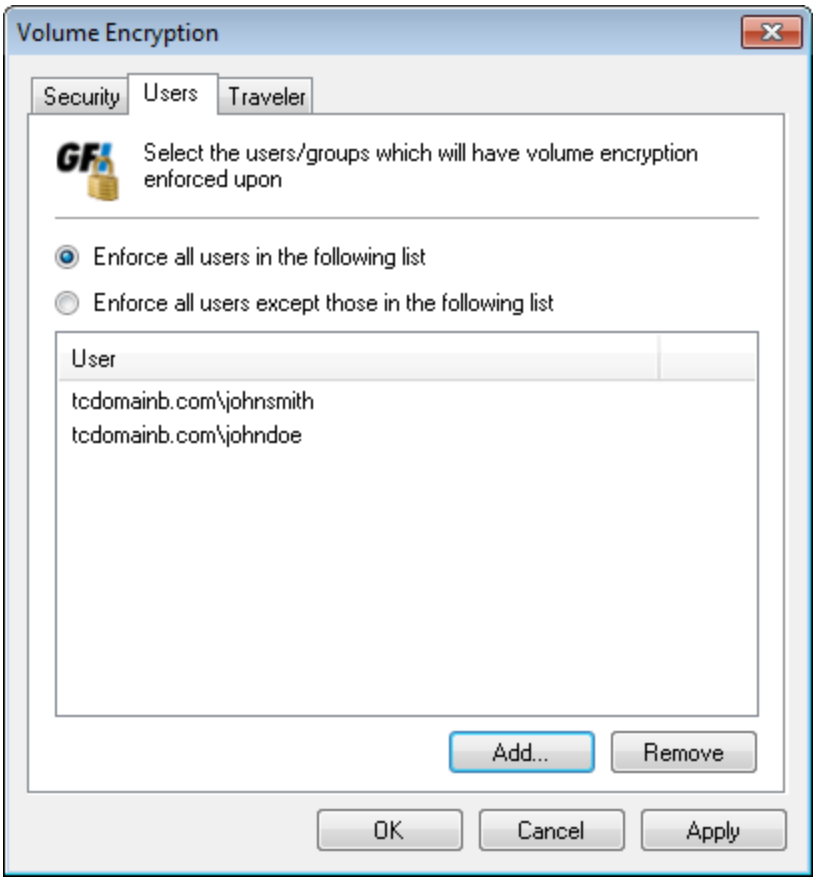


Screenshot 66: Opções de Encryption - Guia Security

5. A partir da guia **Security**, configure os recursos descritos abaixo:

Table 14: Volume Encryption - Opções de Security

Opção	Descrição
Recovery Password	Digite uma senha usada se os usuários se esquecerem de ou perderem suas senhas.
Enable user password security	Reforce as restrições a senhas especificadas por usuários finais. Em **Minimum password length**, especifique o comprimento mínimo aceitável para a senha.

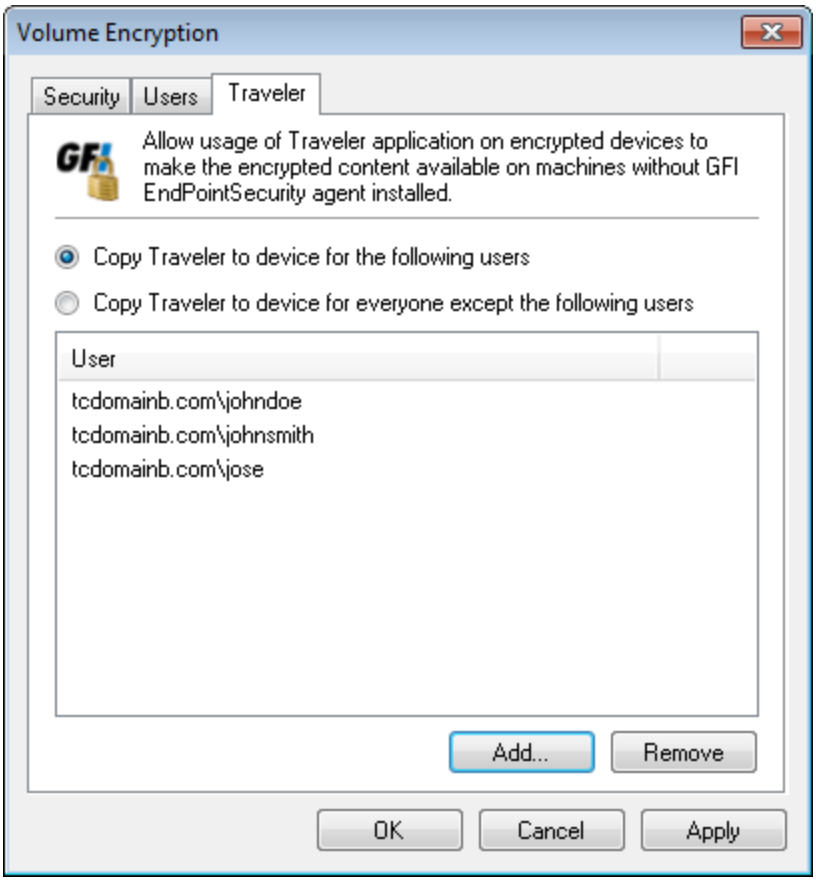


Screenshot 67: Opções de criptografia - Guia Users

6. Selecione a guia **Users** e configure as opções seguintes:

Table 15: Volume Encryption - Opções de Users

Opção	Descrição
Enforce all users in the following list	Selecione os usuários que possuem uma criptografia de volume reforçada em seus dispositivos portáteis. Use os botões **Add** e **Remove** para gerenciar os usuários selecionados.
Enforce all users except those in the following list	Selecione os usuários que ficarão isentos da criptografia de volume. Use os botões Add e Remove para gerenciar os usuários selecionados.



Screenshot 68: Opções de Encryption - Guia Traveler

Obs.

Traveler é um aplicativo que pode ser instalado automaticamente nos dispositivos de armazenamento usando o GFI EndPointSecurity. Este aplicativo permite descriptografar dados criptografados pelo GFI EndPointSecurity em dispositivos de armazenamento, a partir de computadores que não estejam executando um Agente do GFI EndPointSecurity.

7. Selecione a guia **Traveler** e configure as opções seguintes:

Table 16: Volume Encryption - Opções de Traveler

Opção	Descrição
Copy Traveler to device for the following users	Selecione os usuários que terão o Traveler instalado em suas máquinas. Use os botões **Add** e **Remove** para gerenciar os usuários selecionados.
Copy Traveler to device for everyone except the following users	Selecione os usuários que ficarão isentos da instalação do Traveler. Use os botões **Add** e **Remove** para gerenciar os usuários selecionados.

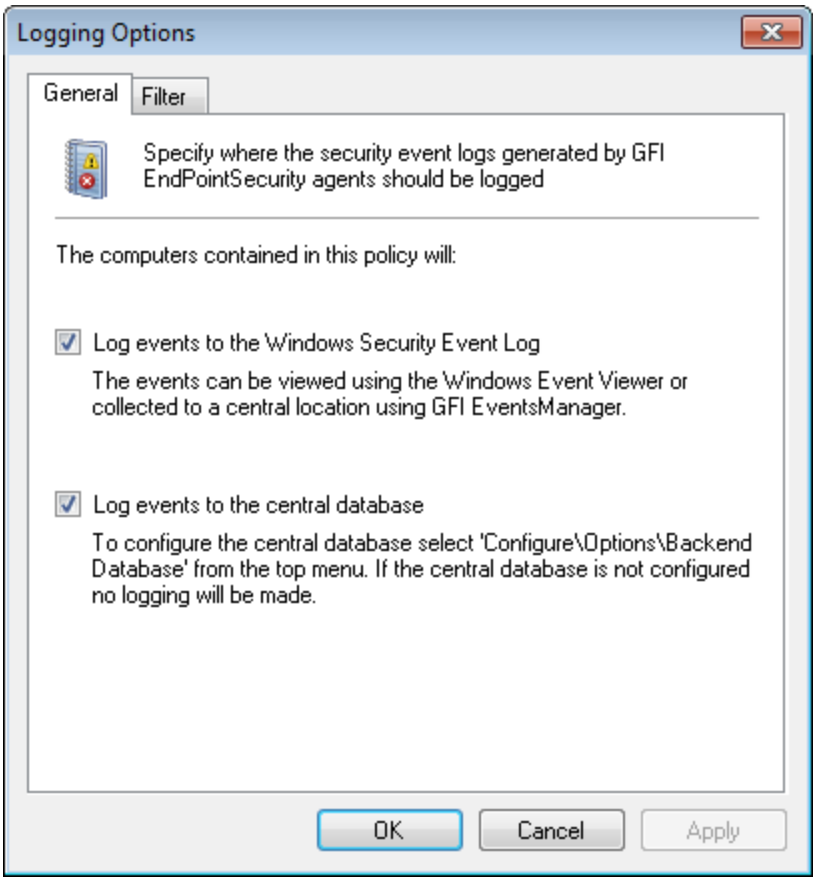
8. Clique em **Apply** e em **OK**.

6.16 Configurar o log de eventos

Os agentes do GFI EndPointSecurity registram eventos relacionados com tentativas de acessar dispositivos e portas de conexão em computadores de destino. Os agentes também registram eventos relacionados com operações de serviço. É possível especificar o local onde estes eventos devem ser armazenados, bem como quais os tipos de eventos que devem se registrados. É possível fazê-lo em uma base de política por política.

Para especificar opções de criação de logs para usuários em uma política de proteção:

1. Clique na guia **Configuration > Protection Policies**.
2. Em **Protection Policies > Security**, selecione a política de proteção a configurar.
3. A partir do painel direito, clique em **Set Logging Options** na seção **Logging and Alerting**.

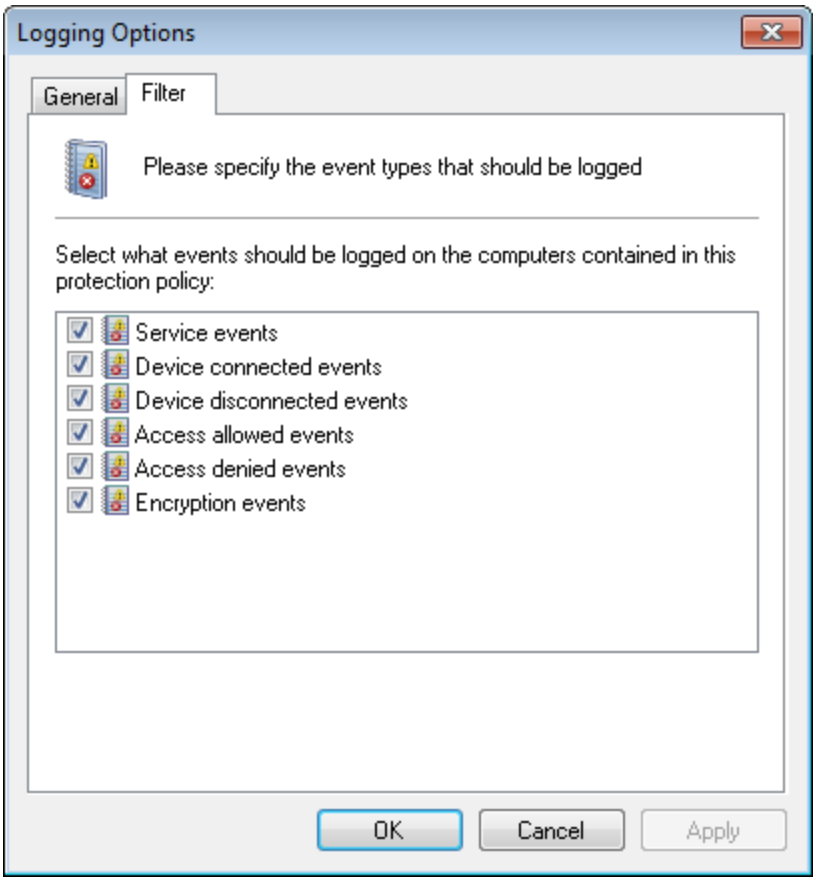


Screenshot 69: Logging Options - Guia General

4. Na caixa de diálogo **Logging Options** clique na guia **General**.
5. Habilitar ou desabilitar as localizações onde serão armazenados os eventos gerados por esta política de proteção:

Opção	Descrição
Log events to the Windows Security Event Log	É possível ver eventos por meio do Visualizador de Eventos do Windows de todos os computadores de destino ou por meio do GFI EventsManager após estes serem coletados em uma localização central.
Log events to the central database	É possível ver os eventos na subguia **Logs Browser** no console de gerenciamento do GFI EndPointSecurity. Esta opção requer a configuração de um banco de dados central. Para obter mais informações, consulte Gerenciar back-end do banco de dados (página 127).

Se ambas as opções se encontrarem habilitadas, é criado um log dos mesmos dados em ambas as localizações.



Screenshot 70: Logging Options - Guia Filter

6. Selecione a guia **Filter** e selecione qualquer um dos seguintes tipos de eventos para criar um log por esta política de proteção. Clique em **OK**.

Para implantar atualizações de políticas de proteção em computadores de destino especificados na política:

1. Clique na guia **Configuration** > **Computers**.
2. A partir de **Common tasks**, clique em **Deploy to all computers…**.

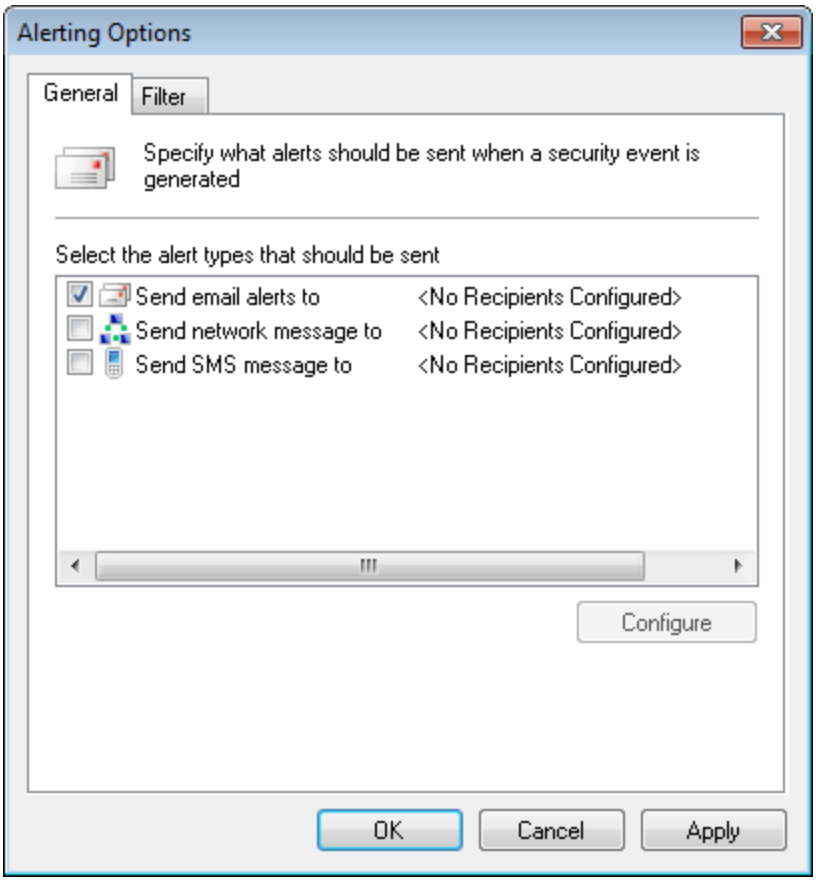
6.17 Configurar alertas

O GFI EndPointSecurity pode ser configurado para enviar alertas a destinatários especificados quando são gerados eventos em particular. É possível configurar alertas para serem enviados por meio de várias opções de alertas e também podem ser especificados tipos de eventos para os quais são enviados alertas. É possível fazê-lo em uma base de política por política.

Os destinatários de alertas não são usuários do Active Directory (AD) e/ou grupos de usuários, mas sim contas de perfil criadas pelo GFI EndPointSecurity para manter os detalhes de contato dos usuários que pretendem receber alertas. A melhor solução é criar destinatários de alertas antes de configurar os alertas. Para obter mais informações, consulte Configurar destinatários de alertas (página 137).

Para especificar opções de alertas para usuários em uma política de proteção:

1. Clique na guia **Configuration > Protection Policies**.
2. Em **Protection Policies > Security**, selecione a política de proteção a configurar.
3. A partir do painel direito, clique em **Alerting options** na seção **Logging and Alerting**.



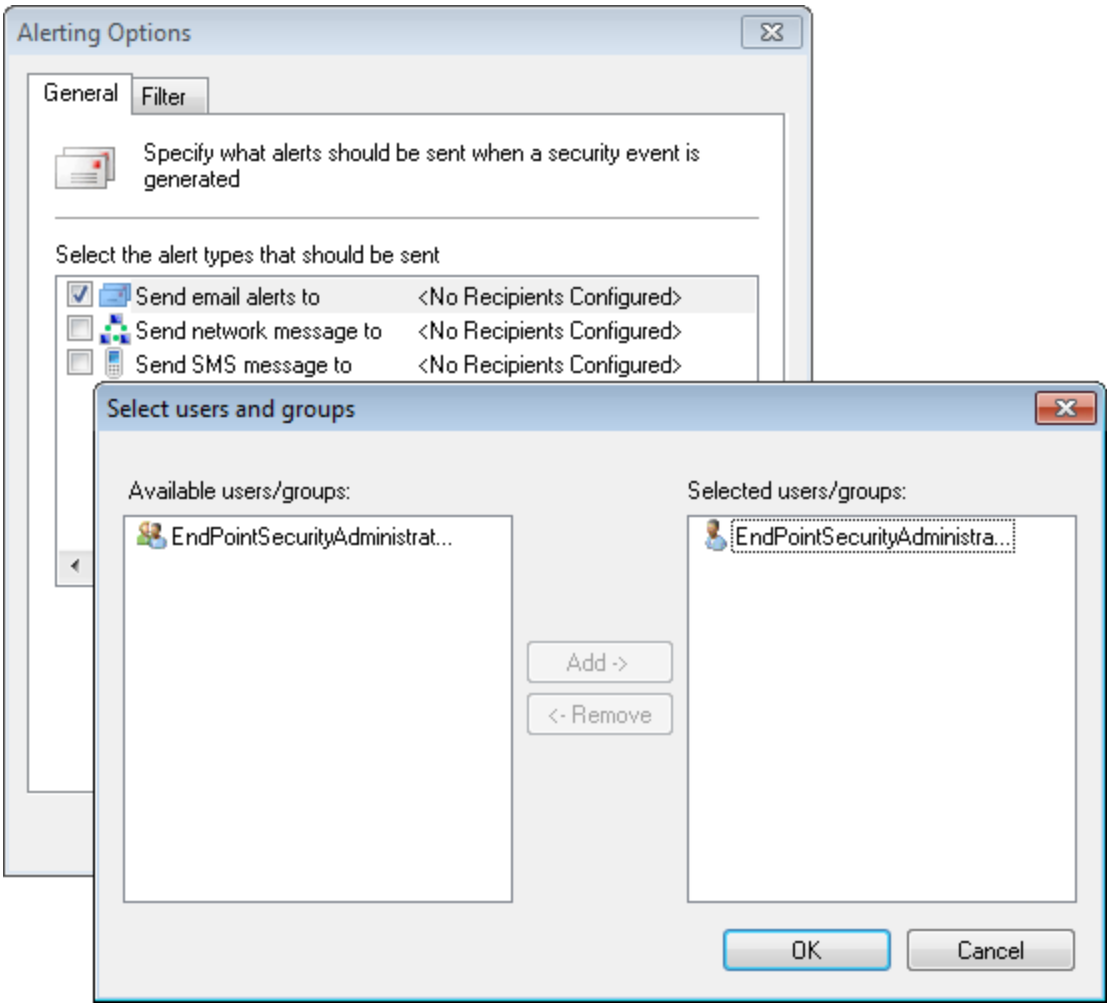
Screenshot 71: Alerting Options - Guia General

4. Na caixa de diálogo **Alerting Options**, clique na guia **General** e selecione qualquer um dos seguintes tipos de alertas a enviar:

» Alertas de email

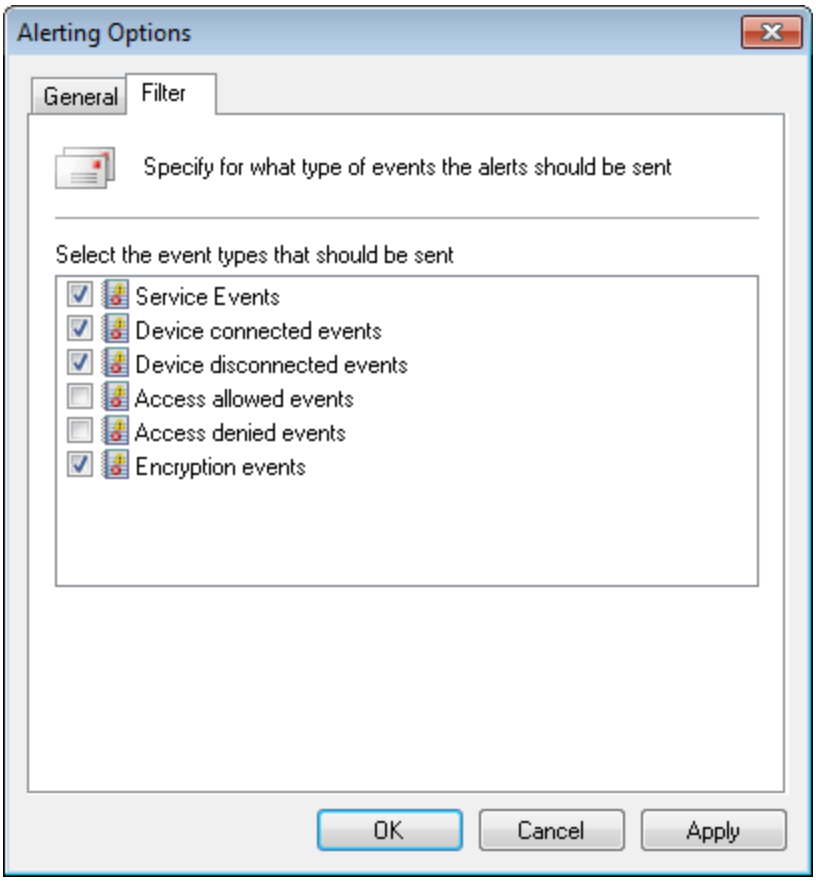
» Mensagens de rede

» Mensagens de SMS.



Screenshot 72: Alerting Options - Configurar usuários e grupos

5. Para cada tipo de alerta habilitado, assinale o tipo de alerta e clique em **Configure** para especificar os destinatários de alertas. Clique em **OK**.



Screenshot 73: Alerting Options - Guia Filter

6. Selecione a guia **Filter**, selecione qualquer um dos seguintes tipos de eventos para os quais são enviados alertas por esta política de proteção. Clique em **OK**.

Para implantar atualizações de políticas de proteção em computadores de destino especificados na política:

1. Clique na guia **Configuration** > **Computers**.
2. A partir de **Common tasks**, clique em **Deploy to all computers…**.

6.18 Configurar uma política como política padrão

O GFI EndPointSecurity fornece a possibilidade de definir a política de proteção que é atribuída a computadores de rede descobertos recentemente pelo recurso de implantação do agente. É possível fazê-lo em uma base de política por política.

Por padrão, o recurso de implantação do agente é definido para usar a política de proteção **General Control**, mas também é possível eleger qualquer outra política de proteção como a política padrão.

Para eleger outra política de proteção como a política de proteção padrão:

1. Clique na guia **Configuration > Protection Policies**.
2. Em **Protection Policies > Security**, selecione a política de proteção a configurar.
3. A partir do painel esquerdo, clique em **Set as default policy** na seção **Common tasks**.

7 Descobrir dispositivos

O GFI EndPointSecurity permite consultar de forma rápida e transparente pontos de extremidade de rede organizacionais, localizar e reportar todos os dispositivos que estão ou estiveram conectados aos computadores de destino verificados. O aplicativo identifica de forma granular dispositivos de ponto de extremidade conectados aos computadores de destino, tanto atualmente como historicamente, e exibe as informações detalhadas na tela assim que a verificação estiver concluída.

Use a guia **Scanning** para verificar computadores de destino e descobrir dispositivos conectados. Por padrão, o GFI EndPointSecurity verifica todas as categorias de dispositivos e portas de conectividade suportadas.

Um computador de destino descoberto pode ser qualquer computador na rede e não pode estar incluído em nenhuma política de proteção do GFI EndPointSecurity. A verificação do dispositivo deve ser executada em uma conta que possui privilégios administrativos sobre o(s) computador(es) de destino.

Tópicos neste capítulo

7.1 Executar uma verificação de dispositivos

Executar uma verificação de dispositivos é fundamental para descobrir novos dispositivos. O GFI EndPointSecurity permite buscar novos dispositivos que estão conectados a seu computador de destino. Isto permite adicionar novos dispositivos assim que estes são detectados no mesmo.

> **Obs.:**
>
> Foi apresentada uma nova política de segurança no Microsoft Vista, Microsoft Windows 7 e Microsoft Windows 2008 que necessita ser habilitada para que o verificador de dispositivos do GFI EndPointSecurity enumere os dispositivos físicos localizados na máquina.

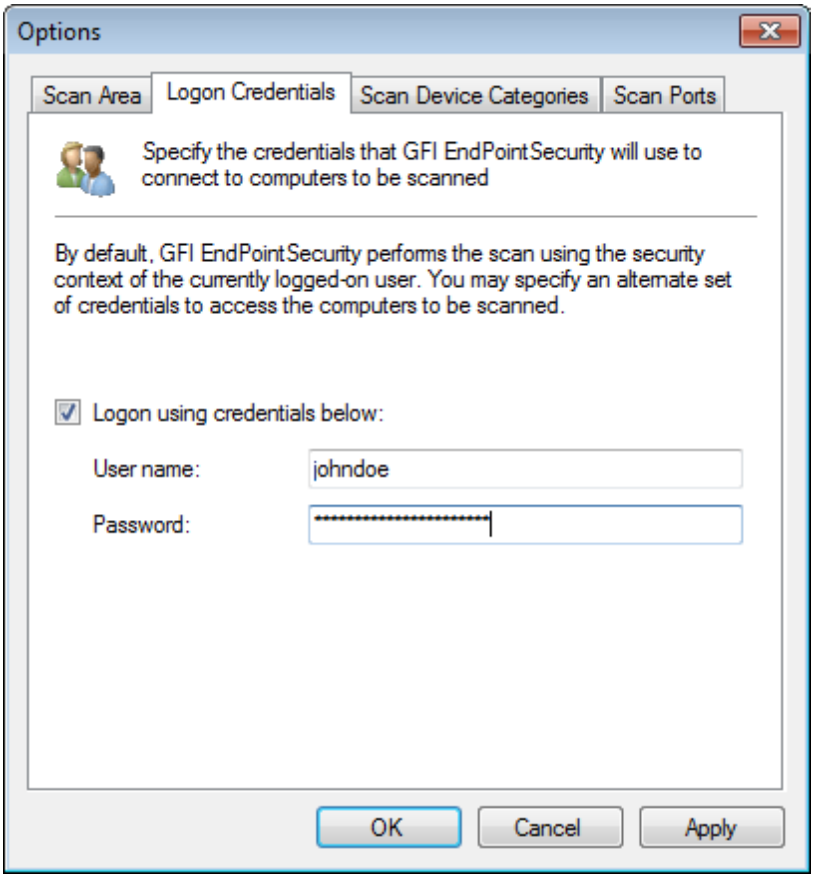
Para habilitar o acesso remoto à interface Plug and play:

1. Efetue o logon no computador com Microsoft Windows Vista, 7 ou Server 2008 com privilégios administrativos
2. Clique em **Start** > **Run**.
3. Digite **gpedit.msc**.
4. Navegue até **Computer Configuration** > **Administrative Templates** > **System** > **Device Installation**.
5. Clique com o botão direito do mouse em **Allow remote access to the PnP interface** e selecione **Properties**.
6. Na guia **Settings**, selecione a opção **Enable**.

7. Clique em **Ok** para salvar as alterações.
8. Reinicie o computador.

Para executar uma verificação do dispositivo:

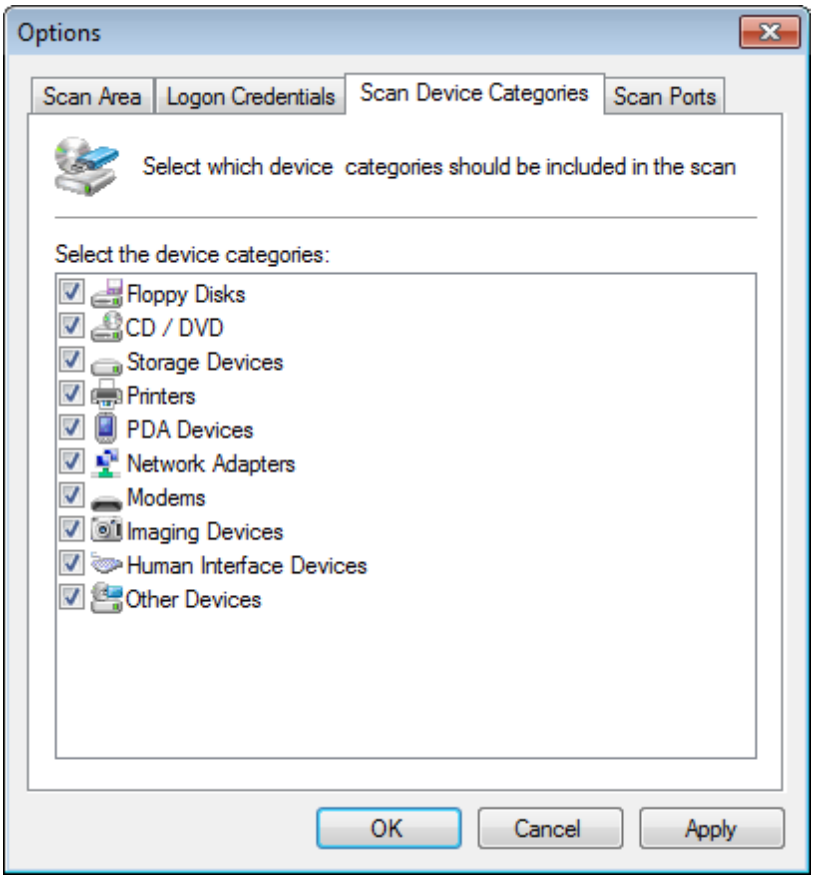
1. Clique na guia **Scanning**.
2. A partir de **Common tasks**, clique em **Options**.
3. A partir da caixa de diálogo **Options**, selecione a guia **Logon Credentials**.



Screenshot 74: Executar uma verificação de dispositivos - Guia Logon Credentials

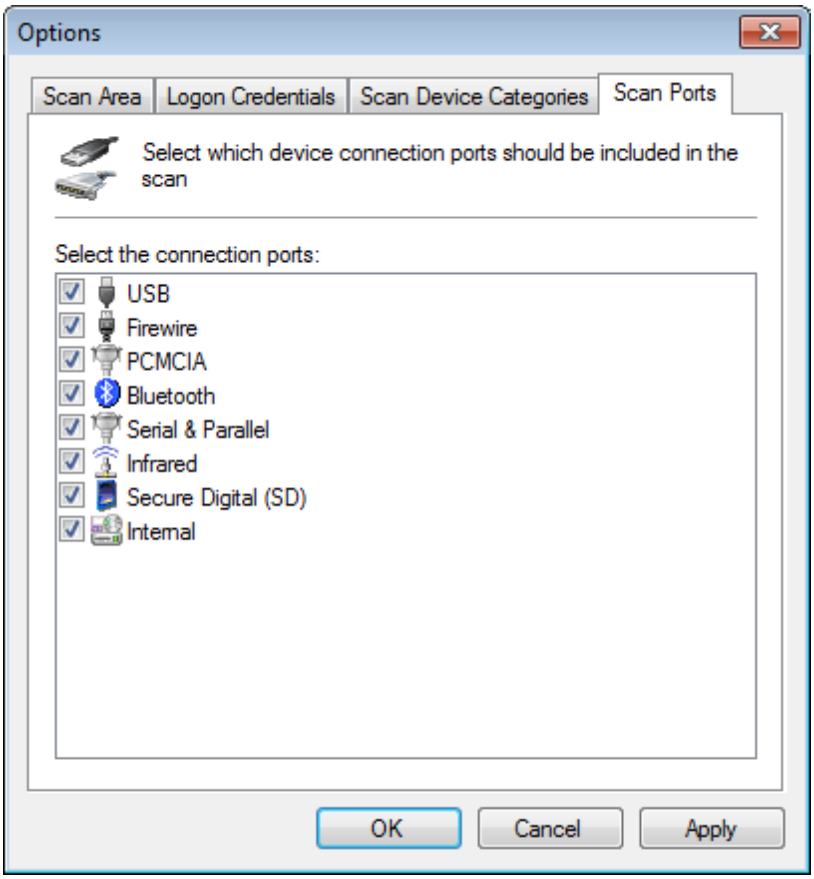
4. A partir da guia **Logon Credentials** da caixa de diálogo **Options**, marque/desmarque a opção **Logon using credentials below** para habilitar/desabilitar o uso de credenciais alternadas.

> **Obs.**
>
> Se não especificar quaisquer credenciais de logon, o GFI EndPointSecurity tenta efetuar logon no computador de destino usando o usuário com sessão iniciada no momento.



Screenshot 75: Executar uma verificação de dispositivos - Guia Scan Device Categories

5. Clique na guia **Scan Device Categories** e selecione as categorias do dispositivo que deseja incluir na verificação.



Screenshot 76: Executar uma verificação de dispositivos - Guia Scan Ports

6. Clique na guia **Scan Ports** e selecione as portas de conexão que deseja incluir na verificação.
7. Clique em **Apply** e em **OK**.
8. Para especificar a verificação nos computadores de destino:

» No painel direito, digite o nome do computador ou o endereço IP do(s) computador(es) de destino na caixa de texto **Scan target**. Clique em **New Scan** para iniciar a verificação no computador especificado.

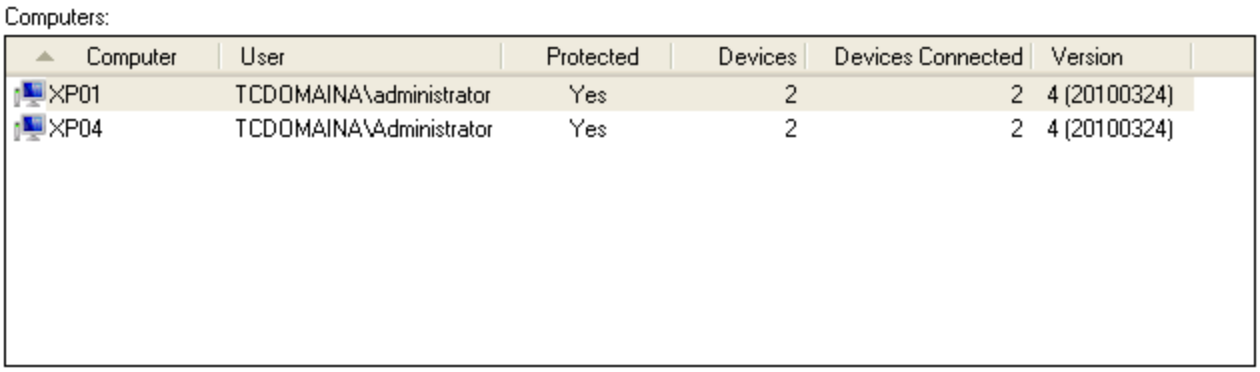
7.2 Analisar resultados de verificação de dispositivos

Os resultados da verificação de dispositivos são exibidos em duas seções:

» Computers

» Devices list.

7.2.1 Computers



Screenshot 77: Área de Computers

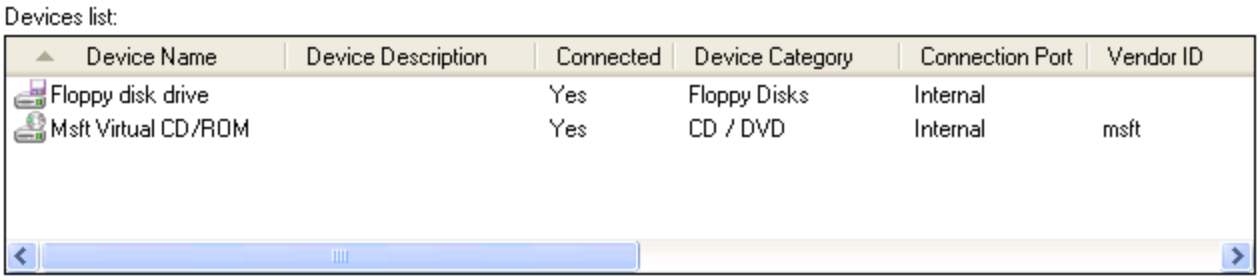
Esta seção exibe os resultados do resumo da verificação de dispositivos para cada computador de destino verificado, incluindo:

- O nome do computador/endereço IP
- O usuário com a sessão iniciada no momento
- Status de proteção, ou seja, se o computador está incluído em uma política de proteção do GFI EndPointSecurity
- O número total de dispositivos conectados no momento e historicamente
- Número de dispositivos conectados no momento.

Se um computador de destino verificado não estiver incluído em qualquer política de proteção do GFI EndPointSecurity, você pode escolher implantar uma política de proteção no computador. Para fazer isso:

1. Clique com o botão direito do mouse no nome/endereço IP do computador relevante na coluna **Computer** e selecione **Deploy agent(s)...**
2. Selecione a política de proteção a implantar. Clique em **Next** para continuar e em **Finish** para iniciar a implantação.

7.2.2 Devices list



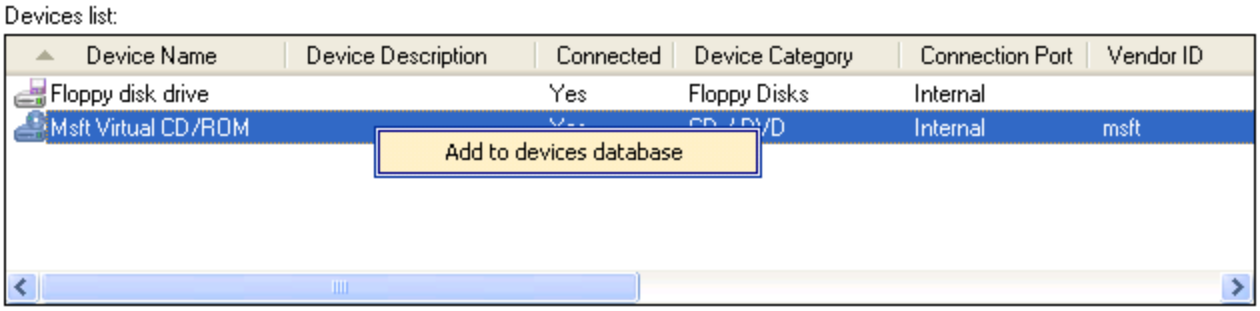
Screenshot 78: Área de Devices list

Esta seção exibe uma lista detalhada de dispositivos descobertos para cada computador verificado, incluindo:

- Nome, descrição e categoria do dispositivo
- Porta de conectividade
- Status de conexão, ou seja, se o dispositivo está conectado ou não no momento.

7.3 Adicionar dispositivos descobertos ao banco de dados

É possível selecionar um ou mais dispositivos descobertos a partir da lista **Devices** e adicioná-los ao banco de dados de dispositivos. Em seguida, estes dispositivos são recuperados deste banco de dados quando o GFI EndPointSecurity listar os dispositivos conectados no momento aos computadores de destino na lista de exclusão e na lista de permissão. Para obter informações, consulte Configurar a lista de exclusão do dispositivo ou Configurar a lista de permissão do dispositivo.



Screenshot 79: Área de Devices list - Adicionar dispositivo ao banco de dados de dispositivos

Para adicionar dispositivos ao banco de dados de dispositivos:

1. Selecione um ou mais dispositivos para adicionar ao banco de dados de dispositivos a partir da seção de lista **Devices**.
2. Clique com o botão direito do mouse nos dispositivos selecionados e selecione **Add to devices database**.
3. Clique em **OK**.

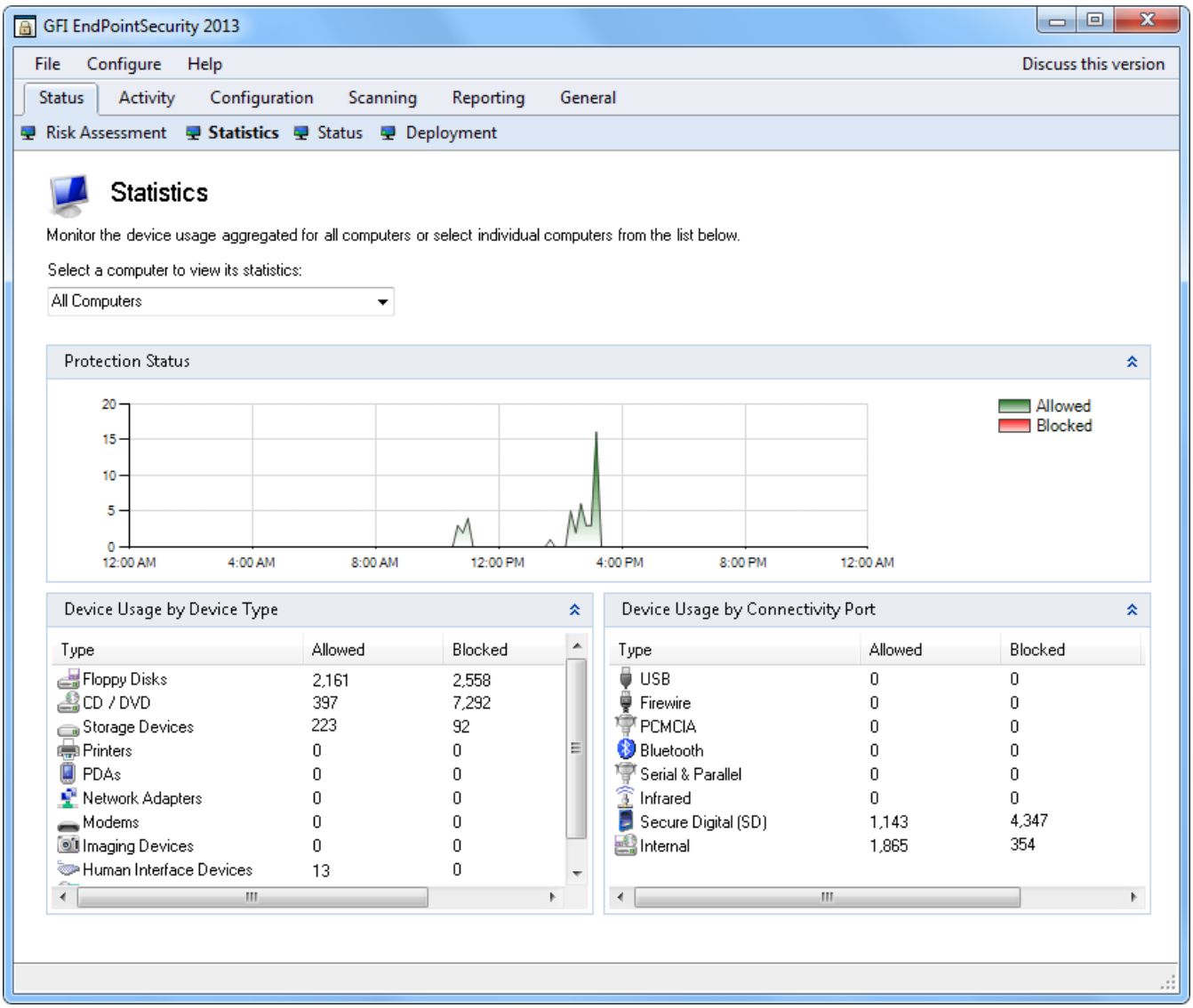
8 Monitorar a atividade de uso do dispositivo

Este capítulo fornece informações sobre como monitorar a atividade de seus dispositivos de rede. O GFI EndPointSecurity permite manter uma trilha de auditoria de todos os eventos gerados pelos Agentes do GFI EndPointSecurity implantados nos computadores de rede. Para realizar a manutenção de uma trilha de auditoria, você deverá habilitar os logs. Para obter mais informações, consulte Configurar o log de eventos (página 95).

Tópicos neste capítulo

8.1 Estatística

Use a subguia Statistics para exibir as tendências diárias de atividade do dispositivo e estatística para um computador específico ou para todos os computadores de rede.



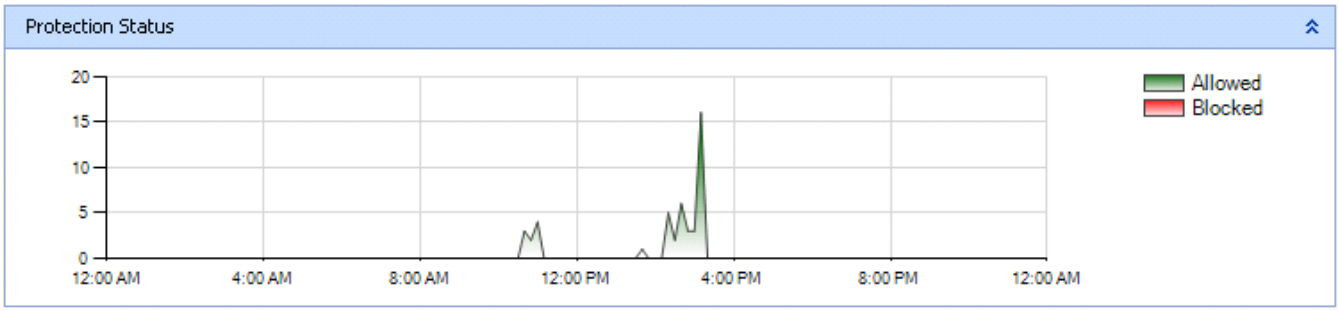
Screenshot 80: Subguia Statistics

Para acessar a subguia Risk Assessment, a partir do console de gerenciamento do GFI EndPointSecurity, clique na guia **Status > Statistics**.

A seção **Statistics** contém informações sobre:

- Status de proteção
- Uso do dispositivo por tipo de dispositivo
- Uso do dispositivo por porta de conectividade

8.1.1 Status de proteção



Screenshot 81: Área Protection Status

Esta seção representa graficamente o uso diário do dispositivo em computadores, diferenciando entre dispositivos que foram bloqueados e dispositivos que foram permitidos pelos agentes. As informações fornecidas podem ser filtradas para um computador específico ou para todos os computadores de rede.

8.1.2 Uso do dispositivo por tipo de dispositivo

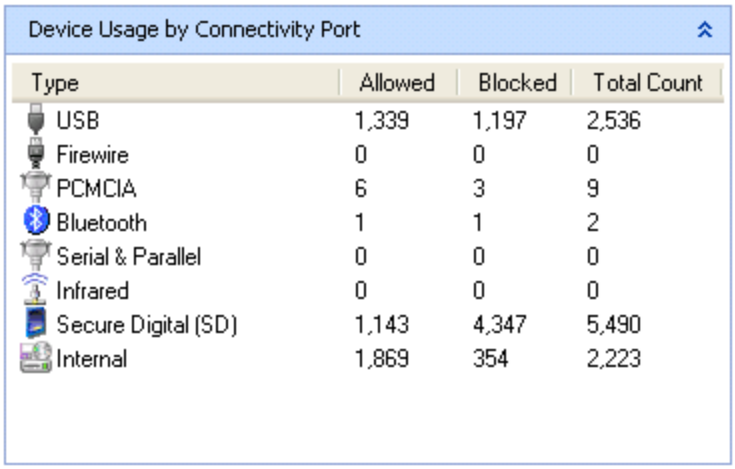
Device Usage by Device Type

Type	Allowed	Blocked	Total Count
Floppy Disks	2	88	90
CD / DVD	2,161	397	2,558
Storage Devices	1,939	5,353	7,292
Printers	11	5	16
PDAs	10	7	17
Network Adapters	16	13	29
Modems	6	5	11
Imaging Devices	5	7	12
Human Interface Devices	4	4	8
Other Devices	200	23	223

Screenshot 82: Área Device Usage by Device Type

Esta seção enumera tentativas de conexão de dispositivo por tipo de dispositivo, que foram permitidas ou bloqueadas. As informações fornecidas podem ser filtradas para um computador específico ou para todos os computadores de rede.

8.1.3 Uso do dispositivo por porta de conectividade



Type	Allowed	Blocked	Total Count
USB	1,339	1,197	2,536
Firewire	0	0	0
PCMCIA	6	3	9
Bluetooth	1	1	2
Serial & Parallel	0	0	0
Infrared	0	0	0
Secure Digital (SD)	1,143	4,347	5,490
Internal	1,869	354	2,223

Screenshot 83: Área Device Usage by Connectivity Port

Esta seção enumera tentativas de conexão de dispositivo por porta de conectividade, que foram permitidas ou bloqueadas. As informações fornecidas podem ser filtradas para um computador específico ou para todos os computadores de rede.

8.2 Atividade

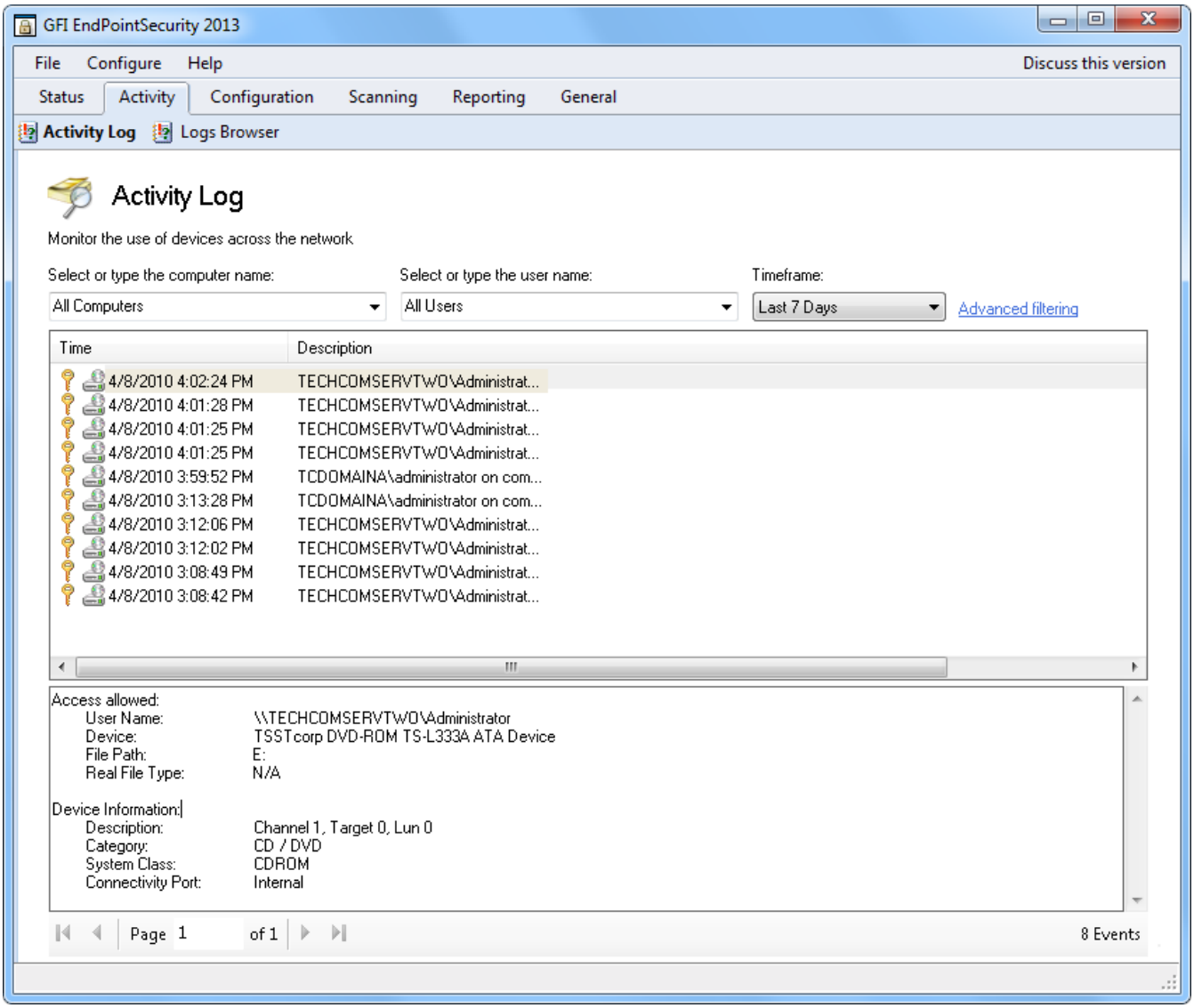
Use a guia Activity para monitorar o uso do dispositivo na rede e os eventos registrados de um computador em específico ou de todos os computadores de rede.

A seção Activity contém informações sobre:

- Log de atividade
- Filtragem avançada
- Navegador de logs
- Criar consultas de eventos

8.2.1 Log de atividade

Esta subguia permite monitorar os dispositivos em uso na rede. Selecione o computador e/ou o usuário a partir das listas suspensas relevantes para filtrar a lista Activity Log por computador e/ou por usuário. Além disso, esta guia permite filtrar ainda mais a lista por meio dos filtros de hora fornecidos.



Screenshot 84: Subguia Activity Log

Para acessar a subguia Activity Log, a partir do console de gerenciamento do GFI EndPointSecurity clique na guia **Activity > Activity Log**.

Para exibir mais detalhes sobre um evento em particular, clique no evento. São exibidas informações adicionais no painel de descrição de eventos na parte inferior da subguia.

Para personalizar a subguia Activity Log para se adequar às necessidades da sua empresa, clique com o botão direito do mouse no cabeçalho e selecione as colunas que devem ser adicionadas ou removidas da exibição.

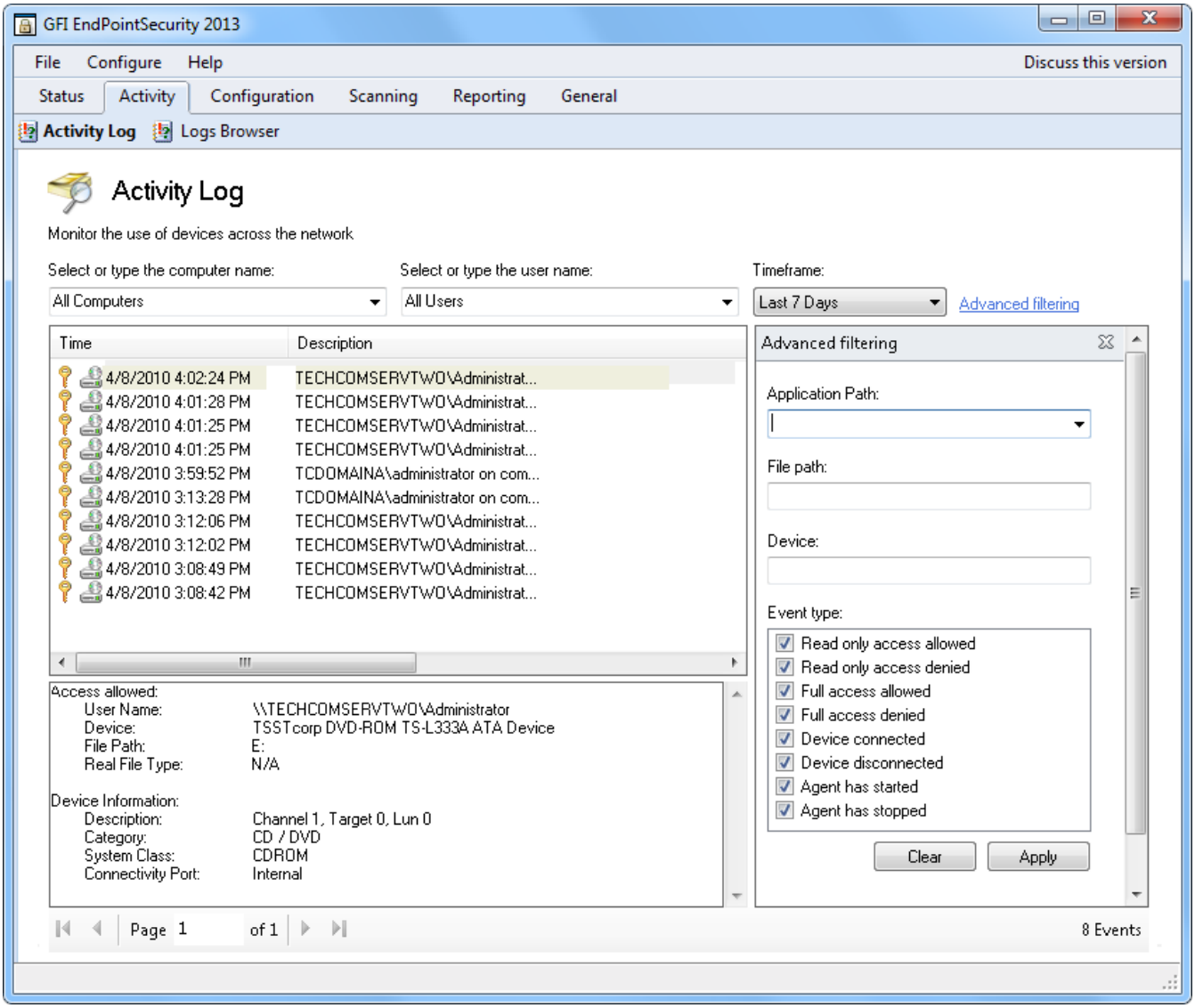
Para alterar a posição da coluna, selecione o cabeçalho da coluna, arraste e largue-o na posição necessária.

8.2.2 Filtragem avançada

Este recurso permite filtrar ainda mais os logs de histórico do uso do dispositivo usando um ou mais critérios do conjunto seguinte:

- Caminho do aplicativo
- Caminho do arquivo

- Dispositivo
- Tipo de evento.



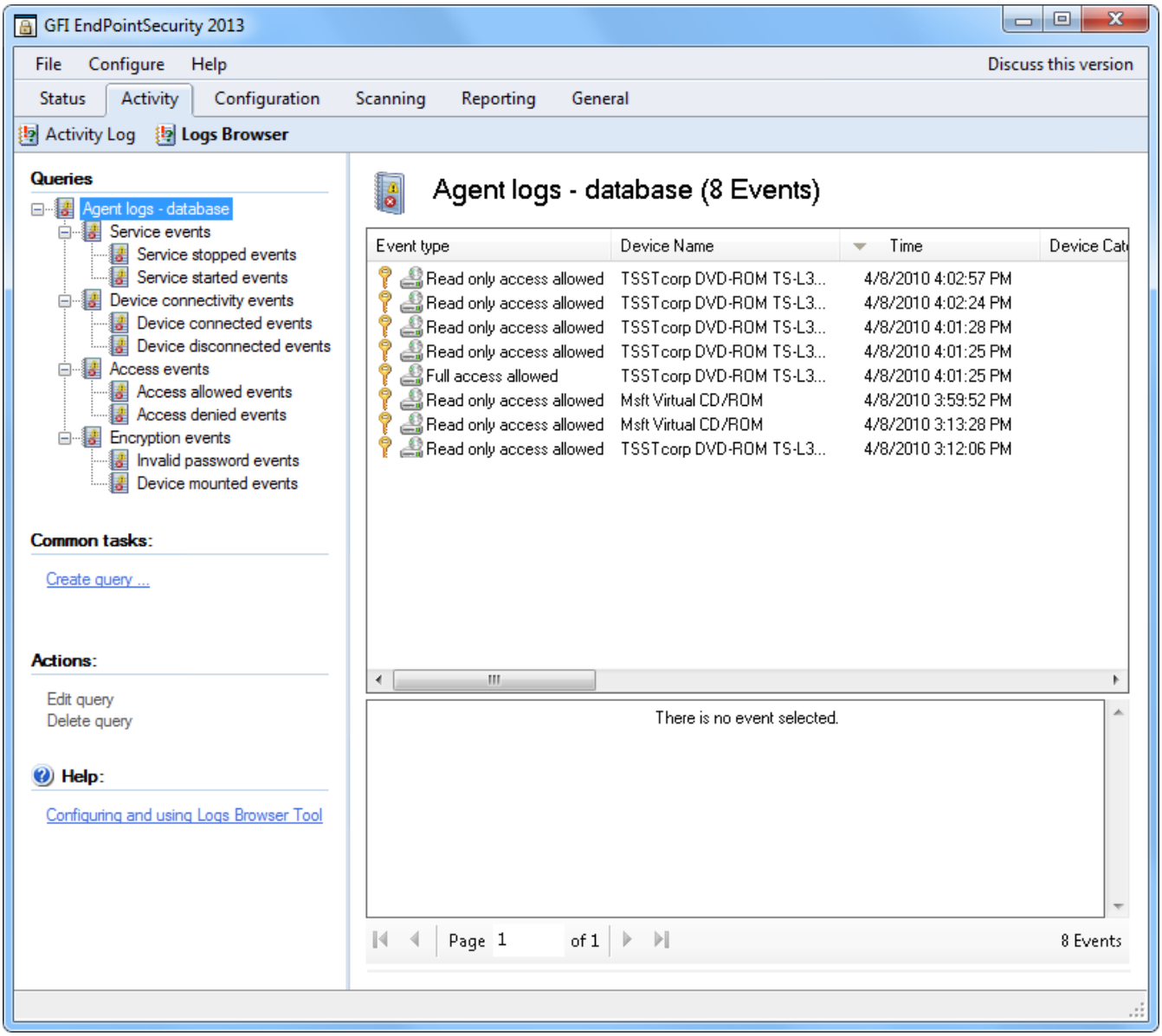
Screenshot 85: Subguia Activity Log - Advanced filtering

Para acessar as opções de filtragem avançada do Activity Log, clique em **Advanced filtering** na subguia **Activity Log**.

8.2.3 Navegador de logs

A subguia Logs Browser permite acessar e procurar eventos armazenados no momento no back-end do banco de dados.

O GFI EndPointSecurity inclui também um construtor de consultas para simplificar a pesquisa de eventos específicos. Com o construtor de consultas é possível criar filtros personalizados que filtram dados de eventos e exibem somente as informações que você necessita procurar, sem excluir registros do back-end do banco de dados.



Screenshot 86: Subguia Logs Browser

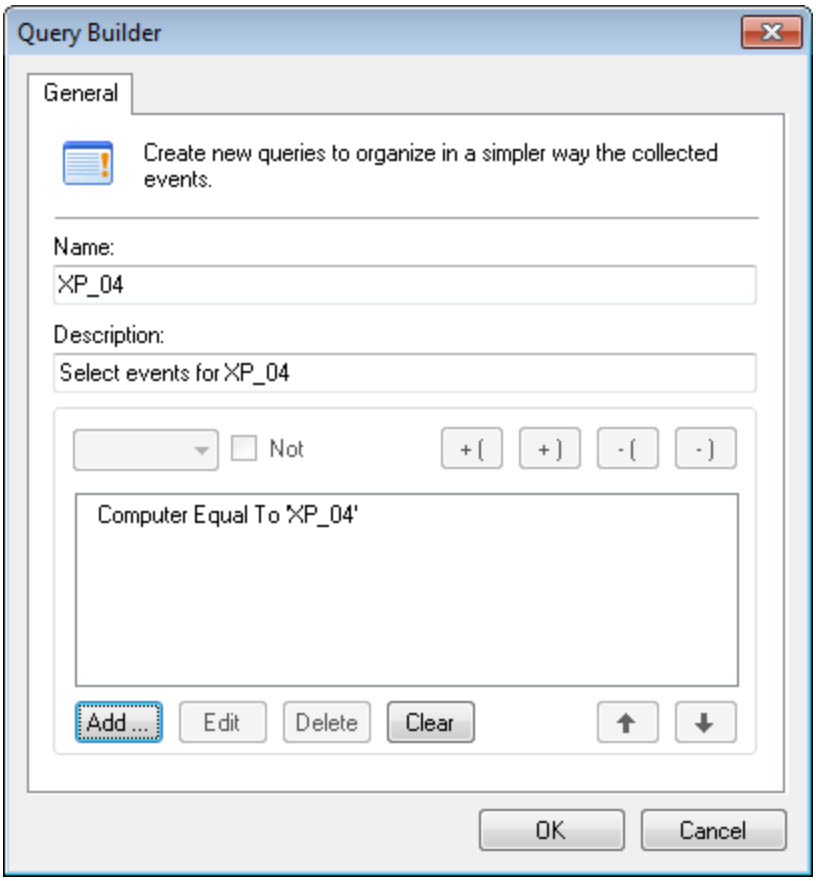
Para acessar a subguia Logs Browser, a partir do console de gerenciamento a partir do GFI EndPointSecurity, clique na guia **Activity > Logs Browser**.

Para exibir mais detalhes sobre um evento em particular, clique no evento. São exibidas informações adicionais no painel de descrição de eventos na parte inferior da subguia.

8.2.4 Criar consultas de eventos

Para criar consultas de eventos personalizadas:

1. A partir do console de gerenciamento do GFI EndPointSecurity, clique na guia **Activity**.
2. Clique na subguia **Logs Browser**.
3. No painel esquerdo, clique com o botão direito do mouse no nó **Agent logs - database** e selecione **Create query…**.



Screenshot 87: Opções de Query Builder

4. Na caixa de diálogo **Query Builder**, especifique um nome e uma descrição para a nova consulta.
5. Clique em **Add…**, configure a(s) condição(ões) de consulta necessária(s) e clique em **OK**. Repita até que todas as condições de consulta necessárias tenham sido especificadas.
6. Clique em **OK** para finalizar suas configurações. A consulta personalizada é adicionada como um subnó no nó **Agent logs - database**.

Obs.

É também possível filtrar os resultados das consultas de eventos existentes criando subconsultas mais específicas. Para isso, clique com o botão direito do mouse em uma consulta e selecione **Create query…**.

9 Monitorar status

Este capítulo fornece informações relacionadas com o monitoramento do status do GFI EndPointSecurity, bem como o status dos agentes GFI EndPointSecurity. A exibição de status fornece informações gráficas e estatísticas relacionadas com o uso do dispositivo.

Tópicos neste capítulo

9.1 Exibição da avaliação do risco

Use a subguia Risk Assessment para exibir o status de:

- Nível de avaliação do risco nos computadores de rede com agentes GFI EndPointSecurity neles instalados.
- Agentes do GFI EndPointSecurity implantados nos computadores de rede.
- Uso do dispositivo, como o número e a porcentagem de dispositivos bloqueados e o número de dispositivos permitidos.
- Nível de ameaça dos dispositivos na rede.

Screenshot 88: Subguia Risk Assessment

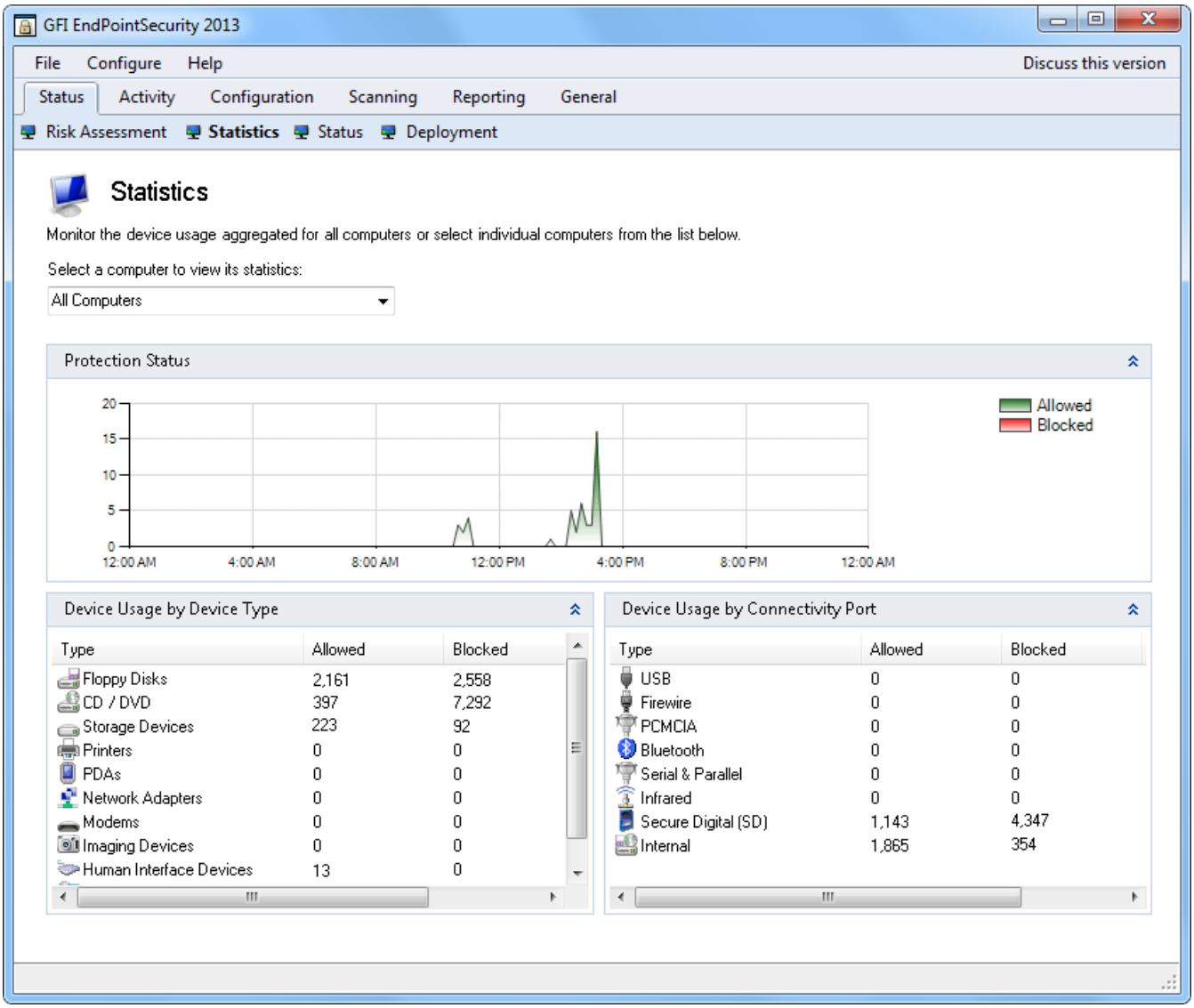
Para acessar a subguia Risk Assessment a partir do console de gerenciamento do GFI EndPointSecurity, clique na guia **Status > Risk Assessment**.

Recurso	Descrição
1	Esta seção mostra: » Os resultados da avaliação do risco exibidos na medição dos computadores de rede. » A opção para verificar novamente a rede e obter os resultados de avaliação do risco mais recentes. » A hora da última avaliação do risco.

Recurso	Descrição
2	Esta seção lista os valores acumulados do número de: » Pontos de extremidade verificados » Verificações bem-sucedidas » Pontos de extremidade protegidos » Pontos de extremidade desprotegidos » Dispositivos descobertos Esta seção também apresenta: » A rede onde os agentes estão instalados » A hora e a data da última avaliação do risco.
3	Esta seção representa graficamente o número de agentes que estão de momento: » A aguardar a instalação em computadores de rede » Protegido por GFI EndPointSecurity » Não protegido por GFI EndPointSecurity
4	Esta seção representa todos os agentes implantados nos computadores de rede, diferenciando aqueles atualmente online daqueles que estão offline. Para obter mais informações, consulte Exibição do status (página 118).
5	Esta seção representa graficamente os níveis de porcentagem de ameaça do dispositivo como registrado pelos agentes dos computadores de rede que têm o GFI EndPointSecurity instalado.
6	Esta seção representa graficamente as porcentagens de acessos de usuário por categoria do dispositivo da quantidade acumulada total de acessos do usuário a dispositivos, como registrados pelos agentes. Acessos do usuário a dispositivos referem-se a acessos a dispositivos permitidos e bloqueados.
7	Esta seção lista: » A conta do usuário em que o serviço doGFI EndPointSecurity está sendo executado. » O nível do fator de risco. » O atual status da criptografia no ponto de extremidade. » O status do recurso de verificação do tipo de arquivo. » O status do recurso de verificação do conteúdo.

9.2 Exibição de estatística

Use a subguia Statistics para exibir as tendências diárias de atividade do dispositivo e estatística para um computador específico ou para todos os computadores de rede.



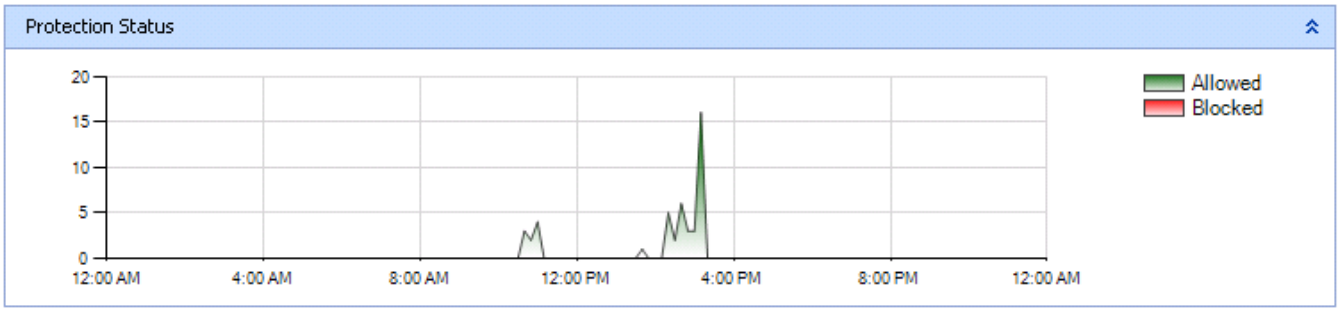
Screenshot 89: Subguia Statistics

Para acessar a subguia Risk Assessment, a partir do console de gerenciamento do GFI EndPointSecurity, clique na guia **Status > Statistics**.

A seção **Statistics** contém informações sobre:

- Status de proteção
- Uso do dispositivo por tipo de dispositivo
- Uso do dispositivo por porta de conectividade

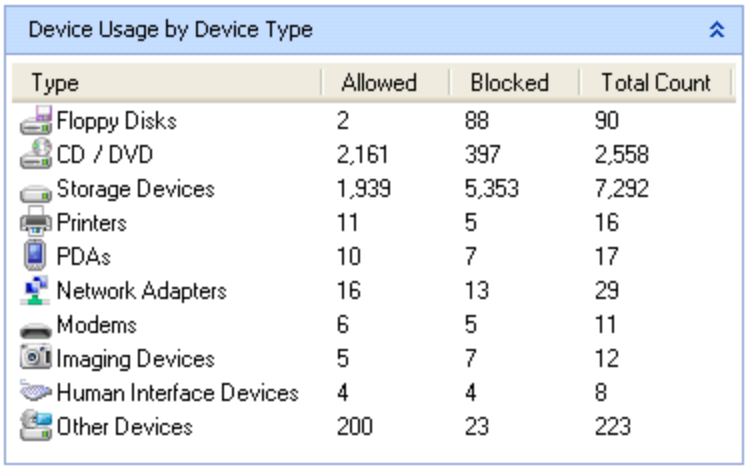
9.2.1 Status de proteção



Screenshot 90: Área Protection Status

Esta seção representa graficamente o uso diário do dispositivo em computadores, diferenciando entre dispositivos que foram bloqueados e dispositivos que foram permitidos pelos agentes. As informações fornecidas podem ser filtradas para um computador específico ou para todos os computadores de rede.

9.2.2 Uso do dispositivo por tipo de dispositivo

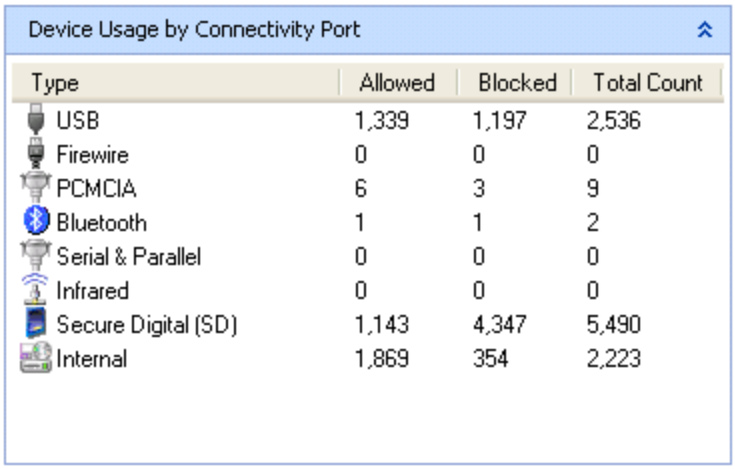

Device Usage by Device Type

Type	Allowed	Blocked	Total Count
Floppy Disks	2	88	90
CD / DVD	2,161	397	2,558
Storage Devices	1,939	5,353	7,292
Printers	11	5	16
PDAs	10	7	17
Network Adapters	16	13	29
Modems	6	5	11
Imaging Devices	5	7	12
Human Interface Devices	4	4	8
Other Devices	200	23	223

Screenshot 91: Área Device Usage by Device Type

Esta seção enumera tentativas de conexão de dispositivo por tipo de dispositivo, que foram permitidas ou bloqueadas. As informações fornecidas podem ser filtradas para um computador específico ou para todos os computadores de rede.

9.2.3 Uso do dispositivo por porta de conectividade


Device Usage by Connectivity Port

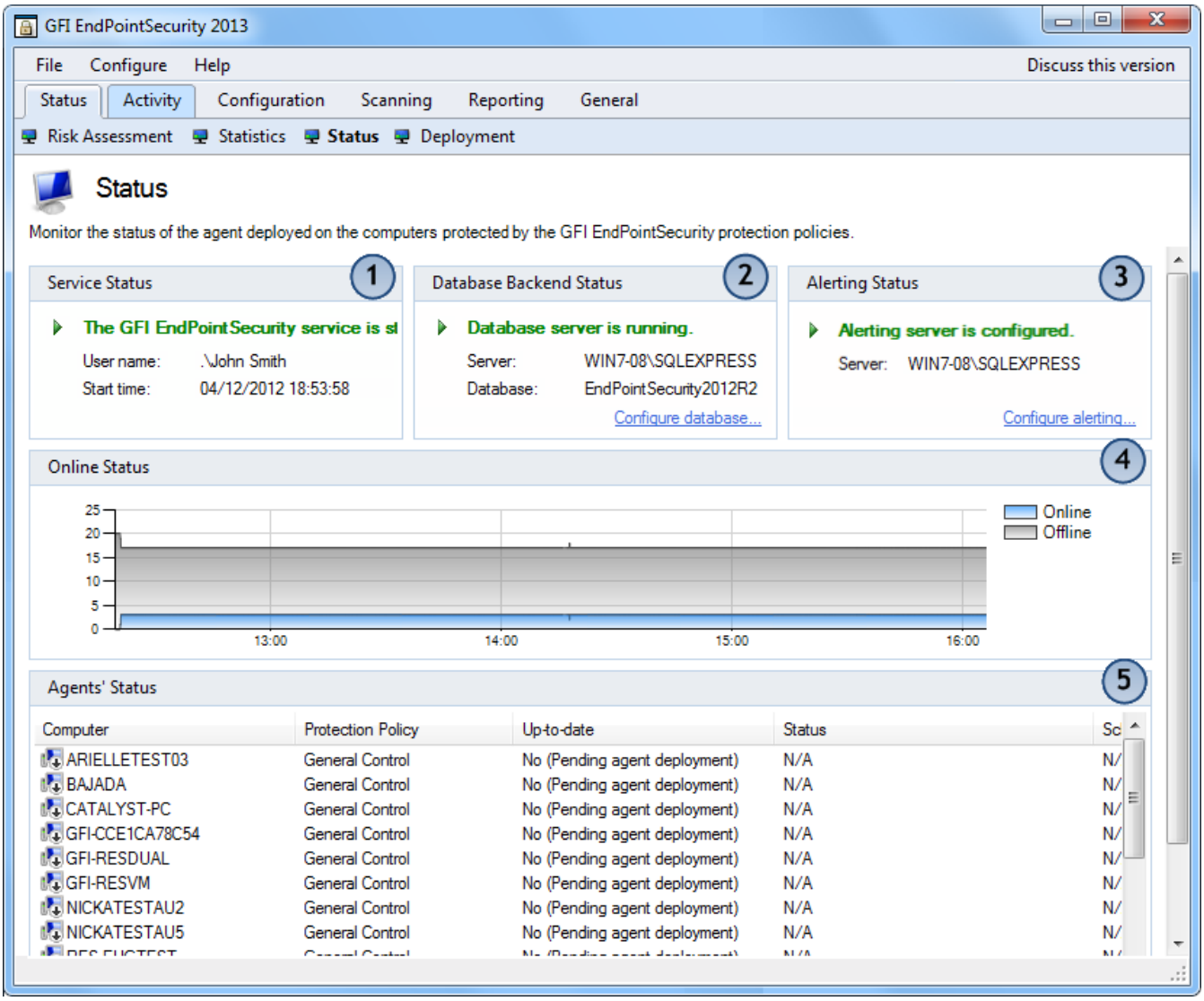
Type	Allowed	Blocked	Total Count
USB	1,339	1,197	2,536
Firewire	0	0	0
PCMCIA	6	3	9
Bluetooth	1	1	2
Serial & Parallel	0	0	0
Infrared	0	0	0
Secure Digital (SD)	1,143	4,347	5,490
Internal	1,869	354	2,223

Screenshot 92: Área Device Usage by Connectivity Port

Esta seção enumera tentativas de conexão de dispositivo por porta de conectividade, que foram permitidas ou bloqueadas. As informações fornecidas podem ser filtradas para um computador específico ou para todos os computadores de rede.

9.3 Exibição do status

Use a subguia Status para determinar o status de todas as operações de implantação realizadas pelos destinos de rede. Para cada computador de destino, as informações exibidas mostram:



Screenshot 93: Subguia Status

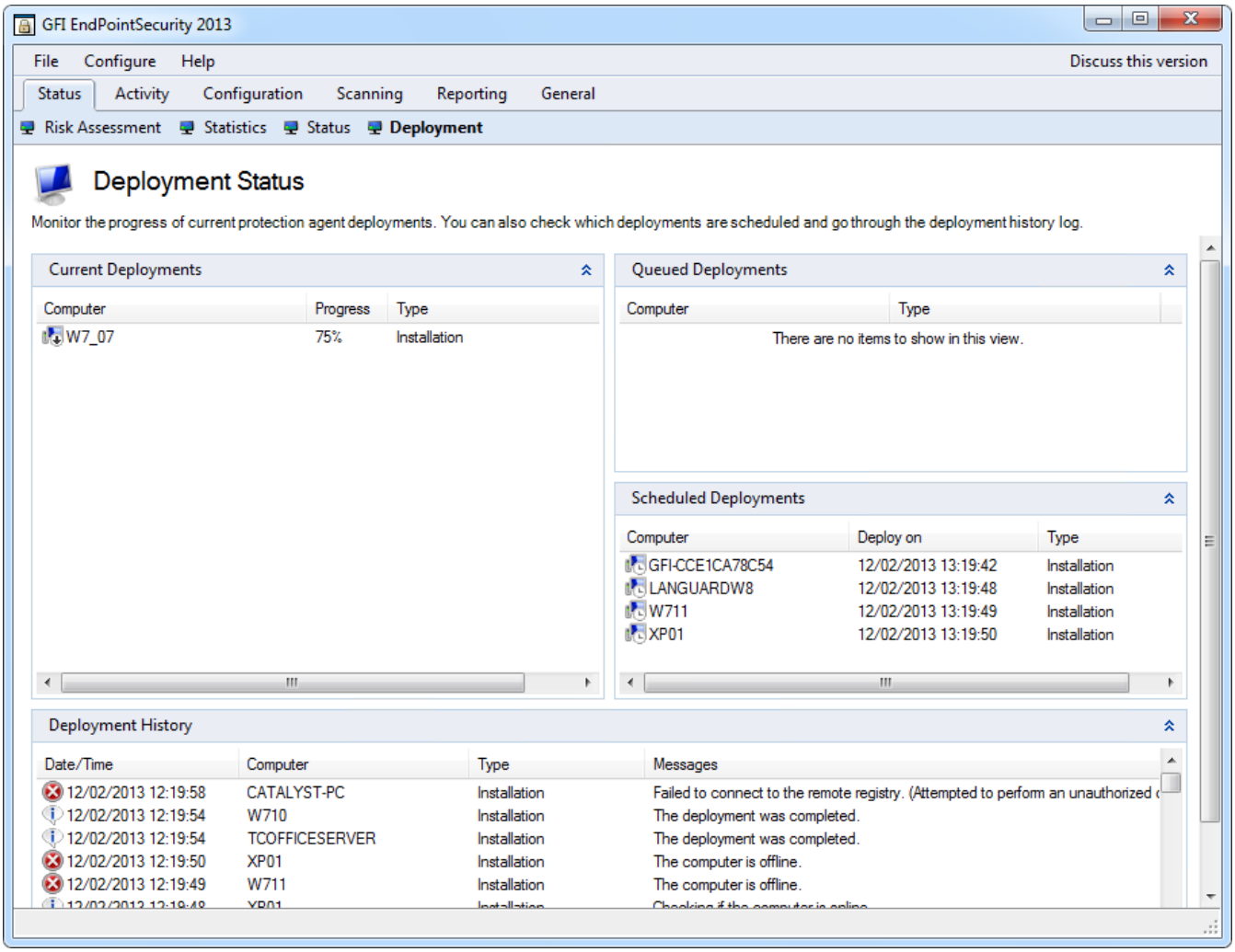
Recurso	Descrição
1	Esta seção lista: » O status operacional do serviço do console de gerenciamento GFI EndPointSecurity. » A conta do usuário em que o serviço doGFI EndPointSecurity está sendo executado. » A hora em que o serviço foi iniciado pela última vez.
2	Esta seção lista: » O status operacional do servidor de banco de dados atualmente em uso pelo GFI EndPointSecurity. » O nome ou endereço IP do servidor de banco de dados atualmente usado pelo GFI EndPointSecurity. » O nome do banco de dados onde está arquivando eventos do GFI EndPointSecurity. Para modificar qualquer configuração atual do banco de dados, clique em **Configure database...**. Esta ação inicia a caixa de diálogo **Database Backend**. Para obter mais informações, consulte Gerenciar back-end do banco de dados (página 127).
3	Esta seção lista: » O status operacional do servidor de alerta atualmente usado pelo GFI EndPointSecurity. » O nome ou endereço IP do servidor de alerta atualmente usado pelo GFI EndPointSecurity. Para modificar qualquer configuração relacionada com os alertas atuais, clique em **Configure alerting...**. Esta ação inicia a caixa de diálogo **Alerting Options**. Para obter mais informações, consulte Configurar alertas (página 97).

Recurso	Descrição
4	Esta seção representa graficamente todos os agentes implantados nos computadores de rede, diferenciando entre aqueles atualmente online e offline.
5	Esta seleção lista: » Nome do computador de destino e política de proteção aplicável. » O status do agente do GFI EndPointSecurity, atualmente implantado e atualizado ou aguardando implantação. » O status do computador de destino, atualmente online ou offline. Para implantar agentes pendentes: 1. Selecione um ou mais computadores a partir de **Agents' Status**. 2. Clique com o botão direito do mouse nos computadores selecionados e selecione **Deploy selected agent(s)** ou **Schedule deployment for selected agent(s)...**. 3. Clique em **OK**. **Obs.** Se um computador de destino se encontrar offline, a implantação terá a diferença de uma hora. O GFI EndPointSecurity tenta implantar essa política a cada hora, até o computador de destino estar de novo online. **Obs.** Cada agente envia seu status online para o GFI EndPointSecurity regularmente. Se estes dados não forem recebidos pelo aplicativo principal, o agente é considerado offline.

9.4 Vista do status de implantação

- Sobre a vista do status de implantação
- Implantações atuais
- Implantações em fila
- Implantações agendadas
- Histórico de implantações

9.4.1 Sobre a vista do status de implantação



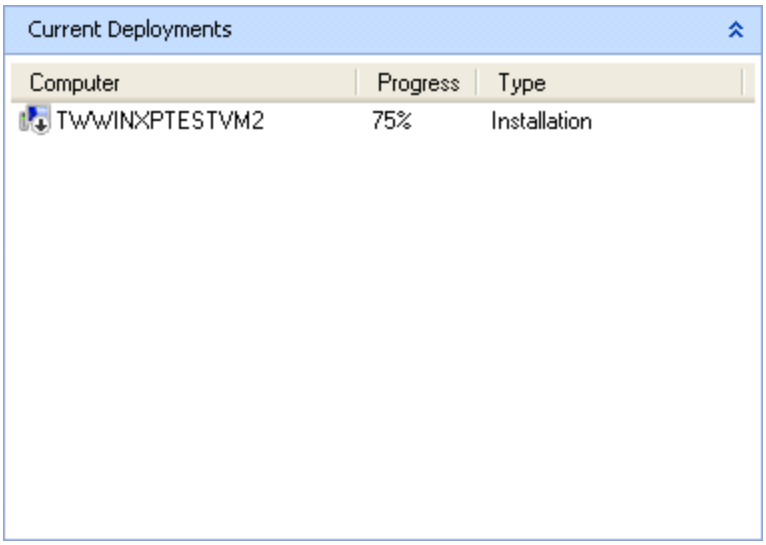
Screenshot 94: Subguia Deployment

Use a subguia Deployment para ver:

- Atividade da implantação atual
- Implantações em fila
- Implantações agendadas
- Histórico de implantações.

Para acessar a subguia Deployment, a partir do console de gerenciamento do GFI EndPointSecurity, clique na guia **Status > Deployment**.

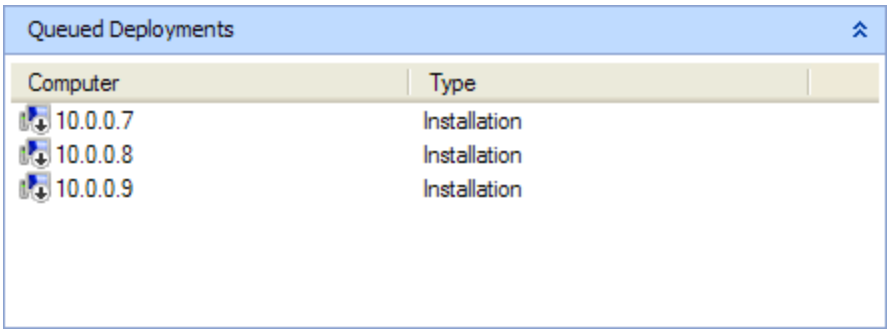
9.4.2 Implantações atuais



Screenshot 95: Área Current Deployments

Esta seção exibe uma lista de implantações que estão ocorrendo no momento. A informação fornecida inclui o nome do computador, o progresso de implantação e o tipo de implantação. A implantação é uma instalação, desinstalação ou atualização.

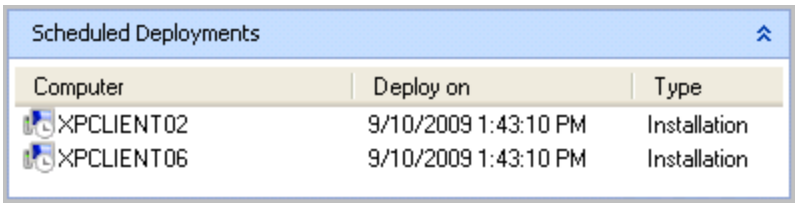
9.4.3 Implantações em fila



Screenshot 96: Área Queued Deployments

Esta seção exibe uma lista de implantações pendentes. A informação fornecida inclui o nome do computador e o tipo de implantação.

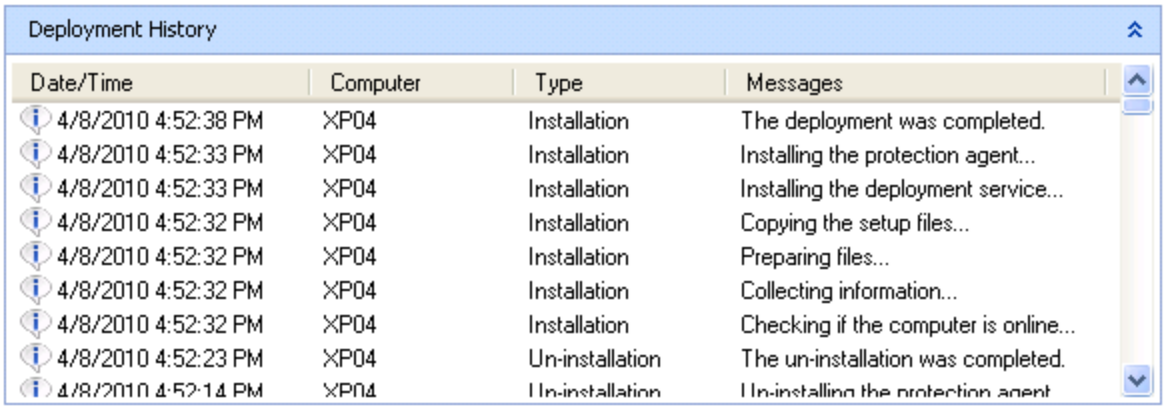
9.4.4 Implantações agendadas



Screenshot 97: Área Scheduled Deployments

Esta seção exibe uma lista de implantações agendadas. A informação fornecida inclui o nome do computador, a hora agendada e o tipo de implantação.

9.4.5 Histórico de implantações



Screenshot 98: Área Deployment History

Esta seção exibe uma trilha de auditoria para todos os estágios de todas as implantações de agentes ou políticas de proteção realizadas pelo GFI EndPointSecurity. As informações fornecidas incluem o carimbo de data/hora de cada entrada do log, o nome do computador, o tipo de implantação, bem como as mensagens de erro e de informação geradas durante o processo de implantação. Para obter mais informações, consulte Solução de problemas e suporte (página 149).

Para remover as entradas de log exibidas, clique com o botão direito do mouse na área **Deployment History** e selecione **Clear all messages**.

10 Relatórios

O GFI EndPointSecurityGFI ReportPack é um suplemento de relatórios integralmente desenvolvido para GFI EndPointSecurity. Este pacote de relatórios pode ser agendado para gerar automaticamente relatórios de nível IT gráfico e gerenciamento baseados em dados coletados pelo GFI EndPointSecurity, dando a você a capacidade de incluir no relatório dispositivos conectados à rede, tendências de uso do dispositivo pela máquina ou pelo usuário, arquivos copiados para e de dispositivos (incluindo nomes reais dos arquivos copiados) e muito mais.

Tópicos neste capítulo

10.1 GFI EndPointSecurity GFI ReportPack

Para gerar relatórios, necessita de baixar e instalar o suplemento do GFI EndPointSecurity GFI ReportPack. Para baixar o suplemento visite:
http://www.gfi.com/endpointsecurity/esecreportpack.htm

Para obter mais informações sobre consulte GFI EndPointSecurity GFI ReportPack:

1. Clique na guia **Reporting**.
2. No painel esquerdo, selecione ou **GFI EndPointSecurity GFI ReportPack** ou **GFI ReportCenter**.

> **Obs.**
> É necessária uma conexão com a Internet.

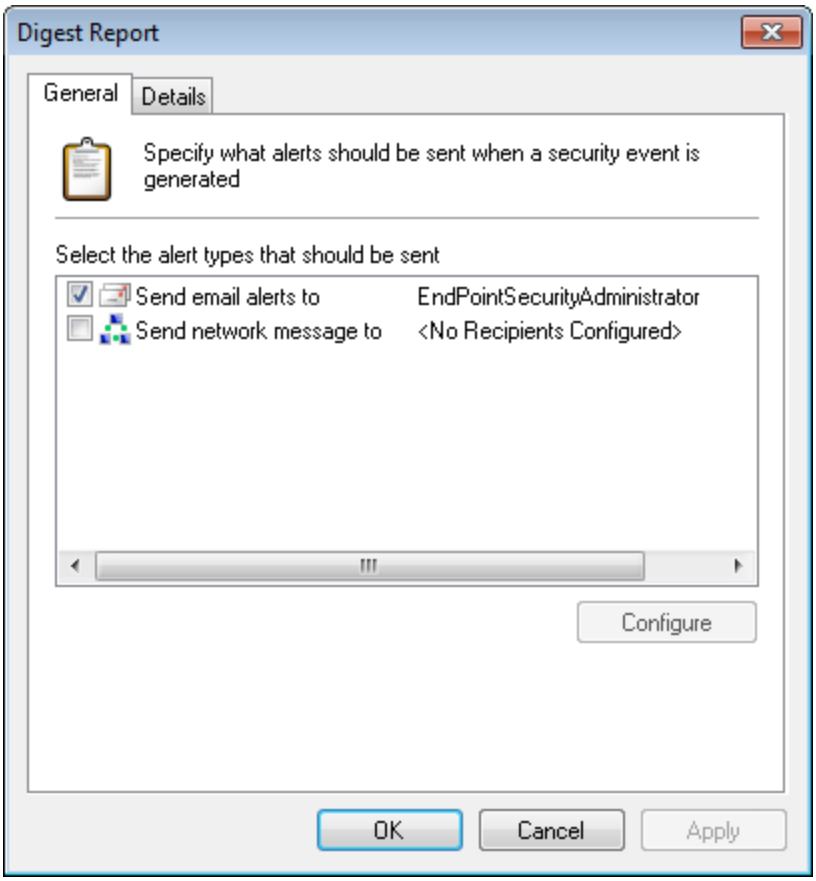
10.2 Gerar relatório resumido

GFI EndPointSecurity habilita a gerar relatórios resumidos para os destinatários configurados. Relatórios resumidos contêm um resumo da atividade estatística periódica como detectado pelo GFI EndPointSecurity.

Os destinatários de alertas não são usuários do Active Directory (AD) e/ou grupos de usuários, mas sim contas de perfil criadas pelo GFI EndPointSecurity para manter os detalhes de contato dos usuários que pretendem receber alertas. A melhor solução é criar destinatários de alertas antes de configurar os alertas. Para obter mais informações, consulte Configurar destinatários de alertas (página 137).

Para configurar relatórios resumidos:

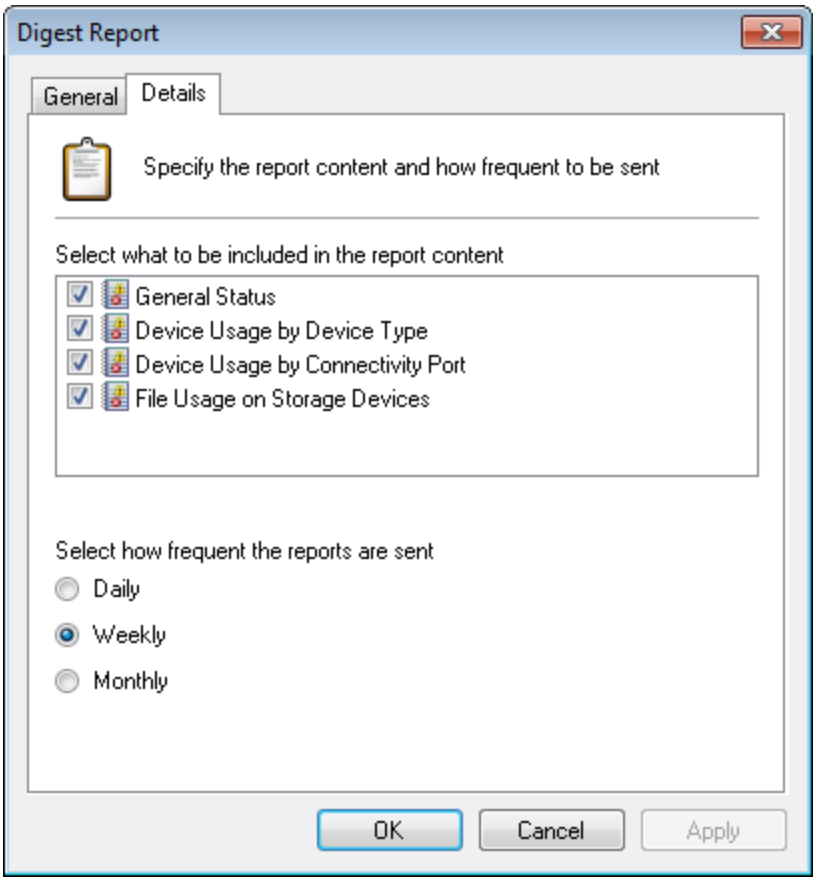
1. Clique na guia **Configuration** > subguia **Options**.
2. A partir de **Configure**, clique em **Alerting options** e a partir do painel direito, clique em **Configure the digest report**.



Screenshot 99: Opções de Digest Report - Guia General

3. A partir da guia **General** da caixa de diálogo **Digest Report**, marque/desmarque o método de alerta preferencial.

4. Para cada tipo de alerta selecionado, clique em **Configure** para especificar o(s) usuário(s)/grupo (s) destinatários do alerta.



Screenshot 100: Opções de Digest Report - Guia Details

5. Clique na guia **Details** para marcar/desmarcar itens do conteúdo do relatório para incluir no relatório resumido.
6. Selecione enviar frequência do relatório, de **Daily**, **Weekly** ou **Monthly**.
7. Clique em **Apply** e em **OK**.

11 Gerenciar back-end do banco de dados

Este capítulo fornece informações relacionadas com o gerenciamento e a manutenção do banco de dados onde os dados coletados pelo GFI EndPointSecurity são armazenados. Após instalar o GFI EndPointSecurity, é possível escolher o seguinte:

- Baixar e instalar uma instância do Microsoft SQL Server Express Edition e criar automaticamente um banco de dados para o GFI EndPointSecurity. Isto pode ser realizado por meio do **Quick Start wizard**.
- Realizar a conexão a uma instância disponível do Microsoft SQL Server e realizar a conexão a um banco de dados existente ou, por outro lado, criar um novo. Esta ação pode ser realizada por meio do **Quick Start wizard**, nas subguias **General Status** ou **Options**.

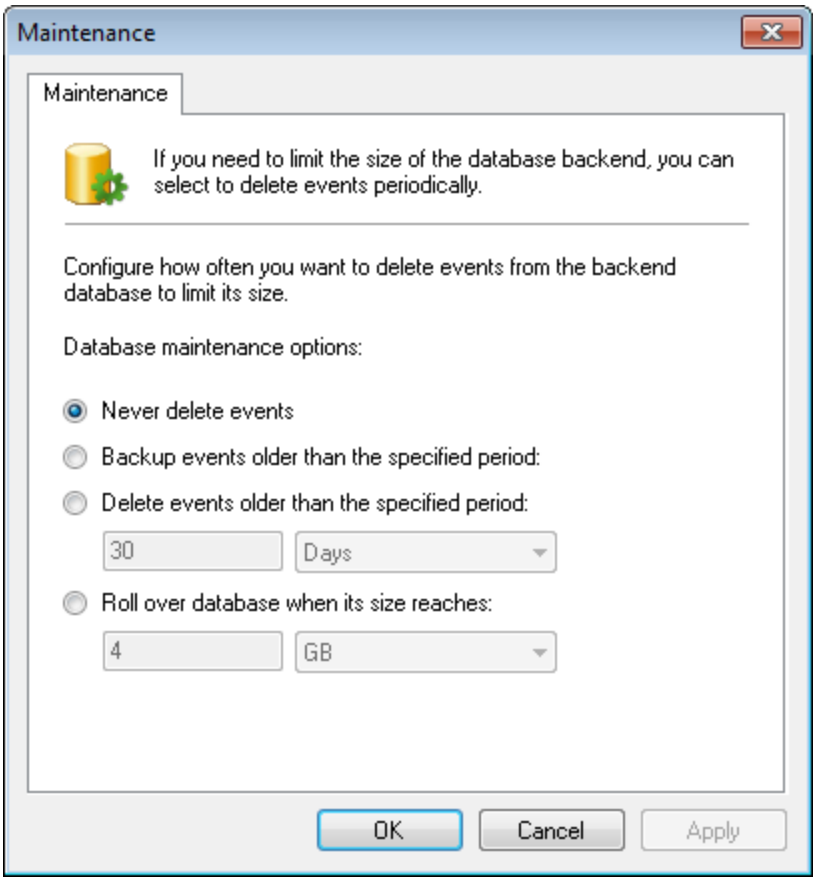
Tópicos neste capítulo

11.1 Realizar a manutenção do back-end do banco de dados

A manutenção periódica do banco de dados é essencial para evitar que o back-end do banco de dados aumente demasiado. O GFI EndPointSecurity fornece a capacidade de configurar parâmetros que efetuem a manutenção de seu back-end do banco de dados automaticamente.

Para configurar a manutenção do back-end do banco de dados:

1. Clique na guia **Configuration** > subguia **Options**.
2. A partir de **Configure**, selecione **Database Backend**.
3. A partir do painel direito, clique em **Database maintenance**.



Screenshot 101: Opções de Maintenance

4. A partir da caixa de diálogo **Maintenance**, configure o número de vezes que os eventos são excluídos do back-end do banco de dados. Selecione a partir das opções descritas abaixo:

Table 17: Opções de manutenção do banco de dados

Opção	Descrição
Never delete events	Mantenha todos os eventos no back-end do banco de dados, sem excluir os anteriores. **Obs.** Certifique-se de que a exclusão do manual de registros antigos seja realizada para evitar a perda de desempenho do GFI EndPointSecurity.
Backup events older than the specified period	Selecione esta opção e especifique quão antigos os eventos devem ser antes de ser realizado o seu backup para um banco de dados separado.
Delete events older than the specified period	Selecione esta opção e especifique quão antigos os eventos devem ser antes de serem excluídos.
Roll over database when its size reaches	Especifique o tamanho máximo que um banco de dados pode alcançar antes de o GFI EndPointSecurity mudar automaticamente para um novo banco de dados.

5. Clique em **Apply** e em **OK**.

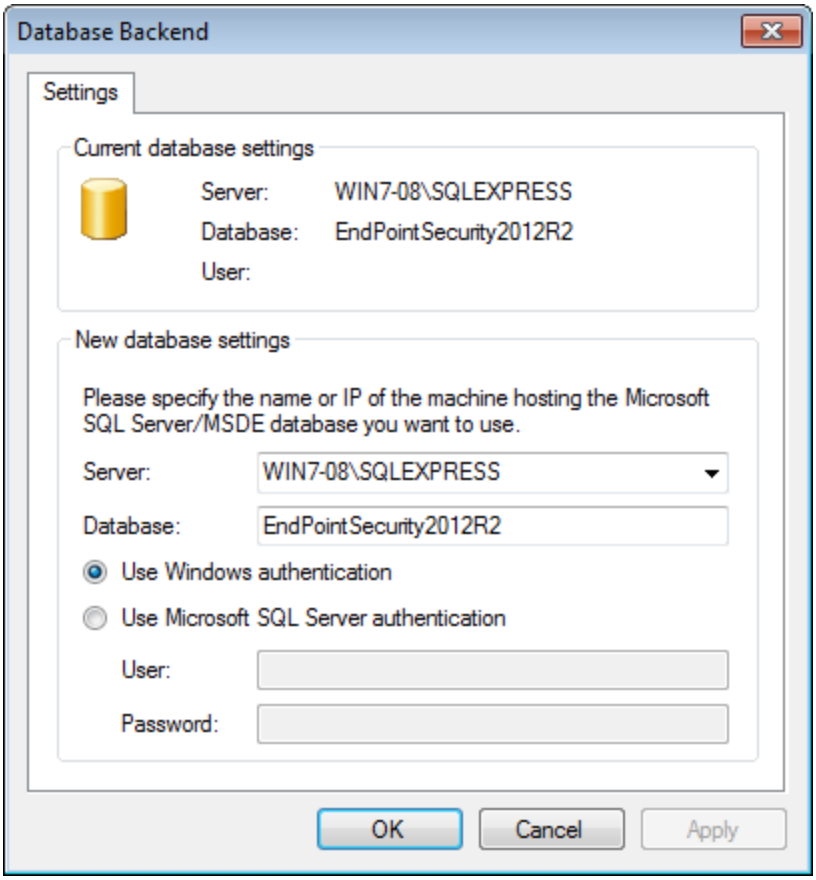
Obs.

Uma vez que o Microsoft SQL Express 2005 possui um limite de tamanho de banco de dados de 4 GB e o Microsoft SQL Express 2008 R2 possui um limite de banco de dados de 10 GB, recomenda-se o uso da opção Roll over database. Para obter mais informações sobre o Microsoft SQL Server Edition, especificações do mecanismo, consulte http://go.gfi.com/?pageid=ESEC_SqlSpecs.

11.2 Usar uma instância existente do SQL Server

Para realizar a conexão a uma instância existente do SQL Server:

1. Clique na guia **Configuration** > subguia **Options**.
2. A partir de **Configure**, selecione **Database Backend**.
3. A partir do painel direito, clique em **Change database backend**.



Screenshot 102: Alterar o Database Backend

4. A partir do menu suspenso **Server**, selecione o SQL Server que deseja usar.
5. Especifique o nome do banco de dados na caixa de texto **Database**.
6. Selecione o modo de autenticação e especifique as credenciais de logon, se necessário.
7. Clique em **Apply** e em **OK**.

12 Opções de alertas

Este capítulo fornece informações sobre a configuração de opções de alertas e destinatários de alertas do GFI EndPointSecurity. Os alertas são uma parte fundamental da operação do GFI EndPointSecurity que ajuda a tomar medidas corretivas assim que uma ameaça é detectada.

Tópicos neste capítulo

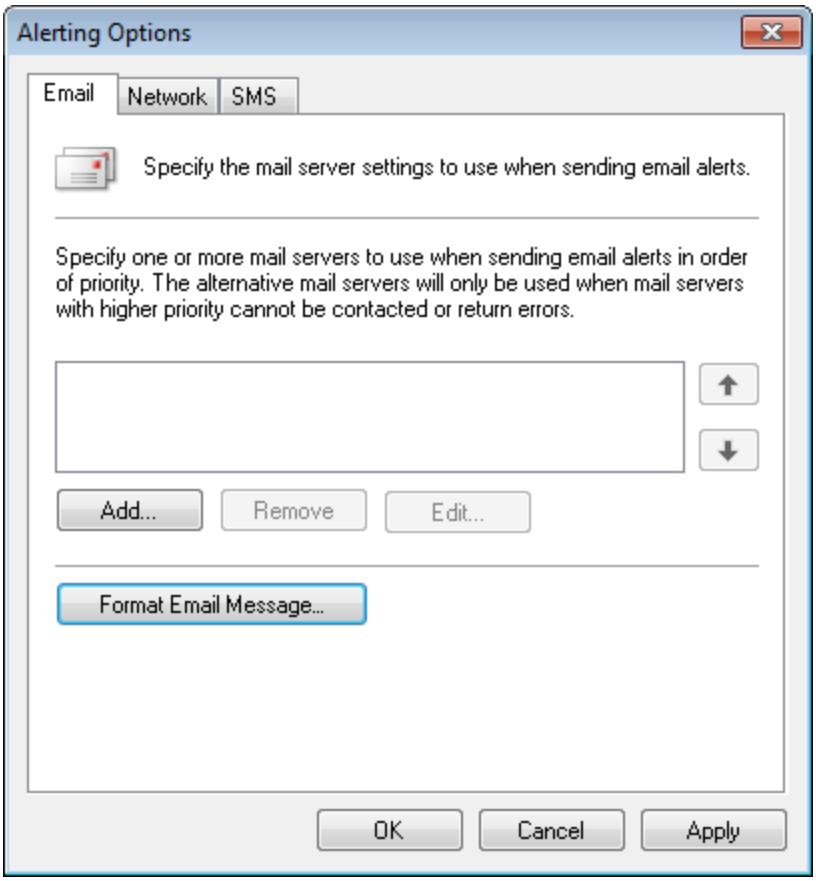
12.1 Configurar opções de alertas

O GFI EndPointSecurity permite configurar as seguintes opções de alertas:

- As configurações do servidor de email, os detalhes do remetente e a mensagem de email que são usados quando ocorrem alertas de email
- A mensagem de rede a usar ao enviar alertas de rede
- O gateway de SMS e a mensagem de SMS que são usados ao enviar alertas de SMS.

Para configurar opções de alertas:

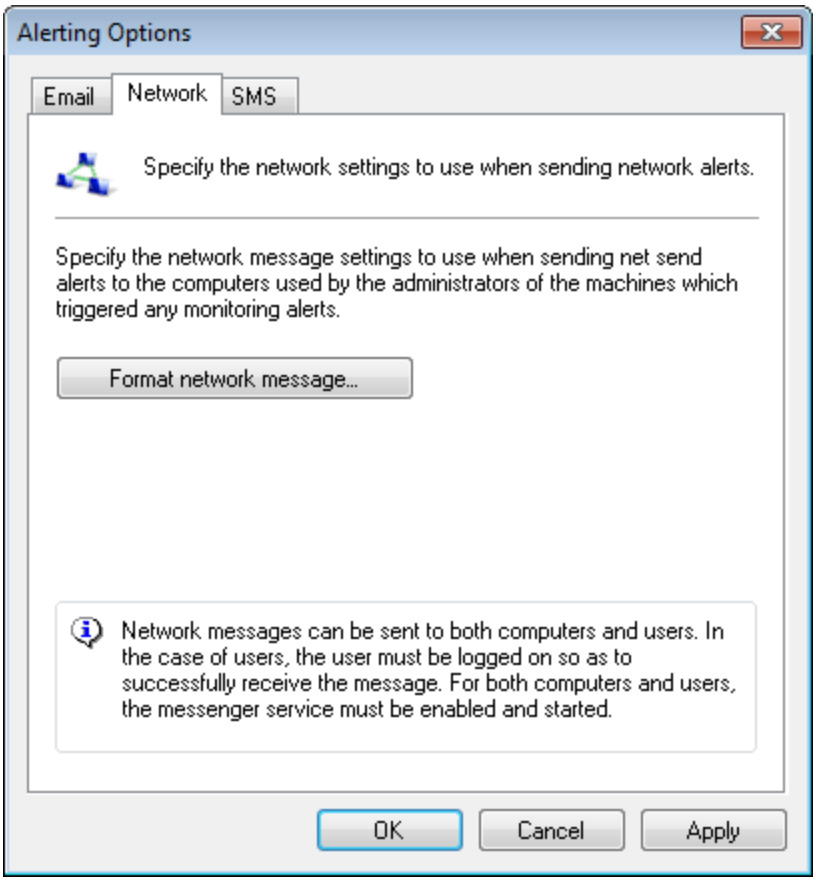
1. Clique na guia **Configuration** > subguia **Options**.
2. Em **Configure**, clique com o botão direito do mouse no nó **Alerting Options** e selecione **Edit alerting options...**.



Screenshot 103: Alerting Options - Guia Email

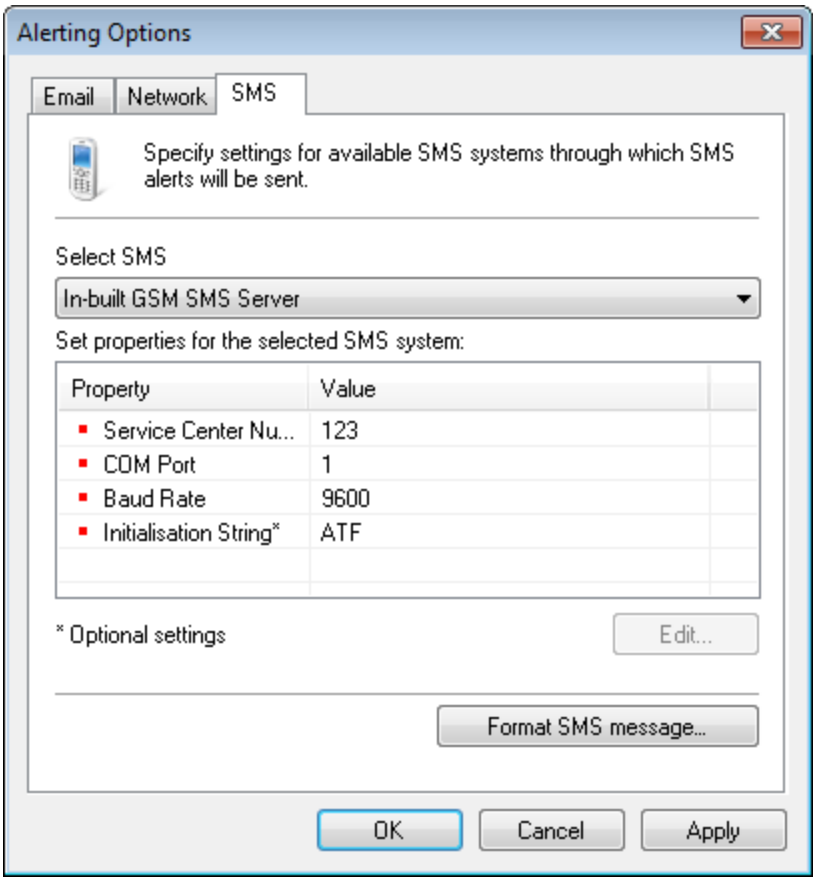
3. A partir da guia **Email**, clique em **Add...** para especificar as configurações do servidor de email. Clique em **OK** para fechar a caixa de diálogo **Mailserver properties**.

4. Para editar a mensagem de email, clique em **Format Email Message…**, modifique os campos **Subject** e **Message** conforme necessário e clique em **Save**.



Screenshot 104: Alerting Options - Guia Network

5. Clique na guia **Network > Format network message…** para editar a mensagem de rede. Clique em **Save**.



Screenshot 105: Alerting Options - Guia SMS

6. Clique na guia **SMS** e, a partir do menu suspenso **Select SMS**, selecione o gateway de SMS que deseja usar. Os sistemas de SMS suportados incluem:

- GSM integrado do SMS
- Gateway de SMS do GFI FaxMaker
- Email Clickatell para gateway de serviços de SMS
- O SMS genérico fornece gateway.

7. A partir da área **Set properties for the selected SMS system**, realce a propriedade que deseja configurar e clique em **Edit**. Repita esta etapa para cada propriedade do sistema de SMS que deseja modificar.

8. Clique em **Format SMS message…** para modificar o Assunto e a Mensagem conforme necessário. Clique em **Save**.

9. Clique em **OK**.

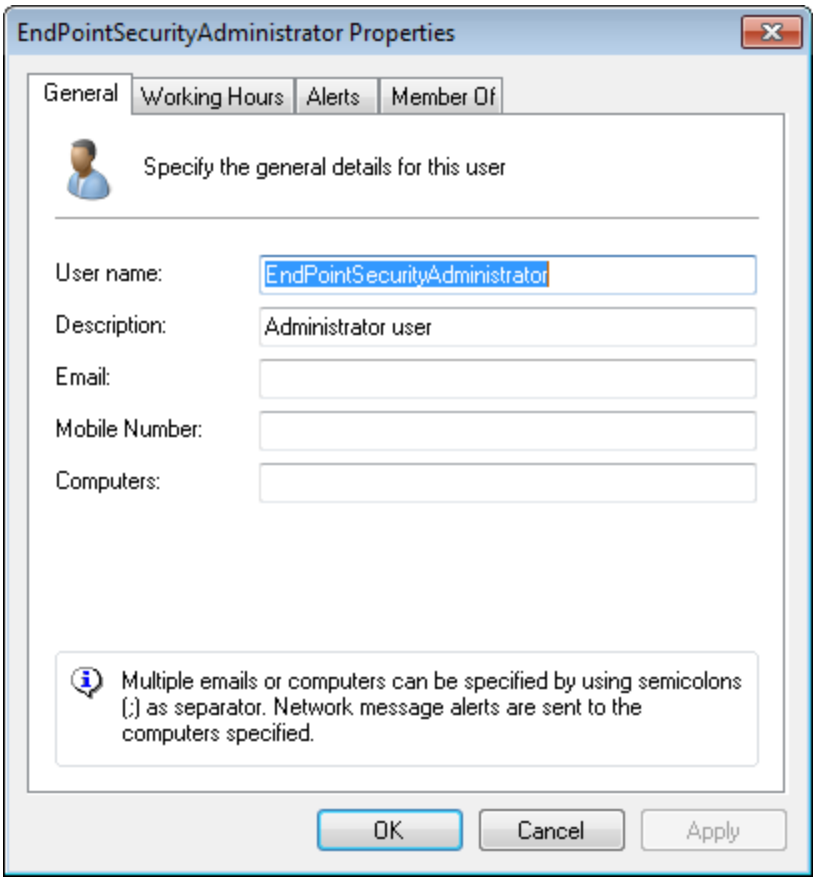
12.2 Configurar a conta de administrador de alertas

O GFI EndPointSecurity permite configurar contas de perfil para manter os detalhes de contato dos usuários que pretendem receber alertas de email, mensagens de rede e mensagens de SMS. Após a instalação, o GFI EndPointSecurity cria automaticamente uma conta de administrador de alertas. Os administradores de alertas não são usuários do Active Directory (AD) e/ou grupos de usuários.

Por padrão, o GFI EndPointSecurity cria automaticamente uma conta de EndPointSecurityAdministrator (para fins de alerta) após a instalação e define-a como um membro do grupo de notificação EndPointSecurityAdministrators.

Para configurar a conta GFI EndPointSecurityAdministrator:

1. Clique na guia **Configuration** > subguia **Options**.
2. Em **Configure**, clique no subnó **Alerting Options > Users**.
3. No painel direito, clique com o botão direito do mouse em **EndPointSecurityAdministrator** e selecione **Properties**.

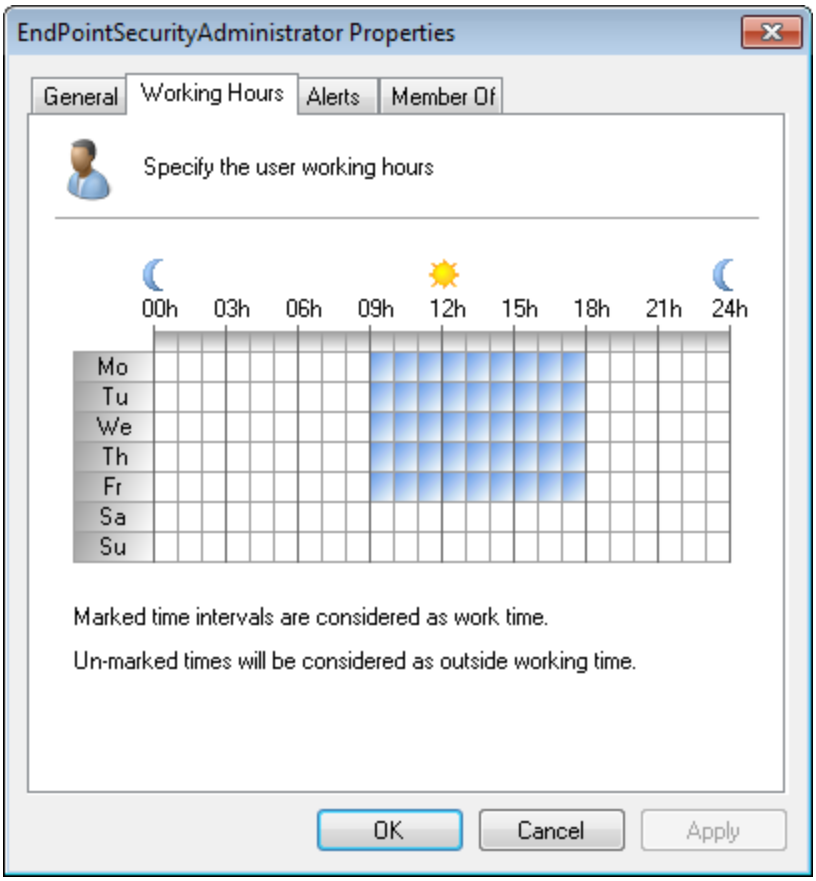


Screenshot 106: Opções de EndPointSecurityAdministrator Properties - Guia General

4. A partir da guia General, digite os seguintes detalhes:

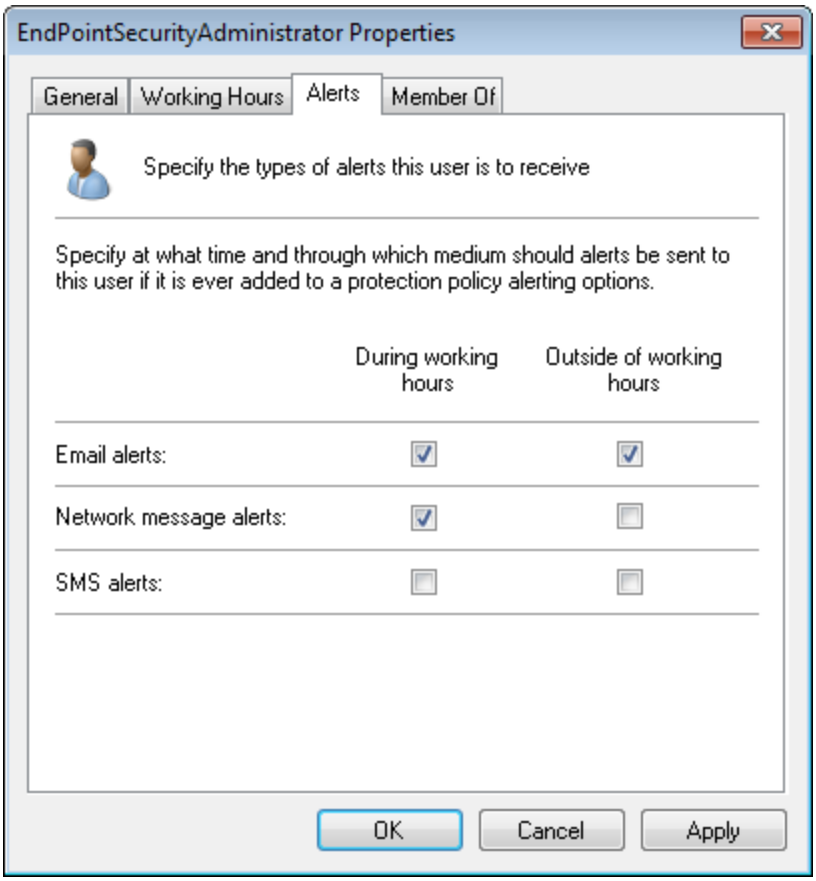
- Nome de usuário da conta
- Descrição da conta
- Endereço de email
- Número de celular
- Computadores (as mensagens de rede são enviadas aos computadores especificados).

> **Obs.**
>
> Pode ser especificado mais que um endereço de email e mais que um nome de computador/endereço IP. Entradas separadas com ponto-e-vírgula ";".



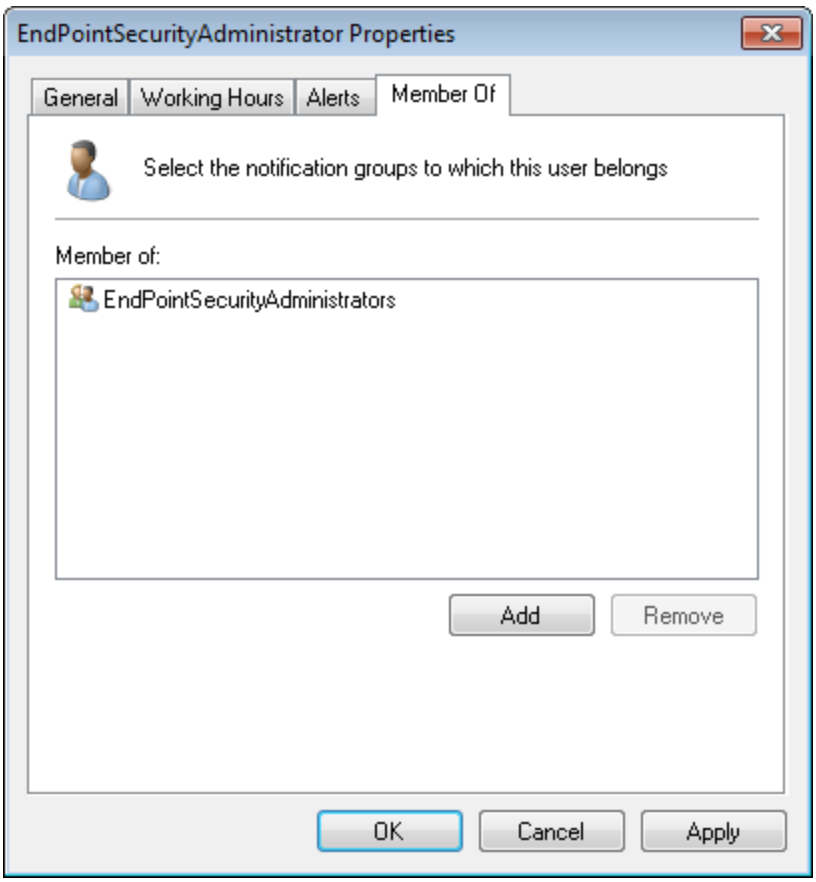
Screenshot 107: Opções de EndPointSecurityAdministrator Properties - Guia Working Hours

5. Clique na guia **Working Hours** e marque o horário de expediente normal do usuário. Intervalos de tempo marcados são considerados horas de trabalho.



Screenshot 108: Opções de EndPointSecurityAdministrator Properties - Guia Alerts

6. Clique na guia **Alerts** e selecione os alertas a enviar e as horas em que os alertas são enviados.



Screenshot 109: Opções de EndPointSecurityAdministrator Properties - Guia Member Of

7. Clique na guia **Member Of** e clique em **Add** para adicionar o usuário ao(s) grupo(s) de notificação.
8. Clique em **Apply** e em **OK**.

12.3 Configurar destinatários de alertas

O GFI EndPointSecurity permite configurar outras contas de perfil (além da conta GFI EndPointSecurityAdministrator padrão) para manter os detalhes de contato dos usuários que pretendem receber alertas de email, mensagens de rede e mensagens de SMS.

Os destinatários de alertas não são usuários do Active Directory (AD) e/ou grupos de usuários, mas sim contas de perfil criadas pelo GFI EndPointSecurity para manter os detalhes de contato dos usuários que pretendem receber alertas.

- Criar destinatários de alertas
- Editar propriedades dos destinatários de alertas
- Excluir destinatários de alertas

12.3.1 Criar destinatários de alertas

Para criar um novo destinatário de alertas:

1. Clique na guia **Configuration** > subguia **Options**.
2. Em **Configure**, clique no subnó **Alerting Options > Users**.
3. A partir do painel esquerdo, clique em **Create user…**.
4. Para obter mais informações sobre como configurar as definições para criar um novo destinatário, consulte Configurar a conta de administrador de alertas.

12.3.2 Editar propriedades dos destinatários de alertas

Para editar propriedades dos destinatários de alertas:

1. Clique na guia **Configuration** > subguia **Options**.
2. Em **Configure**, clique no subnó **Alerting Options > Users**.
3. A partir do painel direito, clique com o botão direito do mouse no usuário que deseja editar e selecione **Properties**.
4. Para obter mais informações sobre como configurar as definições para editar um destinatário, consulte Configurar a conta de administrador de alertas.

12.3.3 Excluir destinatários de alertas

Para excluir um destinatário de alertas:

1. Clique na guia **Configuration** > subguia **Options**.
2. Em **Configure**, clique no subnó **Alerting Options > Users**.
3. A partir do painel direito, clique com o botão direito do mouse no usuário que deseja editar e selecione **Delete**.
4. Clique em **Yes** para confirmar a exclusão.

12.4 Configurar grupos de destinatários de alertas

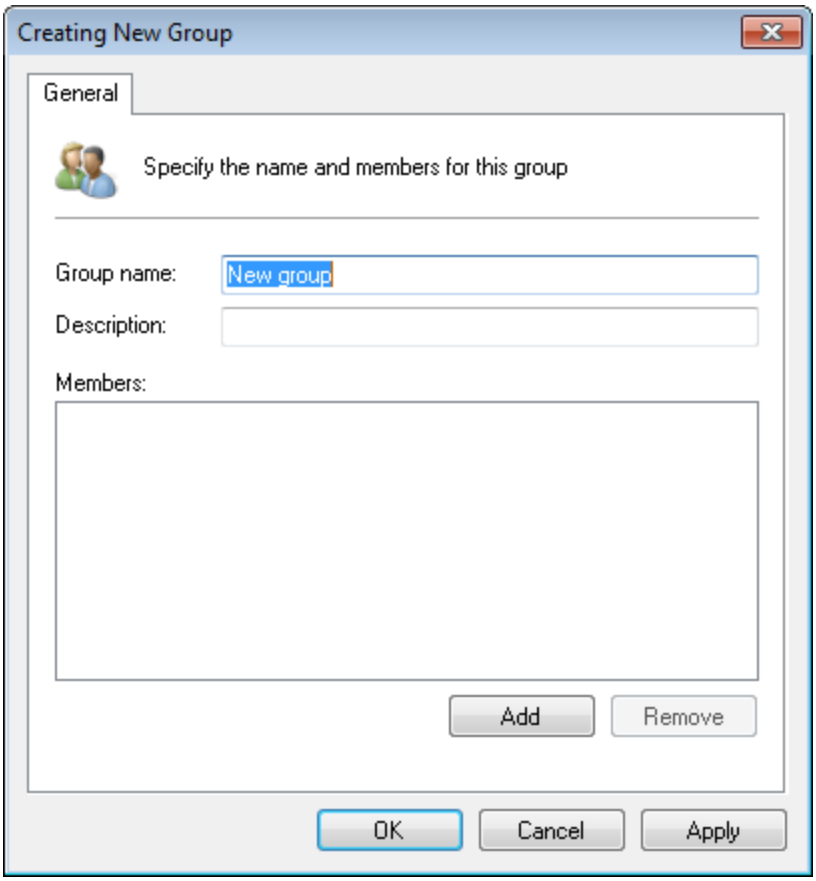
O GFI EndPointSecurity permite organizar os destinatários de alertas em grupos de forma a facilitar o gerenciamento dos destinatários de alertas.

- Criar grupos de destinatários de alertas
- Editar propriedades de grupos de destinatários de alertas
- Excluir grupos de destinatários de alertas

12.4.1 Criar grupos de destinatários de alertas

Para criar um novo grupo de destinatários de alertas:

1. Clique na guia **Configuration** > subguia **Options**.
2. Clique no subnó **Alerting Options > Groups**.
3. A partir do painel esquerdo, clique em **Create group…**.



Screenshot 110: Opções de Creating New Group

4. Na caixa diálogo **Creating New Group** digite o nome do grupo e uma descrição opcional.
5. Clique em **Add** para selecionar o(s) usuário(s) que pertence(m) a este grupo de notificações e clique em **OK**.

12.4.2 Editar propriedades de grupos de destinatários de alertas

Para editar as propriedades de grupos de destinatários de alertas:

1. Clique na guia **Configuration** > subguia **Options**.
2. Clique no subnó **Alerting Options > Groups**.
3. A partir do painel direito, clique com o botão direito do mouse no grupo que deseja editar e selecione **Properties**.

4. Para obter mais informações sobre como editar as configurações de grupos, consulte Criar grupos de destinatários de alertas.

12.4.3 Excluir grupos de destinatários de alertas

Para excluir um grupo de destinatários de alertas:

1. Clique na guia **Configuration** > subguia **Options**.
2. Clique no subnó **Alerting Options > Groups**.
3. A partir do painel direito, clique com o botão direito do mouse no grupo que deseja excluir e selecione **Delete**.
4. Clique em **Yes** para confirmar a exclusão do grupo.

13 Configuração do GFI EndPointSecurity

O GFI EndPointSecurity permite configurar os computadores nos quais deseja instalar atualizações e exibir mensagens do usuário.

Tópicos neste capítulo

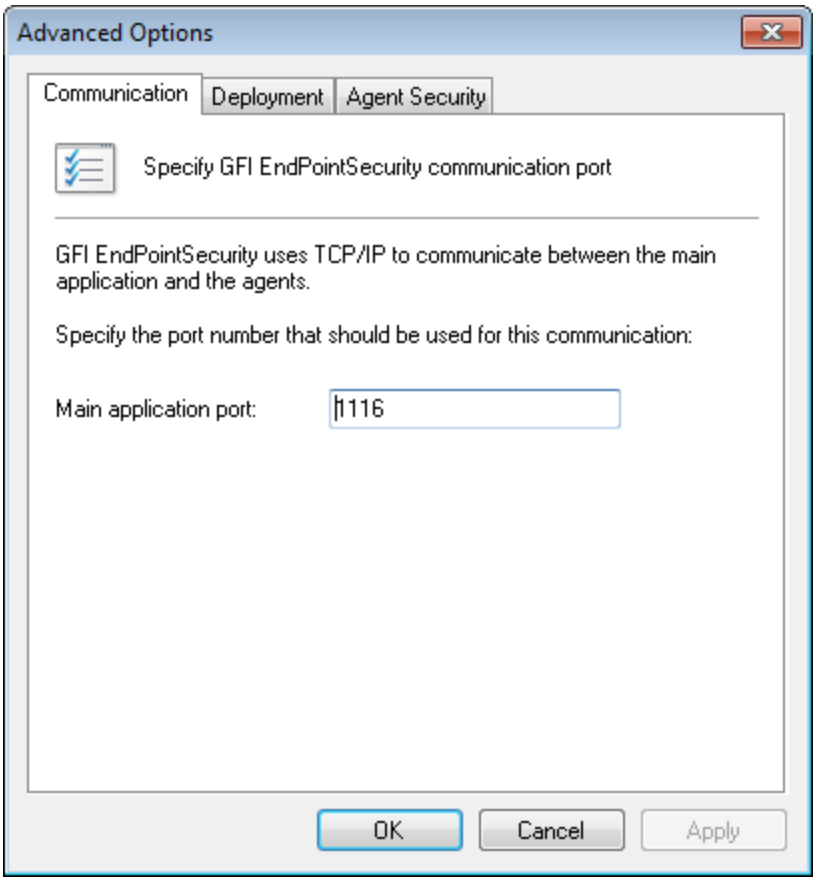
13.1 Configurar opções avançadas

O GFI EndPointSecurity permite configurar as opções avançadas de Agente seguintes:

- Porta de comunicação principal TCP/IP
- Opções de implantação
- Senha de controle de agentes.

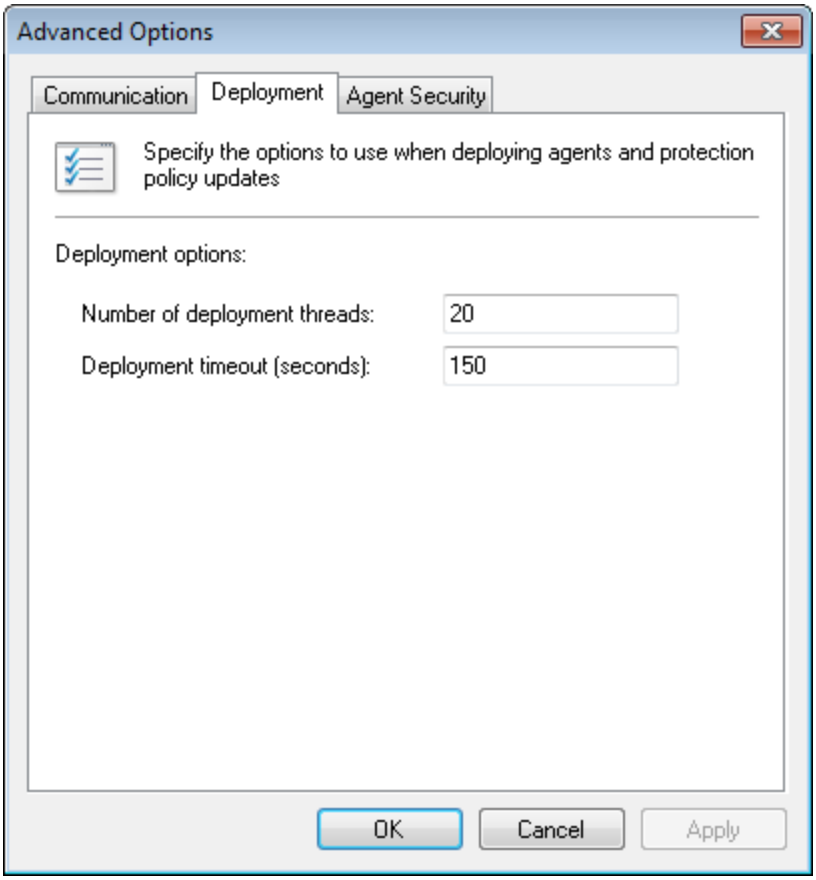
Para configurar opções avançadas:

1. Clique na guia **Configuration** > subguia **Options**.
2. Em **Configure**, clique com o botão direito do mouse no nó **Advanced Options** e selecione **Modify advanced options...**.



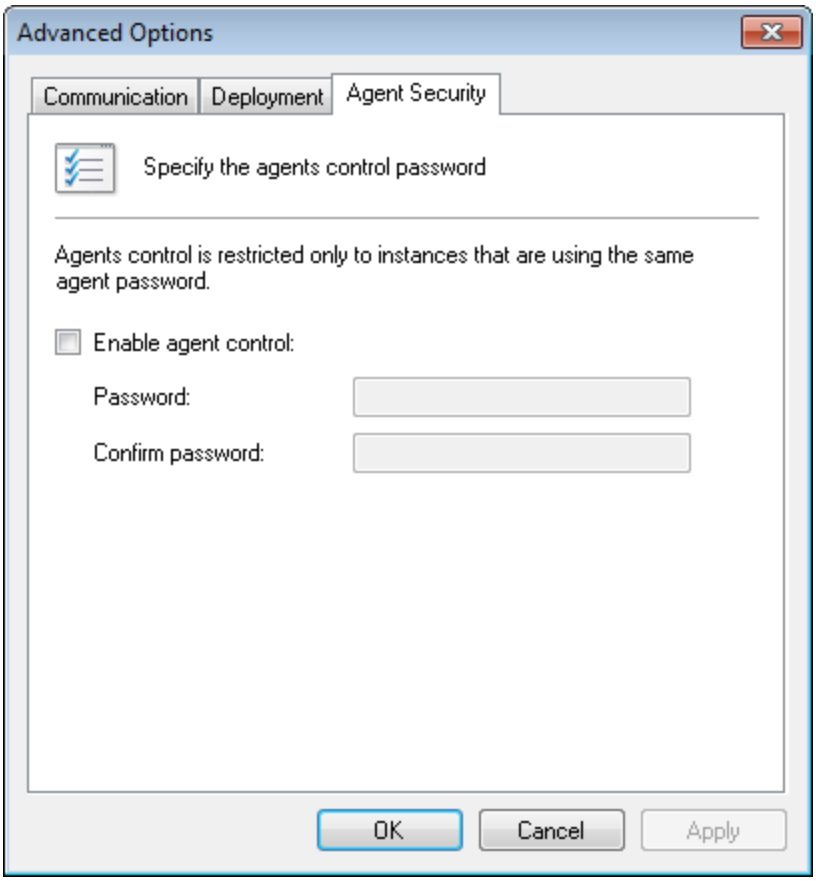
Screenshot 111: Advanced Options - Guia Communication

3. A partir da guia **Communication**, digite o número da porta TCP/IP a ser usado para comunicação entre o GFI EndPointSecurity e os Agentes do GFI EndPointSecurity. Por padrão, é especificada a porta **1116**.



Screenshot 112: Advanced Options - Guia Deployment

4. Clique na guia **Deployment** e digite os valores **Number of deployment threads** e **Deployment timeout (seconds)** necessários.



Screenshot 113: Advanced Options - Guia Agent Security

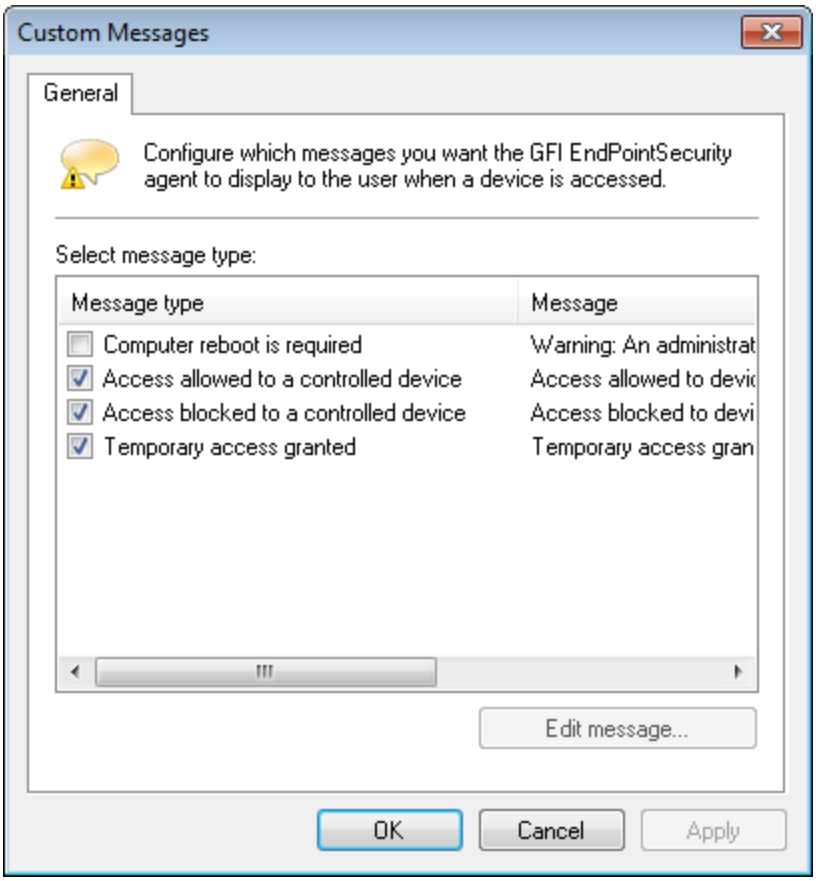
5. Clique na guia **Agent Security** e marque/desmarque a opção **Enable agent control**. Use esta opção para atribuir credenciais de logon particulares a todos os agentes do GFI EndPointSecurity implantados em sua rede.
6. Clique em **Apply** e em **OK**.

13.2 Configurar mensagens do usuário

O GFI EndPointSecurity permite personalizar as mensagens que são exibidas pelos Agentes do GFI EndPointSecurity em computadores de destino, quando os dispositivos são acessados.

Para personalizar as mensagens do usuário:

1. Clique na guia **Configuration** > subguia **Options**.
2. Em Configure, clique com o botão direito do mouse em Custom Messages e selecione Customize user messages.



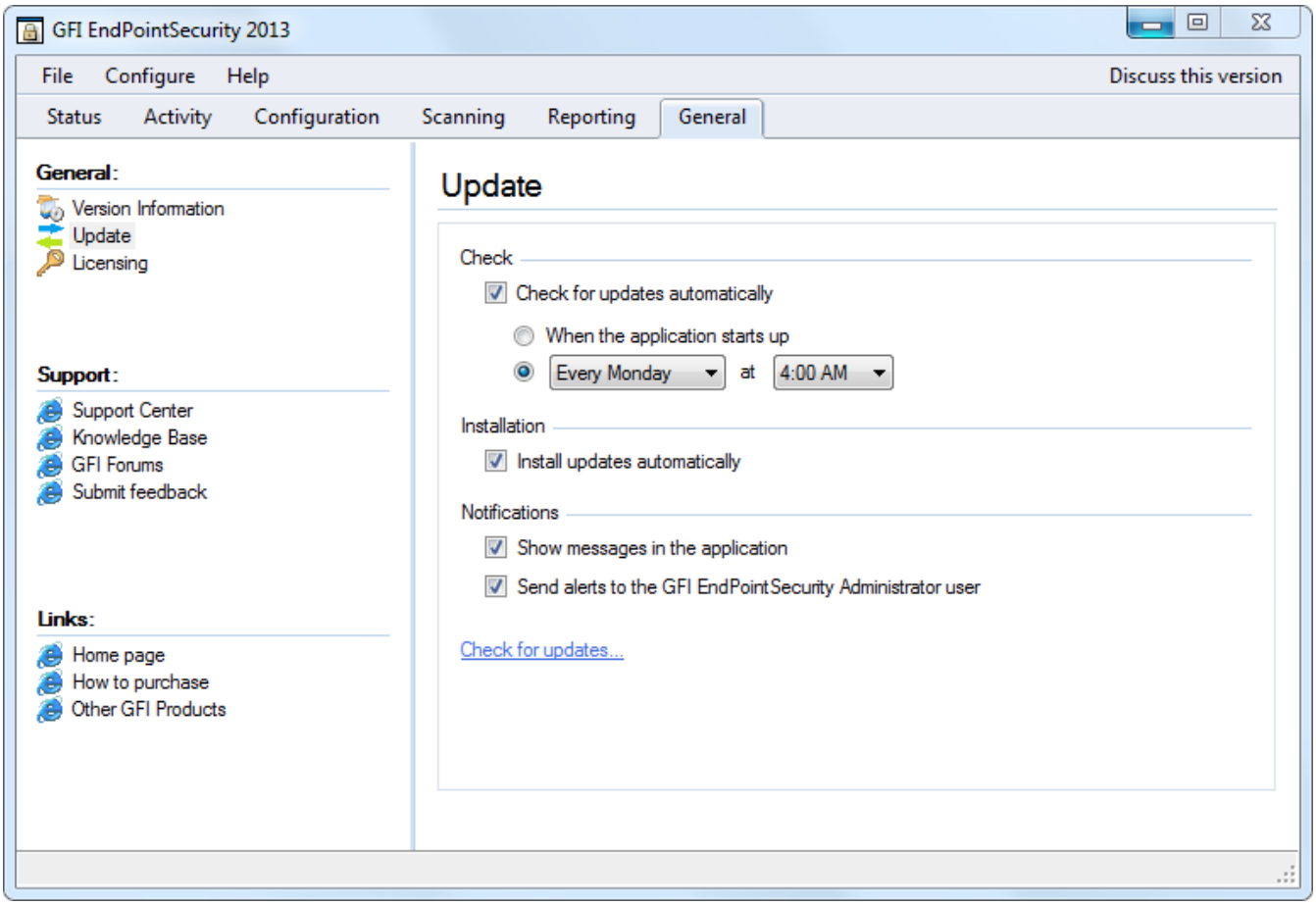
Screenshot 114: Opções da caixa de diálogo Custom Messages

3. Marque/desmarque os tipos de mensagem que deseja personalizar.
4. Para cada tipo de mensagem selecionado, clique em **Edit message…**, modifique o texto conforme necessário e clique em **Save**. Repita esta etapa para cada mensagem que deseja modificar.
5. Clique em **Apply** e em **OK**.

13.3 Configurar atualizações do GFI EndPointSecurity

O GFI EndPointSecurity pode ser configurado para baixar e instalar atualizações automaticamente se estiverem agendadas ou em inicialização. Para configurar atualizações:

1. Clique na guia **General**.
2. A partir do painel esquerdo, clique em **Updates**.



Screenshot 115: Guia General - Updates

3. A partir do painel direito, configure as opções descritas abaixo:

Table 18: Opções de atualização

Opção	Descrição
Check for updates automatically	Efetuar a conexão aos servidores de atualização GFI e baixar atualizações do produto automaticamente. Selecionar When the application starts up ou especificar um dia e uma hora para verificar e baixar atualizações.
Install updates automatically	Se for encontrada uma atualização, o GFI EndPointSecurity irá baixar e instalar a atualização automaticamente.
Show messages in the application	Se for encontrada uma atualização e esta for instalada, é exibida uma mensagem no aplicativo GFI EndPointSecurity.
Send alerts to the GFI EndPointSecurity Administrator user	Assim que uma atualização é baixada e instalada, é enviada uma mensagem de email ao Administrador do GFI EndPointSecurity. Para obter mais informações, consulte Configurar a conta de administrador de alertas (página 133).
Check for updates	Clicar no link para executar instantaneamente o mecanismo de atualizações do GFI EndPointSecurity, baixar e instalar quaisquer atualizações em falta.

14 Diversos

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

Tópicos neste capítulo

14.1 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 116: 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.

14.2 Desinstalar o GFI EndPointSecurity

O GFI EndPointSecurity permite desinstalar facilmente os agentes do GFI EndPointSecurity e o aplicativo GFI EndPointSecurity.

Este capítulo acompanha os seguintes tópicos:

- Desinstalar agentes do GFI EndpointSecurity
- Desinstalar aplicativo GFI EndpointSecurity

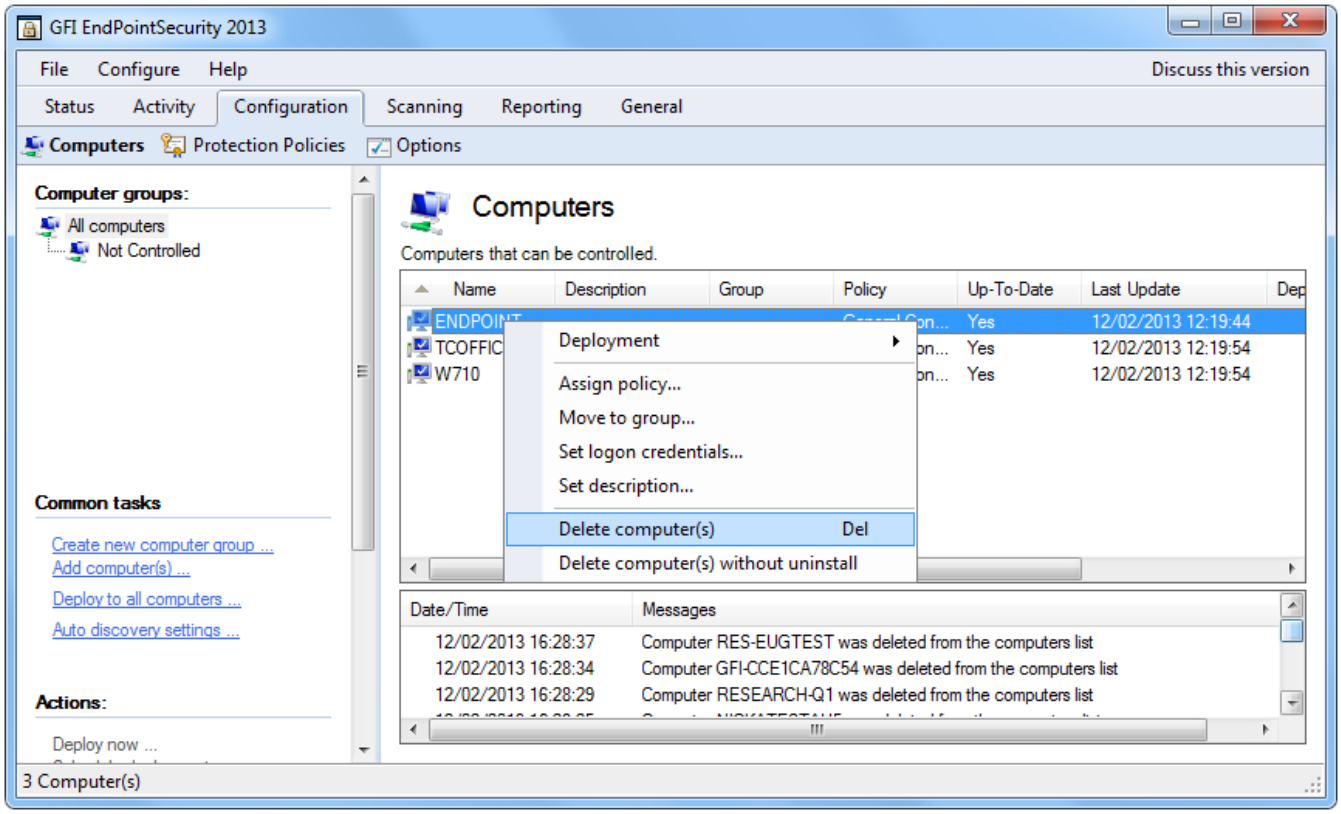
Aviso

Os agentes do GFI EndPointSecurity não são desinstalados automaticamente durante a desinstalação do aplicativo GFI EndPointSecurity. É melhor desinstalar primeiro os agentes do GFI EndPointSecurity e depois o aplicativo GFI EndPointSecurity.

14.2.1 Desinstalar agentes do GFI EndPointSecurity

Para desinstalar um agente do GFI EndPointSecurity:

1. A partir do console de gerenciamento do GFI EndPointSecurity, clique na guia **Configuration**.
2. Clique na subguia **Computers**.



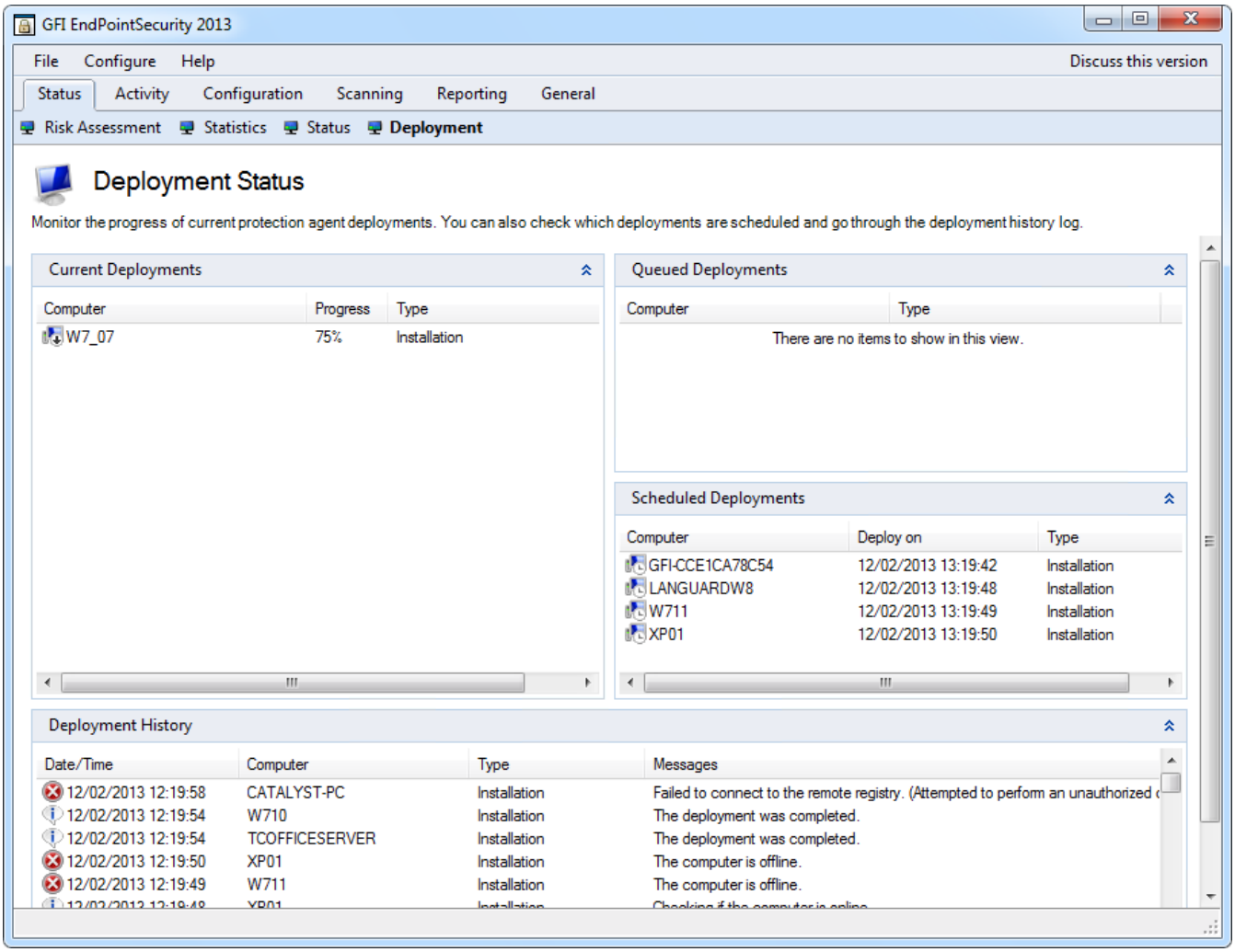
Screenshot 117: Subguia Computers - excluir computador(es)

3. No painel direito, clique com o botão direito do mouse no computador de destino que deseja desinstalar e selecione:

Deleting Computer(s)	
Deleting computer(s) - **with** uninstallation	O GFI EndPointSecurity implantará atualizações da política de proteção e desinstalará o Agente.
Deleting computer(s) - **without** uninstallation	O GFI EndPointSecurity implantará atualizações na política de proteção e removerá a entrada do computador relevante da lista Computers. Porém, este deixa o agente instalado no computador de destino. Esta opção é útil caso o computador de destino tenha sido removido da rede e o aplicativo GFI EndPointSecurity não consiga conectar-se ao mesmo para desinstalar o agente.

4. Clique em **Yes** para confirmar a exclusão do computador selecionado da lista.

5. 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**.



Screenshot 118: Subguia Deployment

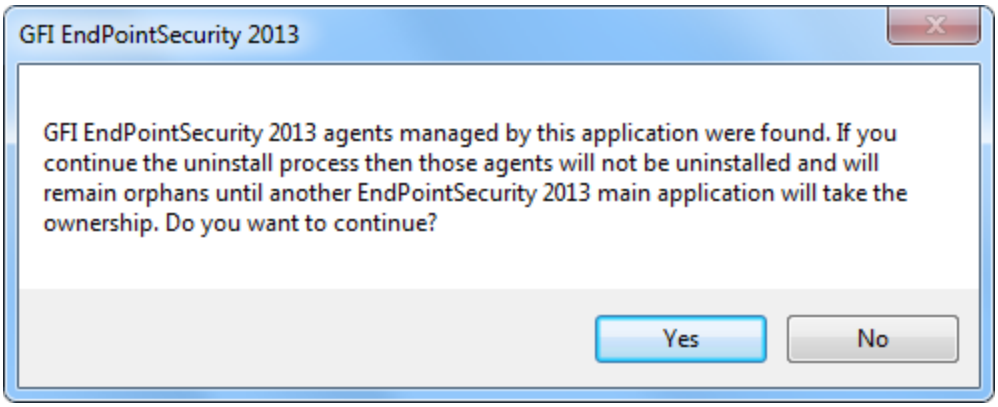
6. A partir da área **Deployment History**, confirme se a desinstalação foi concluída com êxito a partir do computador de destino.

14.2.2 Desinstalar o aplicativo GFI EndPointSecurity

Para desinstalar o aplicativo GFI EndPointSecurity:

> **Obs.**
>
> Execute o desinstalador como um usuário com privilégios administrativos no computador.

1. A partir de **Microsoft Windows Control Panel**, selecione a opção **Add/Remove Programs** ou **Programs and Features**.
2. Selecione GFI EndPointSecurity.
3. Clique em **Change** para iniciar a desinstalação do aplicativo GFI EndPointSecurity.
4. Clique em **Next** na tela inicial de boas-vindas para dar continuidade à desinstalação.



Screenshot 119: Mensagem de informação de desinstalação

Obs.

Caso alguns agentes ainda se encontrem instalados, é exibida uma caixa de diálogo de informação perguntando se deseja continuar (os agentes permanecerão instalados e órfãos) ou não com o processo de desinstalação. Para obter mais informações sobre a desinstalação de agentes, consulte a seção Desinstalar agentes do GFI EndPointSecurity neste capítulo.

5. Selecione a opção **Uninstall without deleting configuration files** ou **Complete uninstall** e clique em **Next** para continuar.
6. Quando estiver concluída, clique em **Finish** para concluir a desinstalação.

14.3 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.

15 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 19: 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 120: 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 121: 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 122: 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 123: 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.

16 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.

17 Índice

V

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