GFI MailEssentials™

Guia do administrador

Versão do documento: 2.1.1

Última atualização (mês/dia/ano): 6/25/2014

Índice

Lista de figuras

1 Introdução

1.1 Sobre este manual

O objetivo deste Guia do administrador é ajudar você a instalar, executar, configurar e solucionar problemas do GFI MailEssentials em sua rede. A tabela abaixo descreve o conteúdo deste guia.

Capítulo	Descrição
Sobre	» Os componentes e as ferramentas que compõem o GFI MailEssentials » Como funciona a verificação de emails de entrada e saída » Visão geral dos mecanismos que protegem seu sistema de email » Cenários típicos de implantação Para obter mais informações, consulte Sobre o GFI MailEssentials (página 13).
Instalação	» Os vários ambientes e infraestruturas de email compatíveis com o GFI MailEssentials » Pré-requisitos do produto aplicáveis a sua rede » Preparar seu ambiente para a instalação do produto » Fornece orientações para executar os procedimentos de instalação e atualização » Ajuda o usuário a executar as etapas necessárias para começar a usar o produto com a configuração padrão. » Testar a instalação e executar o produto. Para obter mais informações, consulte Instalação (página 23).
Monitorar o status	» Usar o Painel para monitorar o status do GFI MailEssentials em tempo real » Gerar estatísticas de uso de emails e relatórios gráficos Para obter mais informações, consulte Monitorar o status (página 54).
Ações do usuário	Explica o que usuários do domínio (não os administradores de domínio) podem fazer com o GFI MailEssentials » Configurar listas de permissão de listas de bloqueio pessoais » Manter emails em quarentena Para obter mais informações, consulte Ações do usuário final (página 21).
Segurança de email	Explica como configurar os mecanismos de verificação de antimalware Para obter mais informações, consulte Segurança de email (página 74).
Anti-spam	» Configurar os filtros anti-spam » O que fazer com os emails identificados como spam » Classificar a ordem de verificação por prioridade do filtro » Configurações anti-spam gerais » Como os usuários classificam emails diretamente na caixa de correio (Verificação de pasta pública) Para obter mais informações, consulte Anti-spam (página 109).
Filtragem de conteúdo	Descreve como configurar mecanismos que fazem a verificação do conteúdo de emails Para obter mais informações, consulte Filtragem de conteúdo (página 176).
Quarentena	Descreva como administrar e usar a quarentena do GFI MailEssentials. Para obter mais informações, consulte Quarentena (página 203).

Capítulo	Descrição
Gerenciamento de email	Usar as ferramentas no console do Email Management Tools » Avisos de isenção de responsabilidade » Respostas automáticas » Lista de servidores » Monitoramento de email Para obter mais informações, consulte Gerenciamento de email (página 226). **OBS.:** No console de gerenciamento de email, você também pode acessar o recurso Pop2Exchange. Para obter mais informações, consulte POP2Exchange - Download de emails do servidor POP3 (página 258).
Configurações gerais	Descreve como personalizar as configurações gerais de seu ambiente. Para obter mais informações, consulte Configurações gerais (página 238).
Diversos	Explica as várias funções e ferramentas que podem ser usadas para gerenciar oGFI MailEssentials. Para obter mais informações, consulte Tópicos diversos (página 249).
Solução de problemas	Este capítulo explica como resolver problemas comuns encontrados ao usar o GFI MailEssentials. Para obter mais informações, consulte Solução de problemas e suporte (página 285).

1.2 Termos e convenções deste manual

Termo	Descrição
	Informações adicionais e referências essenciais para a operação do GFI MailEssentials.
	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 a substituir pelo valor aplicável, como caminhos e nomes de arquivos personalizados.
`Código`	Indica valores de texto a inserir, como comandos e endereços.

Para obter informações sobre termos técnicos e suas definições, como usados neste manual, consulte o Glossário.

2 Sobre o GFI MailEssentials

Tópicos deste capítulo:

2.1 Componentes do GFI MailEssentials

2.1.1 Mecanismo de verificação do GFI MailEssentials

O mecanismo de verificação do GFI MailEssentials analisa o conteúdo de emails de entrada, de saída e internos usando vários mecanismos e filtros. O resultado da análise identifica se um email deve ser bloqueado ou permitido.

> **OBS.**
> Quando você instalar o GFI MailEssentials no Microsoft® Exchange Server 2003, ele verificará o armazenamento de informações do Microsoft® Exchange. Se estiver instalado em uma máquina com o Microsoft® Exchange Server 2007/2010 com as funções de servidor Transporte de Hub e Caixa de Correio, ele também analisará os emails internos.

2.1.2 Interface da Web do GFI MailEssentials

Através da interface da Web do GFI MailEssentials, você pode:

- Monitorar a atividade de verificação de email
- Gerenciar os mecanismos de filtragem e verificação
- Analisar e processar emails em quarentena
- Configurar recursos de gerenciamento de email
- Gerar relatórios

2.1.3 GFI MailEssentialsMenu de controle

Use o GFI MailEssentials Switchboard para configurar:

- Iniciar a interface do usuário doGFI MailEssentials
- Configurar os nomes de diretório virtual para interface da Web e RSS
- Habilitar/desabilitar o processamento de emails

- Habilitar/desabilitar o rastreamento
- Configurar backups de email antes e depois de processamento
- Definir o local de armazenamento da quarentena e o URL público da quarentena
- Especificar a conta de usuário para as configurações Transferir para pasta do Exchange”
- Especificar portas remotas
- Habilitar/desabilitar notificações de email com falha

2.2 Filtragem de email de entrada

A filtragem de emails de entrada é o processo através do qual os emails recebidos são verificados e filtrados antes da entrega para o usuário.

Emails de entrada são roteados para o GFI MailEssentials e processados da seguinte forma:

1. Filtros no nível do SMTP (Coleta de diretório, Lista de exclusão temporária, Lista de bloqueio de IP e Lista de bloqueio de DNS de IP) podem ser executados antes que o corpo da mensagem do email seja recebido.

2. O email é verificado pelos mecanismos de filtragem de malware e conteúdo. Todo email que contenha malware será processado de acordo com as ações configuradas. Se um email for considerado seguro, ele passará para a próxima etapa.

3. O email é verificado para ver se é destinado a uma lista no servidor de lista. Se o email corresponder a uma lista, ele será processado pelo servidor de lista.

4. O email de entrada será filtrado pelos filtros de spam. Todo email que não passar pela verificação do filtro de spam será processado como definido nas ações anti-spam. Se um email passar por todos os filtros e não for identificado como spam, ele passará para o próximo estágio.

5. Se estiverem configuradas, as respostas automáticas serão enviadas para o remetente.

6. Se configurado, o monitoramento de email será executado e as ações apropriadas serão tomadas.

7. O email será verificado pelo filtro Novos remetentes.

8. Se o email não for bloqueado por algum mecanismo de verificação ou filtragem, ele será enviado à caixa de correio do usuário.

2.3 Filtragem de emails de saída

A filtragem de emails de saída é o processo através do qual os emails enviados por usuários internos são processados antes de serem enviados pela Internet.

Quando um email de saída é enviado, ele é encaminhado para GFI MailEssentials e processado da seguinte forma:

1. O email é verificado pelos mecanismos de filtragem de malware e conteúdo. Todo email que contenha malware será processado de acordo com as ações configuradas. Se um email for considerado seguro, ele passará para a próxima etapa.

2. Comandos remotos verificam e executam todos comandos remotos em um email, se algum for encontrado. Se nenhum comando for encontrado, o email será encaminhado para a próxima etapa.

3. Se configurado, o aviso de isenção de responsabilidade aplicável será adicionado ao email.

4. Se configurado, o monitoramento de email será executado e as ações apropriadas serão tomadas.

5. Se estiver habilitada, a Lista de permissão automática adicionará os endereços de email dos destinatários à lista de permissão automática. Isso permite automaticamente que respostas desses destinatários sejam direcionadas para o remetente sem serem verificadas quanto a spam.

6. O email será enviado ao destinatário.

2.4 Mecanismos de verificação e filtragem de email

O GFI MailEssentials contém vários mecanismos de verificação e filtragem para evitar que emails mal-intencionados, spam e outros emails indesejados cheguem aos usuários do domínio.

2.4.1 Verificação de emails mal-intencionados

Os seguintes mecanismos verificam e bloqueiam emails com conteúdo mal-intencionado.

Mecanismo de verificação de email	Descrição
Mecanismos de verificação de vírus	O GFI MailEssentials utiliza vários mecanismos antivírus para verificar a presença de vírus em emails de entrada, de saída e internos. GFI MailEssentials é fornecido com os mecanismos de verificação de vírus Vipre and BitDefender. Você também pode adquirir uma licença do Kaspersky, Avira e McAfee.
Proteção de armazenamento de informações	Quando o GFI MailEssentials estiver instalado na máquina do servidor Microsoft® Exchange, o Information Store Protection permite que você use os Virus Scanning Engines para fazer a verificação de vírus no Microsoft® Exchange Information Store.
Verificador de Cavalo de Troia e executáveis	O Verificador de Cavalo de Troia e executáveis analisa e determina a função de arquivos executáveis anexados a emails. O mecanismo de verificação pode colocar posteriormente em quarentena quaisquer atividades executáveis que realizam atividades suspeitas (como Cavalos de Troia).
Mecanismo de exploração de email	O Mecanismo de exploração de email bloqueia explorações incorporadas em um email que podem ser executadas na máquina do destinatário quando o usuário receber ou abrir o email.
HTML Sanitizer	O HTML Sanitizer verifica e remove código de scripts no corpo do email e de anexos.

2.4.2 Mecanismos de filtragem de conteúdo

Os mecanismos a seguir verificam o conteúdo dos emails, verificando parâmetros que correspondam às regras configuradas.

Mecanismo de verificação de email	Descrição
Filtragem de palavra-chave	O recurso de filtragem de palavras-chave permite definir regras que filtram emails com determinadas palavras-chave ou uma combinação de palavras-chave no corpo ou assunto do email.

Mecanismo de verificação de email	Descrição
Filtragem de anexos	A filtragem de anexos permite configurar regras para filtrar que tipos de anexos de email serão permitidos e bloqueados no servidor de email.
Mecanismo de descompactação	O mecanismo de descompactação extrai e analisa arquivos compactados anexados a um email.
Filtragem de conteúdo avançada	A filtragem de conteúdo avançada permite fazer a verificação de dados do cabeçalho de emails e de conteúdo usando condições de pesquisa configuráveis avançadas e expressões regulares (regex).

2.4.3 Mecanismos de filtragem anti-spam

Os mecanismos a seguir verificam e bloqueiam spam.

FILTRO	DESCRIÇÃO	HABILITADO POR PADRÃO
SpamRazer	Um mecanismo anti-spam que determina se um email é spam usando a reputação do email, mensagem da "impressão digital" e análise de conteúdo.	Sim
Anti-phishing	Bloqueia emails que contêm links no corpo da mensagem que direcionam para sites de phishing conhecidos ou se eles contiverem palavras-chave de phishing conhecidas.	Sim
Coleta de diretório	Ataques do tipo Directory harvesting ocorrem quando os remetentes de spam tentam adivinhar endereços de email anexando nomes dos usuários conhecidos a seu domínio. A maioria dos endereços de email é inexistente.	Sim (somente se oGFI MailEssentials estiver instalado em um ambiente de Active Directory)
Lista de bloqueio de email	A Lista de bloqueio de email é um banco de dados personalizado de endereços de email e domínios do qual você não deseja receber emails.	Sim
Lista de bloqueio de IP	A Lista de bloqueio de IP é um banco de dados personalizado de endereços de email e domínios do qual você não deseja receber emails.	Não
Lista de bloqueio DNS IP	A Lista de bloqueio de DNS de IP verifica o endereço IP do servidor de email de envio em relação a uma lista de servidores de email conhecidos por serem remetentes de spam.	Sim
Lista de bloqueio DNS URI	Bloqueia emails que contêm links para domínios listados em lista de bloqueio de URI de spam públicas.	Sim
Estrutura de políticas do remetente	Este filtro usa registros SPF para bloquear emails enviados de endereços IP falsificados, identificando se o endereço IP do remetente é autorizado.	Não
Anti-spoofing	Verifica emails recebidos com um endereço de email do remetente originado de seu próprio domínio em relação a uma lista de endereços IP do GFI MailEssentials. Se o endereço IP do remetente não estiver na lista de endereços IP do servidor do domínio, o email será bloqueado.	Não
Detecção de idioma	Determina o idioma do texto do corpo do email e é configurável para bloquear certos idiomas.	Não
Verificação de cabeçalho	O filtro Verificação de cabeçalho analisa o cabeçalho de email para identificar emails com spam.	Não

FILTRO	DESCRIÇÃO	HABILITADO POR PADRÃO
Verificação de palavras-chave de spam	Este filtro permite a identificação do spam baseada em palavras-chave no email que está sendo recebido.	Não
Análise bayesiana	Um filtro anti-spam que pode ser treinado para determinar com precisão se um email é spam com base na experiência.	Não

2.4.4 Filtros executando no nível do SMTP

Os mecanismos a seguir verificam e bloqueiam emails durante a transmissão por SMTP antes que o email seja recebido. Para obter mais informações, consulte Filtragem da transmissão SMTP (página 152).

FILTRO	DESCRIÇÃO	HABILITADO POR PADRÃO
Lista de bloqueio de IP	A Lista de bloqueio de IP é um banco de dados personalizado de endereços de email e domínios do qual você não deseja receber emails.	Não
Coleta de diretório	Ataques do tipo Directory harvesting ocorrem quando os remetentes de spam tentam adivinhar endereços de email anexando nomes dos usuários conhecidos a seu domínio. A maioria dos endereços de email é inexistente.	Não
Lista de bloqueio DNS IP	A Lista de bloqueio de DNS de IP verifica o endereço IP do servidor de email de envio em relação a uma lista de servidores de email conhecidos por serem remetentes de spam.	Sim
Lista de exclusão temporária	O filtro Lista de exclusão temporária bloqueia temporariamente a entrada de emails recebidos de remetentes desconhecidos. Sistemas de email legítimos normalmente tentam enviar o email após alguns minutos. Os remetentes de spam simplesmente ignoram essas mensagens de erro.	Não

2.4.5 Outros mecanismos

Os mecanismos a seguir ajudam a identificar emails seguros.

FILTRO	DESCRIÇÃO	HABILITADO POR PADRÃO
Lista de permissão	A lista de permissão contém listas de critérios que identificam um email legítimo. Emails que correspondam a esses critérios não são examinados pelos filtros anti-spam e são sempre entregues ao destinatário.	Sim
Novos remetentes	O filtro Novos remetentes identifica emails que foram recebidos de remetentes para os quais emails nunca foram enviados.	Não

2.5 Cenários típicos de implantação

Este capítulo explica os diferentes cenários de instalação e configuração do GFI MailEssentials.

2.5.1 Instalação diretamente no servidor Microsoft® Exchange

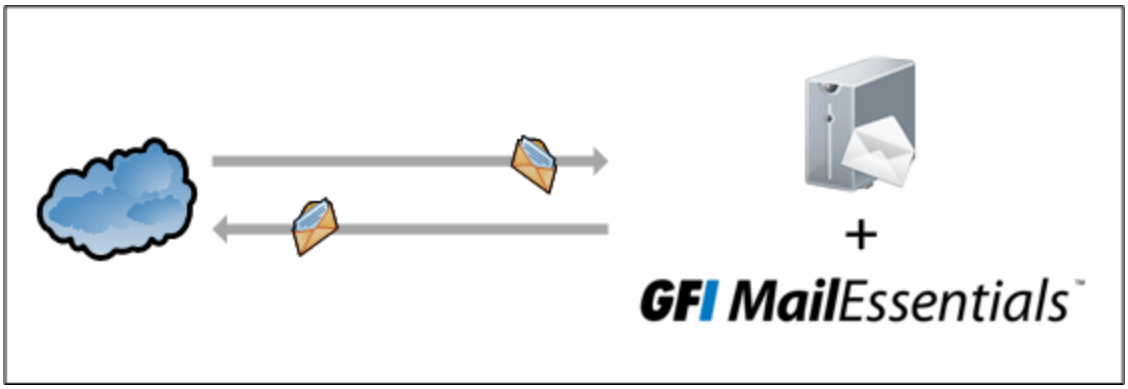


Figure 1: Instalar GFI MailEssentials no seu servidor Microsoft ® Exchange

Você pode instalar o GFI MailEssentials diretamente no Microsoft ® Exchange Server 2003 ou posterior, sem qualquer configuração adicional.

Nos ambientes Microsoft® Exchange 2007/2010, o GFI MailEssentials só pode ser instalado em servidores com as seguintes funções:

- Função de Servidor de Borda ou
- Função de Transporte de Hub ou
- Funções de Transporte de Hub e Caixa de Correio: com esta configuração, o GFI MailEssentials também pode fazer a verificação de vírus em emails internos

No Microsoft® Exchange 2013, o GFI MailEssentials só pode ser instalado no servidor com as seguinte funções:

- Função de transporte de borda ou
- Função caixa de correio.

> **OBS.**
> O GFI MailEssentials oferece suporte a vários servidores de email, mas só pode ser instalado na mesma máquina do Microsoft ® Exchange. No caso de outros servidores de email, por exemplo, o Lotus Domino, instale o GFI MailEssentials em uma máquina separada.

2.5.2 Instalar em um gateway de email ou servidor de retransmissão/perímetro

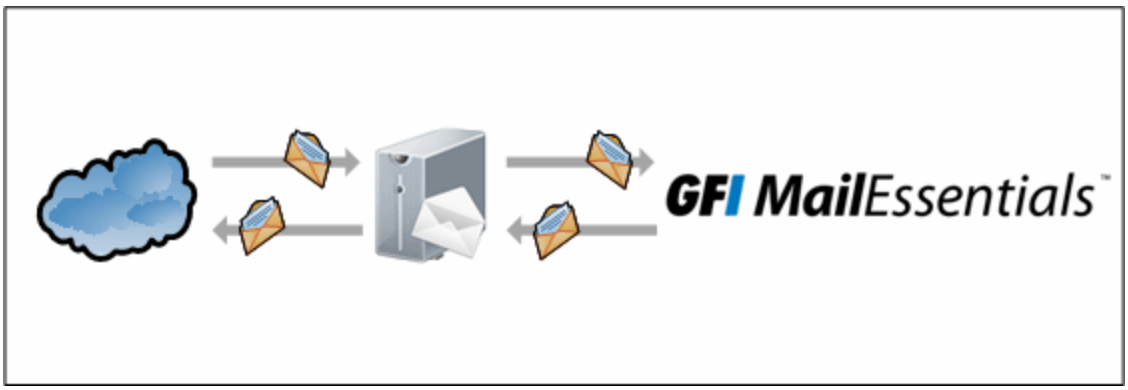


Figure 2: Instalar GFI MailEssentials em um gateway de email/servidor de retransmissão

Essa configuração é normalmente usada para filtrar spam em uma máquina separada, geralmente instalada em DMZ. Nesse ambiente, um servidor (também conhecido como gateway/servidor de perímetro) está configurado para encaminhar emails para o servidor de email. GFI MailEssentials está instalado no gateway/servidor de perímetro para que o spam e malware sejam filtrados antes de chegarem ao servidor de email.

Este método permite filtrar emails bloqueados antes que eles sejam recebidos no servidor de email e reduzir o tráfego desnecessário de email. Ele também oferece tolerância adicional a falhas. Se o servidor de email estiver fora do ar, você poderá receber emails, pois eles são enfileirados na máquina do GFI MailEssentials.

Quando instalado em um servidor separado (isto é, em um servidor que não seja o servidor de email), primeiro você deve configurar a máquina para atuar como um gateway (também conhecido como "host inteligente" ou "servidor de retransmissão de email"). Isso significa que todos os emails de entrada devem passar pelo GFI MailEssentials para verificação antes de serem retransmitidos para o servidor de email para distribuição. Para os emails de saída, o servidor de email deve retransmitir todos os emails de saída para a máquina gateway para verificação antes de serem enviados para o destino.

Se estiver utilizando um firewall, uma boa maneira de implantar o GFI MailEssentials na DMZ.GFI MailEssentials atuará como um host inteligente/servidor de retransmissão de email quando instalado na rede de perímetro (também conhecida como DMZ ou zona desmilitarizada).

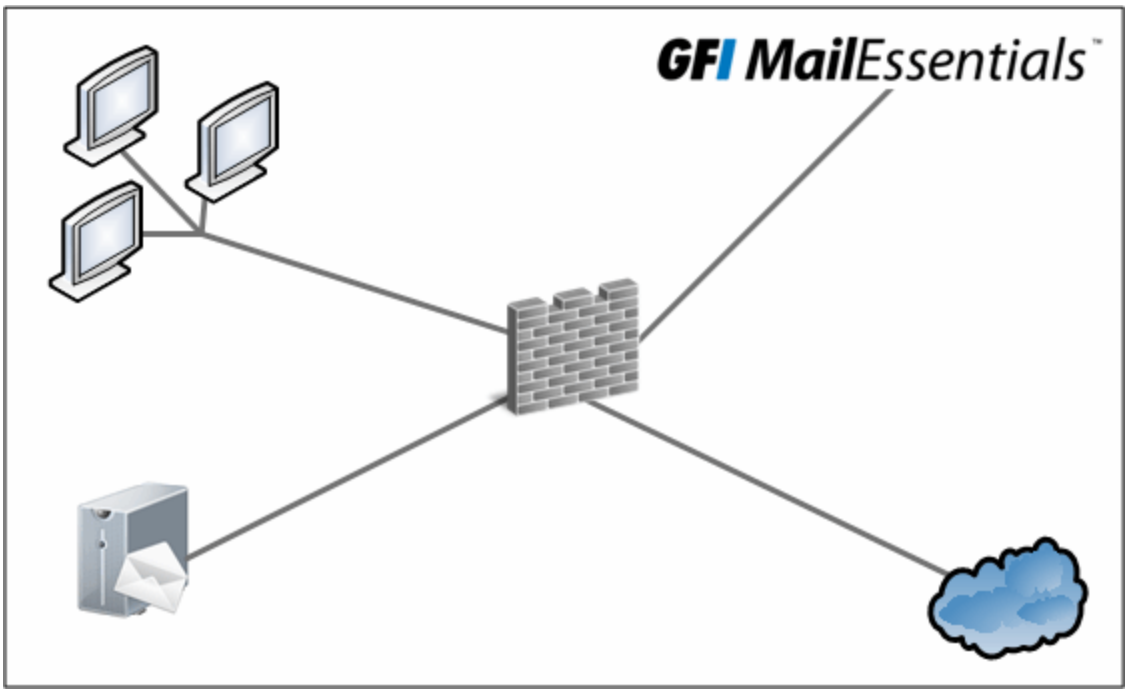


Figure 3: Instalação do GFI MailEssentials em uma máquina separada em uma DMZ

OBS.
Se o GFI MailEssentials tiver sido instalado no servidor de perímetro, você poderá usar os filtros anti-spam executados no nível do SMTP - Coleta de diretório e Lista de bloqueio temporária.

OBS.

Nos ambientes Microsoft® Exchange Server 2007/2010, os servidores de retransmissão de email em uma DMZ podem executar o Microsoft® Exchange Server 2007/2010 com a função de servidor Transporte de Borda.

OBS.

Configure o serviço IIS SMTP para encaminhar emails para seu servidor de email e configure o registro MX de seu domínio para apontar para a máquina gateway. Para obter mais informações, consulte Instalar em um gateway de email ou servidor de retransmissão/perímetro (página 27).

2.6 Ações do usuário final

GFI MailEssentials utiliza grupos do Active Directory para determinar o que é exibido para os usuários conectados quando eles fazem logon no GFI MailEssentials. Se o usuário conectado fizer parte do grupo de administradores, o GFI MailEssentialsserá carregado com todas as opções de configuração que permitem a configuração do GFI MailEssentials. Se o usuário conectado fizer parte do grupo de usuários, o GFI MailEssentials será carregado apenas com um número limitado de opções que permitem que o usuário conectado administre sua própria quarentena e listas de permissão/listas de bloqueio pessoais. O URL usado para fazer logon no GFI MailEssentials é sempre o mesmo, independentemente de o usuário conectado fazer parte do grupo do administrador ou do grupo do Active Directory.

OBSERVAÇÃO

As ações do usuário só estarão disponíveis se o GFI MailEssentials estiver configurado para usar o modo IIS. Para obter mais informações, consulte Modo da interface de usuário (página 250).

Lista de recursos disponíveis para as contas do usuário:

Recurso	Descrição
Listas de permissão e bloqueio pessoais	Os usuários podem configurar uma lista complementar de endereços de email nas listas de permissão e listas de bloqueio, acima da lista definida pelo administrador de sistemas. Este recurso está disponível apenas quando as Lista de permissão pessoal e/ou a Lista de bloqueio pessoal estão habilitadas. Por padrão essas opções não estão habilitadas.
Pesquisa de quarentena	Permite que os usuários acessem e gerenciem os emails de spam que foram colocados em quarentena. Os usuários podem pesquisar, visualizar e, em seguida, aprovar ou excluir os emails em quarentena. Para fazer uso deste recurso, a ação de filtros anti-spam deve ser configurada para colocar em quarentena os emails de spam. Os usuários não podem gerenciar emails de malware em quarentena devido aos riscos de segurança envolvidos.
SpamTag	Os usuários podem utilizar o complemento SpamTag no Microsoft Outlook para gerenciar suas preferências no gerenciamento de emails de spam. O SpamTag deve ser instalado nas máquinas dos usuários para estar acessível pelo Microsoft Outlook. **OBSERVAÇÃO:** Este recurso não está disponível para os usuários na interface da Web GFI MailEssentials. Para obter mais informações, consulte SpamTag para Microsoft Outlook (página 162).
MailInsights®	O MailInsights® é um recurso para relatórios que oferece uma apresentação gráfica dos 20 principais contatos com os quais um usuário se comunicou nos 30 dias anteriores.

Para obter mais informações sobre como os usuários finais podem utilizar o GFI MailEssentials, consulte o GFI MailEssentials Manual do usuário final.

3 Instalação

O objetivo deste capítulo é ajudá-lo a instalar o GFI MailEssentials em sua rede com o mínimo de esforço de configuração.

Tópicos deste capítulo:

3.1 Requisitos do sistema

3.1.1 Requisitos de hardware

Os requisitos mínimos de hardware do GFI MailEssentials são:

Processador

- Mínimo: 2 Ghz
- Recomendado: 2 GHz com vários núcleos

Memória disponível (RAM)

- Mínimo: 1.2 GB
- Recomendado: 1.5 GB

Espaço livre em disco

- Mínimo: 6 GB
- Recomendado: 10 GB

> **OBS.**
> Os requisitos de hardware dependem de diversos fatores, incluindo o volume de email e o número de mecanismos antivírus ativados no GFI MailEssentials. Os requisitos especificados acima são necessários somente para o GFI MailEssentials.

3.1.2 Requisitos de software

Sistemas operacionais compatíveis

» Windows® Server 2003 Standard ou Enterprise (x86 e x64) (incluindo R2) ou posterior (incluindo Microsoft® Windows Server 2012 - edições Standard e DataCenter).

» Windows Small Business Server 2003/2008/2011

Servidores de email compatíveis

O GFI MailEssentials pode ser instalado nos servidores de email a seguir sem qualquer configuração adicional.

» Microsoft® Exchange Server 2013

> **OBS.**
> O Information Store Protection (VSAPI) não é compatível com o Microsoft® Exchange Server 2013 porque o VSAPI foi removido do Microsoft® Exchange Server 2013.

» Microsoft® Exchange Server 2010

» Microsoft® Exchange Server 2007 SP1 ou superior

» Microsoft® Exchange Server 2003

Para obter mais informações, consulte Instalar no servidor Microsoft® Exchange (página 27).

O GFI MailEssentials também pode ser instalado em um ambiente com qualquer servidor de email compatível com SMTP. Nesse caso, o GFI MailEssentials deve ser instalado no servidor gateway/de perímetro para que o spam seja filtrado antes de chegar ao servidor de email.

Para obter mais informações, consulte Instalar em um gateway de email ou servidor de retransmissão/perímetro (página 27).

Navegadores de Internet compatíveis

O GFI MailEssentials pode ser usado com os seguintes navegadores da Internet:

» Microsoft Internet Explorer 8 ou posterior

» Google Chrome versão 22.0.1229.94 (10 de outubro de 2012) ou posterior

» Mozilla Firefox versão 16.0.2 (26 de outubro de 2012) ou posterior.

Outros componentes necessários

» Serviço World Wide Web dos Serviços de Informações da Internet (IIS®)

» Serviço SMTP dos Serviços de Informações da Internet (IIS®): exceto na instalação no servidor Microsoft® Exchange 2007/2010/2013

» Microsoft.NET® Framework 4

» Ativação HTTP WCF: necessária quando o plug-in do SpamTag for usado no Microsoft Outlook

» Função de Autenticação e Serviços de Conteúdo Estático do Windows®: necessários quando você faz a instalação no Microsoft® Windows Server 2008/2008R2

» MSMQ – Microsoft®Messaging Queuing Service – para obter mais informações consulte:

- Instalar o MSMQ no Windows Server 2012
- Instalar o MSMQ no Windows Server 2008
- Instalar o MSMQ no Windows Server 2003

OBS.
Para obter mais informações sobre como instalar os pré-requisitos no Microsoft® Windows Server 2008, consulte:
http://go.gfi.com/?pageid=ME_Win2008
Para obter mais informações sobre como instalar os pré-requisitos no Microsoft® Windows Server 2012, consulte:
http://go.gfi.com/?pageid=ME_Win2012

OBS.
A Information Store Protection do GFI MailEssentials não poderá ser usada se houver outro software estiver registrado para usar a VSAPI do Microsoft® Exchange.

OBS.
O GFI MailEssentials também pode ser instalado em ambientes virtuais como Microsoft® Hyper-V e software de virtualização da VMWare.

» O recurso de grupo de clusters do Microsoft Virtual Server com um cluster de disco físico. Isso é necessário SOMENTE para ambientes que executam clusters do Microsoft® Exchange 2003. Para obter mais informações, consulte Clusters do Microsoft® Exchange 2003 (página 31).

OBS.
Para obter mais informações sobre como criar um Grupo de Recursos para um Servidor Virtual do Exchange em um Cluster do Windows Server, consulte:http://go.gfi.com/?pageid=ME_Clusterresourcegrouphowto.

3.1.3 Software antivírus e de backup

A verificação do software antivírus e de backup pode causar problemas no GFI MailEssentials. Isso ocorre quando esses softwares negam o acesso a determinados arquivos exigidos pelo GFI MailEssentials.

Desative a verificação feita por softwares antivírus e de backup de terceiros nas seguintes pastas:

Instalações de 32 bits (x86)	Instalações de 64 bits (x64)
<..\Program Files\Common Files\GFI>	<..\Program Files (x86)\Common Files\GFI>
<GFI MailEssentials installation path>\GFI\MailEssentials\	
<..\Inetpub\mailroot> - se instalado em uma máquina gateway.	
<..\Program Files\Exchsrvr\Mailroot>: se instalado no mesmo computador do Microsoft® Exchange 2003	
<..\Program Files\Microsoft\Exchange Server\TransportRoles>: se instalado no mesmo computador do Microsoft® Exchange 2007	

Instalações de 32 bits (x86)	Instalações de 64 bits (x64)
<..*Program Files\Microsoft\Exchange Server\V14\TransportRoles*>: se instalado no mesmo computador do Microsoft® Exchange 2010	
<..*Program Files\Microsoft\Exchange Server\V15\TransportRoles*>: se instalado no mesmo computador do Microsoft® Exchange 2013	

3.1.4 Configurações da porta do firewall

Configure seu firewall para permitir as portas usadas pelo GFI MailEssentials.

Porta	Descrição
53 - DNS	Usada pelos seguintes filtros anti-spam: » Lista de bloqueio de DNS de IP » SpamRazer » Lista de bloqueio DNS URI
20 e 21 - FTP	Usadas pelo GFI MailEssentials para estabelecer uma conexão com **ftp.gfi.com** e recuperar as informações de versões mais recentes de produtos.
80 - HTTP	Usado pelo GFI MailEssentials para fazer o download de correções de produtos e atualizações para: » SpamRazer » Anti-phishing » Análise bayesiana » Arquivos de definição antivírus » Verificador de Cavalo de Troia e Executáveis » Mecanismo de exploração de email O GFI MailEssentials faz o download a partir dos seguintes locais: » http://update.gfi.com » http://update.gfisoftware.com » http://support.gfi.com » *.mailshell.com » *.spamrazer.gfi.com **OBS.:** O GFI MailEssentials também pode ser configurado para fazer o download de atualizações por meio de um servidor proxy. Para obter mais informações, consulte Configurações de proxy (página 241).
9090, 9091 - Comunicação remota	Essas portas são utilizadas para a comunicação entre processos. Não é necessário configurar um firewall para permitir conexões a ou a partir das portas remotas uma vez que todos os processos do GFI MailEssentials são executados no mesmo servidor. **OBS.:** Verifique se não há outros aplicativos (exceto GFI MailEssentials) escutando nessas portas. Se outros aplicativos estiverem usando essas portas, elas poderão ser alteradas. Para obter mais informações, consulte Portas remotas (página 279).
389/636 - LDAP/LDAPS	Esta porta é usada nestas situações: » Ambiente do **Microsoft® Exchange**: necessário se o servidor que executa o GFI MailEssentials não tiver acesso/não puder obter a lista de usuários do Active Directory, por exemplo, em um ambiente DMZ ou um outros ambientes que não usem o Active Directory. » **Lotus Domino mail server environment** - necessário para obter endereços de email no servidor Lotus Domino. » **Other SMTP mail server environments** - necessário para obter endereços de email do servidor SMTP.

3.2 Ações pré-instalação

Antes de instalar o GFI MailEssentials, prepare seu ambiente para a implementação.

Tópicos deste capítulo:

» Instalar no Microsoft Exchange Server

» Instalar em um gateway de email ou servidor de retransmissão/perímetro

» Clusters do Microsoft Exchange 2003

» Lotus Domino

3.2.1 Instalar no servidor Microsoft® Exchange

Quando você instalar o GFI MailEssentials no mesmo servidor do Microsoft® Exchange 2003 ou posterior, ações pré-instalação ou configurações não serão exigidas

Nos ambientes Microsoft® Exchange 2007/2010, o GFI MailEssentials só pode ser instalado em servidores com as seguintes funções:

» Função de Servidor de Borda ou

» Função de Transporte de Hub ou

» Funções de Transporte de Hub e Caixa de Correio: com esta configuração, o GFI MailEssentials também pode fazer a verificação de vírus em emails internos

No Microsoft® Exchange 2013, o GFI MailEssentials só pode ser instalado no servidor com as seguinte funções:

» Função de transporte de borda ou

» Função caixa de correio.

3.2.2 Instalar em um gateway de email ou servidor de retransmissão/perímetro

O GFI MailEssentials pode ser instalado:

» Em um servidor de perímetro (por exemplo, em um DMZ)

» Como um servidor de retransmissão de email entre o servidor SMTP de perímetro (gateway) e o servidor de email.

Essa configuração é normalmente usada para filtrar spam em uma máquina separada, geralmente instalada em DMZ. Nesse ambiente, um servidor (também conhecido como gateway/servidor de perímetro) está configurado para encaminhar emails para o servidor de email. GFI MailEssentials está instalado no gateway/servidor de perímetro para que o spam e malware sejam filtrados antes de chegarem ao servidor de email.

O GFI MailEssentials usa o serviço SMTP do IIS como o servidor SMTP e, portanto, o serviço SMTP do IIS deve ser configurado para funcionar como um servidor de retransmissão de email. Para fazer isso:

Etapa 1: Habilitar o serviço SMTP do IIS

Etapa 2: Criar domínios SMTP para a retransmissão de email

Etapa 3: Habilitar a retransmissão de email para seu servidor Microsoft® Exchange

Etapa 4: Proteger o servidor SMTP de retransmissão de email

Etapa 5: Ativar o servidor de email para rotear emails através do gateway

Etapa 6: Atualizar o registro MX de seu domínio para apontar para o servidor de retransmissão de email

Etapa 7: Testar o novo servidor de retransmissão de email

Etapa 1: Habilitar o serviço SMTP do IIS

Windows Server 2003

1. Acesse **Start > Control Panel > Add or Remove Programs > Add/Remove Windows Components**.
2. Selecione **Application Server** e clique em **Details**.
3. Selecione **Internet Information Services (IIS)** e clique em **Details**.
4. Selecione a opção **SMTP Service** e clique em **OK**.
5. Clique em **Next** para finalizar sua configuração.

Windows Server 2008

1. Inicie o Gerenciador de Servidores do Windows.
2. Acesse o nó **Features** e selecione **Add Features**.
3. No **Add Features Wizard**, selecione **SMTP Server**.

> **OBS.**
> O recurso Servidor SMTP pode exigir a instalação de serviços de função e recursos adicionais. Clique em **Add Required Role Services** para continuar a instalação.

4. Nas telas a seguir, clique em **Next** para configurar todos os serviços de função e recursos necessários e clique em **Install** para iniciar a instalação.
5. Clique em **Close** para concluir a configuração.

Etapa 2: Criar domínios SMTP para retransmissão de email

1. Acesse **Start > Control Panel > Administrative Tools > Internet Information Services (IIS) Manager**.

2. No painel esquerdo, expanda o respectivo nó de servidor. Clique com o botão direito do mouse em **Default SMTP Virtual Server** e selecione **Properties**.

4. Expanda o nó **Default SMTP Virtual Server**.

5. Clique com o botão direito do mouse em **Domains** e selecione **New > Domain**.

6. Selecione **Remote** e clique em **Next**.

7. Especifique o nome de domínio da organização (por exemplo, teste.meudominio.com) e clique em **Finish**.

Etapa 3: Como ativar a retransmissão de email para seu servidor Microsoft® Exchange

1. Clique com o botão direito do mouse no novo domínio e selecione **Properties**.

2. Selecione **Allow the Incoming Mail to be Relayed to this Domain**.

3. Selecione **Forward all mail to smart host** e especifique o endereço IP do servidor que gerencia as mensagens de email deste domínio. O endereço IP deve ser delimitado por colchetes, por exemplo, `[123.123.123.123]`, para excluí-los de todas as tentativas de pesquisa de DNS.

4. Clique em **OK** para finalizar suas configurações.

Etapa 4: Proteger seu servidor de retransmissão SMTP

Se não estiver protegido, seu servidor de retransmissão de email poderá ser explorado e usado como uma retransmissão aberta de spam. Para evitar isso, é recomendável que você especifique quais servidores de email podem rotear emails através deste servidor de retransmissão de email (por exemplo, permita somente que servidores específicos usem essa configuração de retransmissão de email). Para isso:

1. Acesse **Start > Control Panel > Administrative Tools > Internet Information Services (IIS) Manager**.

2. No painel esquerdo, expanda o respectivo nó de servidor. Clique com o botão direito do mouse em **Default SMTP Virtual Server** e selecione **Properties**.

3. Na guia **Access**, selecione **Relay**.

4. Selecione **Only the list below** e clique em **Add**.

5. Especifique os IPs dos servidores de email internos que têm permissão para rotear emails através de seu servidor de retransmissão de email. Você pode especificar:

» Computadores simples: autorize uma máquina específica a retransmitir email por esse servidor. Use o botão Pesquisa de DNS para procurar um endereço IP de um host específico.

» Grupo de computadores: autorize computadores específicos a encaminhar emails por meio deste servidor.

» Domínio: permita que todos os computadores em um domínio específico encaminhem emails por meio deste servidor.

> **OBS.**
> A opção **Domain** adiciona uma sobrecarga de processamento que pode degradar o desempenho do serviço SMTP. Isso acontece devido à pesquisa de DNS reversa acionada em todos os endereços IP (dentro desse domínio) que tentam rotear emails através deste servidor de retransmissão.

Etapa 5: Habilitar o servidor de email para rotear emails através do GFI MailEssentials

Microsoft® Exchange Server 2003

Configure conectores SMTP que encaminhem todos os emails para o GFI MailEssentials.

1. Inicie o **Exchange System Manager**.

2. Clique com o botão direito do mouse em **Connectors**, clique em **New > SMTP Connector** e especificar um nome de conector.

3. Selecione **Forward all mail through this connector to the following smart host** e especifique o IP do servidor de retransmissão do GFI MailEssentialsentre colchetes, por exemplo, `[123.123.1.123]`.

4. Clique em **Add** e selecione o servidor de retransmissão de email do GFI MailEssentials.

5. Clique em **OK**.

6. Acesse a guia **Address Space**.

7. Clique em **Add**, selecione **SMTP** e clique em **OK**.

8. Digite o nome do domínio e clique em **OK**.

9. Selecione **Allow messages to be relayed to these domains**.

10. Clique em **OK**.

Lotus Notes

Para obter mais informações sobre como configurar o roteamento no Lotus Domino, consulte o Installation Guide(Domino).

Servidor de email SMTP/POP3

Configure seu servidor de email para rotear todos os emails de entrada e saída por meio do GFI MailEssentials No programa de configuração de seu servidor de email, use a opção de retransmitir todos os emails de saída por meio de outro servidor de email (esta opção é normalmente denominada com algo semelhante a **Forward all messages to host**. Digite o nome do computador ou o IP da máquina que executa o GFI MailEssentials. Salve as novas configurações e reinicie o servidor de email.

Etapa 6: Atualizar o registro MX de seu domínio para que ele aponte para o servidor de retransmissão de email

Atualize o registro MX de seu domínio para que aponte para o IP do novo servidor de retransmissão de email. Se seu servidor DNS for gerenciado pelo seu provedor de serviços de Internet, peça ao provedor para atualizar o registro MX para você.

> **OBS.**
> Se o registro MX não for atualizado, todos os emails serão roteados diretamente para o servidor de email, ignorando o GFI MailEssentials.

Como verificar se o registro MX foi atualizado

Para verificar se o registro MX foi atualizado:

1. No prompt de comando, digite em `nslookup` e pressione **Enter**.

2. Digite `set type=mx` e pressione **Enter**.

3. Especifique o nome do domínio de email e pressione **Enter**.

O registro MX deverá retornar os endereços IP dos servidores de retransmissão de email.

Etapa 7: Como testar seu novo servidor de retransmissão de email

Antes de instalar o GFI MailEssentials, verifique se o novo servidor de retransmissão de email está funcionando corretamente.

Como testar a conexão de entrada SMTP do IIS

1. Envie um email de uma conta "externa" (por exemplo, de uma conta do Gmail) para um endereço de email/usuário interno.

2. Confirme se o destinatário pretendido recebeu o email de teste no respectivo cliente de email.

Testar a conexão de saída SMTP do IIS

1. Envie um email a partir de uma conta de email "interna" para uma conta de externa (exemplo, uma conta Gmail).

2. Confirme se o destinatário/usuário externo desejado recebeu o email de teste.

> **OBS.**
> Você também pode usar o Telnet para enviar manualmente o email de teste e obter mais informações sobre solução de problemas. Para obter mais informações, consulte:
> http://go.gfi.com/?pageid=ME_TelnetPort25

3.2.3 Clusters do Microsoft® Exchange 2003

Este tópico contém instruções sobre como instalar e desinstalar o GFI MailEssentials em clusters do Microsoft® Exchange 2003.

Um cluster é um grupo de servidores, tecnicamente conhecidos como nós, que trabalham coletivamente como um único servidor. Esse ambiente oferece alta disponibilidade e mecanismos failover para garantir a disponibilidade constante de recursos e aplicativos, incluindo infraestruturas de email. Se um dos nós no cluster falhar/não estiver disponível, os recursos e aplicativos migrarão para outro nó do cluster.

> **OBS.**
> O GFI MailEssentials só pode ser instalado em um ambiente de cluster Ativo-Passivo. Em um cluster ativo/passivo, um mecanismo de "failover" garante que sempre que um cluster ativo falhar, um dos nós passivos disponíveis se tornará ativo (ou seja, assumirá a função do nó com falha).

Para instalar o GFI MailEssentials em um cluster do Microsoft® Exchange Server 2000/2003 certifique-se de que:

» Todos os aplicativos estejam fechados.

» O Microsoft® Exchange Server 2000/2003 esteja instalado no modo de cluster.

» Um recurso de grupo de cluster do Servidor Virtual do Exchange existe e contém, além de outros elementos, um recurso de cluster de disco físico.

» Todos os nós do cluster devem estar desativados, exceto o nó no qual o GFI MailEssentials será instalado primeiramente.

1. Inicie o processo de instalação e certifique-se de que:

- Todos os arquivos estejam instalados na unidade de disco rígido compartilhada
- Se você estiver instalando no website padrão da máquina

2. Ao concluir, inicie o website padrão usando o Gerenciador do IIS.

3. Acesse **Control Panel > Administrative Tools > Cluster Administrator** e crie um novo grupo de recursos (clique com o botão direito do mouse em **Groups > New > Group**).

4. Digite `GFI MailEssentials` como o nome e `Services for GFI MailEssentials` como a descrição. Clique em **Next**.

5. Mova todos os nós disponíveis para **Preferred Owners** e clique em **Finish**.

6. Clique com o botão direito do mouse em **GFI MailEssentials > New > Resource**.

7. Defina o nome para `GFI List Server`.

8. Configure o Tipo de recurso para Serviço Genérico e clique em **Next**.

9. Configure todos os nós disponíveis para os possíveis proprietários e clique em **Next**.

10. Clique em **Next**.

11. Defina o nome do serviço para `listserv` e clique em Avançar.

12. Clique em **Finish**.

13. Repita os passos de 7 a 12 com as seguintes informações:

Nome	Nome do serviço
GFI MailEssentials AS Scan Engine	gfiscans
GFI MailEssentials Attendant	gfimesattendant
GFI MailEssentials Autoupdater	gfimesavupdate
GFI MailEssentials AV Scan Engine	GFIScanM
GFI MailEssentials Backend	gfimesbackend
GFI MailEssentials Enterprise Transfer	gfimetrxsvc
GFI MailEssentials Legacy Attendant	gfiasmsecatt
GFI MailEssentials Quarantine Action Services	gfimesqashost
GFI POP2Exchange	gfipop2exch

14. Ao concluir, ative o grupo do GFI MailEssentials.

15. Desative este nó e inicie um novo nó.

16. Repita as etapas 1 e 2 para todos os nós de cluster.

Desinstalar o GFI MailEssentials em um ambiente de cluster

Garanta que apenas um nó de cluster esteja ativado. Todos os outros devem estar desativados.

1. Interrompa todos os serviços da GFI

2. Faça o backup do conteúdo na pasta de instalação do GFI MailEssentials em um local diferente.

3. Exclua todos os Serviços da GFI de Cluster Resources do GFI MailEssentials do grupo.

4. Inicie todos os serviços da GFI e garanta que todos os serviços de cluster e serviços Exchange estejam funcionando.

5. Desinstale a partir do primeiro nó.

6. Abra o miniaplicativo de serviços para certificar-se de que não existe nenhum serviço do GFI MailEssentials que não tenha sido excluído. Para cada serviço que ainda esteja presente no miniaplicativo de serviços, execute o seguinte comando no prompt de comando: `sc delete <Nome do serviço>`. Por exemplo, execute `sc delete gfiasmsecatt` se o Legacy Attendant do GFI MailEssentials ainda estiver presente.

7. Abra o editor de registro do sistema e exclua a chave: `Computer\HKEY_LOCAL_MACHINE\SOFTWARE\GFI`

8. Copie o backup de GFI MailEssentials para onde ele foi instalado.

9. Desative o nó atual e inicie o próximo nó. Certifique-se de que todos os serviços de cluster, serviços do Exchange e serviços do GFI MailEssentials estejam ativos e funcionando

10. Desinstale o GFI MailEssentials.

11. Abra o miniaplicativo de serviços para certificar-se de que não existe nenhum serviço do GFI MailEssentials que não tenha sido excluído. Para cada serviço que ainda esteja presente no miniaplicativo de serviços, execute o seguinte comando no prompt de comando: `sc delete <Nome do serviço>`. Por exemplo, execute `sc delete gfiasmsecatt` se o Legacy Attendant do GFI MailEssentials ainda estiver presente.

12. Repetir os passos 7 ao 11 para todos os nós restantes.

13. Exclua a pasta de instalação e seu backup do GFI MailEssentials. No administrador do cluster, exclua todos os serviços da GFI.

3.2.4 Lotus Domino

Informações sobre o uso do GFI MailEssentials com o Lotus Domino.

» Incompatibilidades do Lotus Domino

» Informações sobre a instalação do Lotus Domino

» Configuração da pasta anti-spam do Lotus Domino

Incompatibilidades do Lotus Domino

Memos/emails internos não são verificados

O GFI MailEssentials não verifica os memorandos/emails internos enviados pelo Lotus Domino, pois o formato do remetente/destinatário do Lotus Domino não está em um formato compatível. Quando os memorandos/emails internos são passados para o GFI MailEssentials, eles acabam no topo da fila e não são processados.

> **OBS.**
> Não passe memorandos/emails internos por meio do GFI MailEssentials.

O Servidor de Lista do GFI MailEssentials não funciona com o Lotus Domino

A criação de boletins informativos ou listas de discussão não funciona no domínio interno do Lotus Domino. Essa opção não deve ser usada. Se for usada, os usuários do Lotus Domino não serão capazes de enviar emails para a lista.

Guia de instalação do GFI MailEssentials para Lotus Domino

Use as informações nesta seção para instalar e configurar o Lotus Domino com o GFI MailEssentials. Instale o GFI MailEssentials em uma máquina separada e, em seguida, instale o Lotus Domino, como mostrado na figura abaixo.

Figure 4: Instalação do GFI MailEssentials em um servidor separado de Lotus Domino

Instale o GFI MailEssentials executando o arquivo de instalação do GFI MailEssentials e seguindo as instruções na tela. Para obter mais informações, consulte Instalação (página 23).

Se o GFI MailEssentials estiver instalado em uma máquina com o Active Directory, o diálogo a seguir poderá ser exibida. Selecione **No, I do not have Active Directory…** para instalar o GFI MailEssentials no modo SMTP.

Configure a máquina na qual o GFI MailEssentials estiver instalado para funcionar como um gateway (também conhecido como "smart host" ou servidor de "retransmissão de email") para todos os emails. Efetivamente, todos os emails de entrada devem passar por essa máquina antes de serem retransmitidos para o servidor de email para distribuição (é o primeiro a receber todos os emails destinados a seu servidor de email).

O mesmo se aplica aos emails de saída. O servidor de email deve retransmitir todos os emails de saída para a máquina de gateway para verificação antes que esses emails sejam enviados para destinatários externos pela Internet (ele precisa ser a última "parada" para emails destinados à Internet). Dessa forma, o GFI MailEssentials verifica todos os emails de entrada e de saída enviados para os destinatários.

O registro MX de seu domínio deve apontar para o servidor de retransmissão de emails

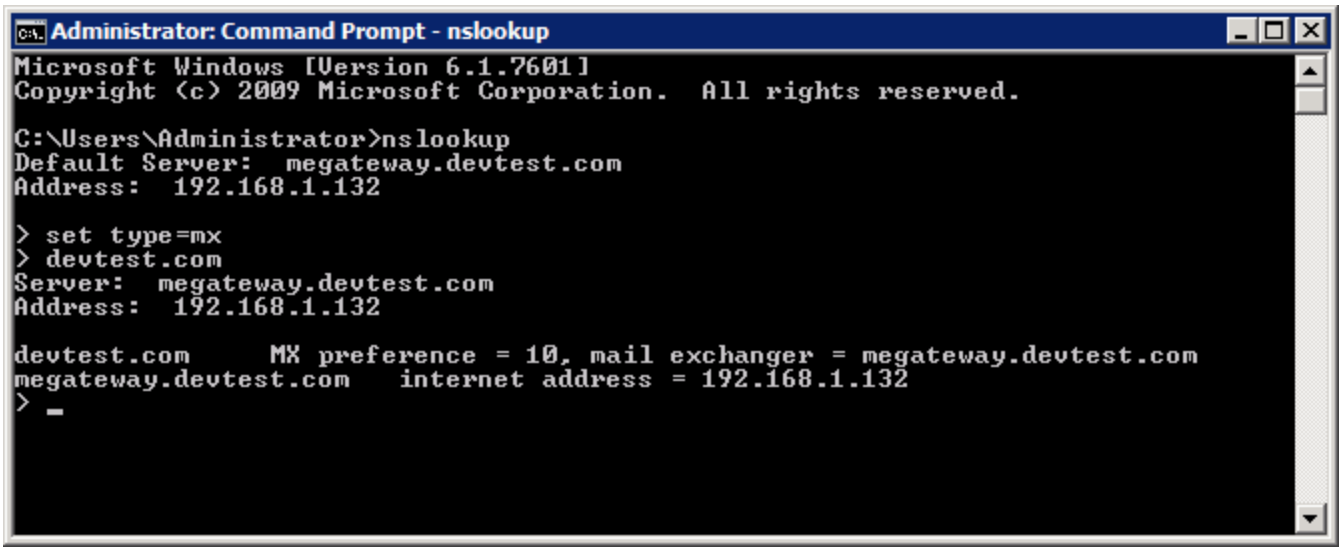
> **OBS.**
> Se seu ISP gerencia o servidor DNS, solicite que esse provedor faça a atualização para você.

Como o novo servidor de retransmissão de email deve receber primeiro todos os emails de entrada, atualize o registro MX de seu domínio para que ele aponte para o IP do novo servidor de retransmissão de email/gateway.

Verifique o registro MX de seu servidor DNS da seguinte forma:

1. No prompt de comando, digite `nslookup` e pressione **Enter**.
2. Digite `set type=mx` e pressione **Enter**.
3. Digite o domínio do email e pressione **Enter**.

O registro MX deve retornar um único IP que corresponda ao endereço IP da máquina que executa o GFI MailEssentials.



Screenshot 1: Como verificar o registro MX do DNS

4. Teste o novo servidor de retransmissão de email. Antes de instalar o GFI MailEssentials, verifique se o novo servidor de retransmissão de email está funcionando corretamente.

5. Teste a conexão de entrada SMTP do IIS do servidor de retransmissão de email enviando um email de uma conta externa para um usuário interno (use o webmail, por exemplo **mail.live.com** se não tiver uma conta externa disponível). Verifique se o cliente de email recebeu o email.

6. Teste a conexão de saída SMTP do IIS do servidor de retransmissão de email enviando um email para uma conta externa de um cliente de email. Verifique se o usuário externo recebeu o email.

> **OBS.**
> Como alternativa, em vez de um cliente de email, envie o email manualmente através do Telnet. Isso fornecerá mais informações sobre solução de problemas.

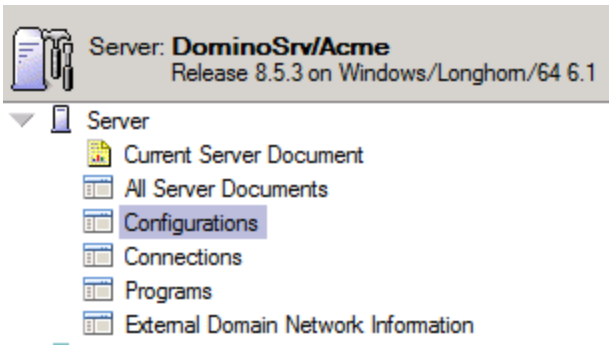
Para obter mais informações, consulte:

http://support.microsoft.com/support/kb/articles/Q153/1/19.asp

Configurar o Lotus Domino para enviar emails de saída através do GFI MailEssentials

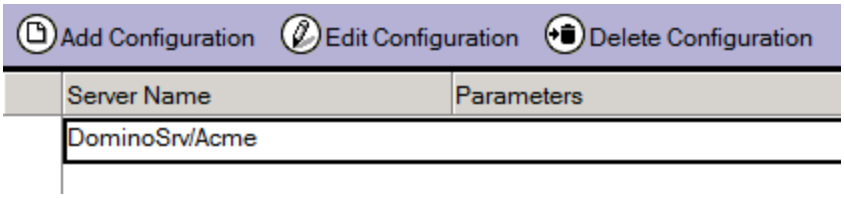
Para direcionar todos os emails de saída para o servidor no qual o GFI MailEssentials está instalado, o Lotus Domino precisa ser configurado como descrito a seguir.

1. No Lotus Domino Administrator, clique na guia **Configuration** e selecione **Server > Configurations**.



Screenshot 2: Lotus Domino Administrator - clique na opção Configurations.

2. Depois que a seção de configuração for selecionada, a janela principal mostrará a configuração do servidor. Selecione o servidor desejado e clique em **Edit configuration**.

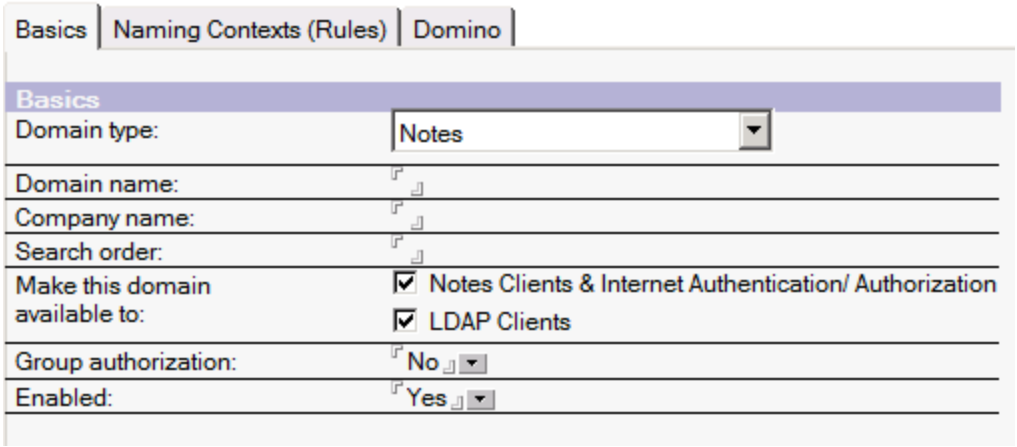


Screenshot 3: Clique em Edit configuration

Na página de configuração do documento, selecione a guia **Router/SMTP** e certifique-se de que a opção **Basics** esteja selecionada. Clique duas vezes no conteúdo para ativar o modo de edição. Selecione **Relay host for messages leaving the local internet domain** e digite o endereço IP da máquina na qual o GFI MailEssentials está instalado. Clique em **Save and Close** para salvar o documento de configuração.

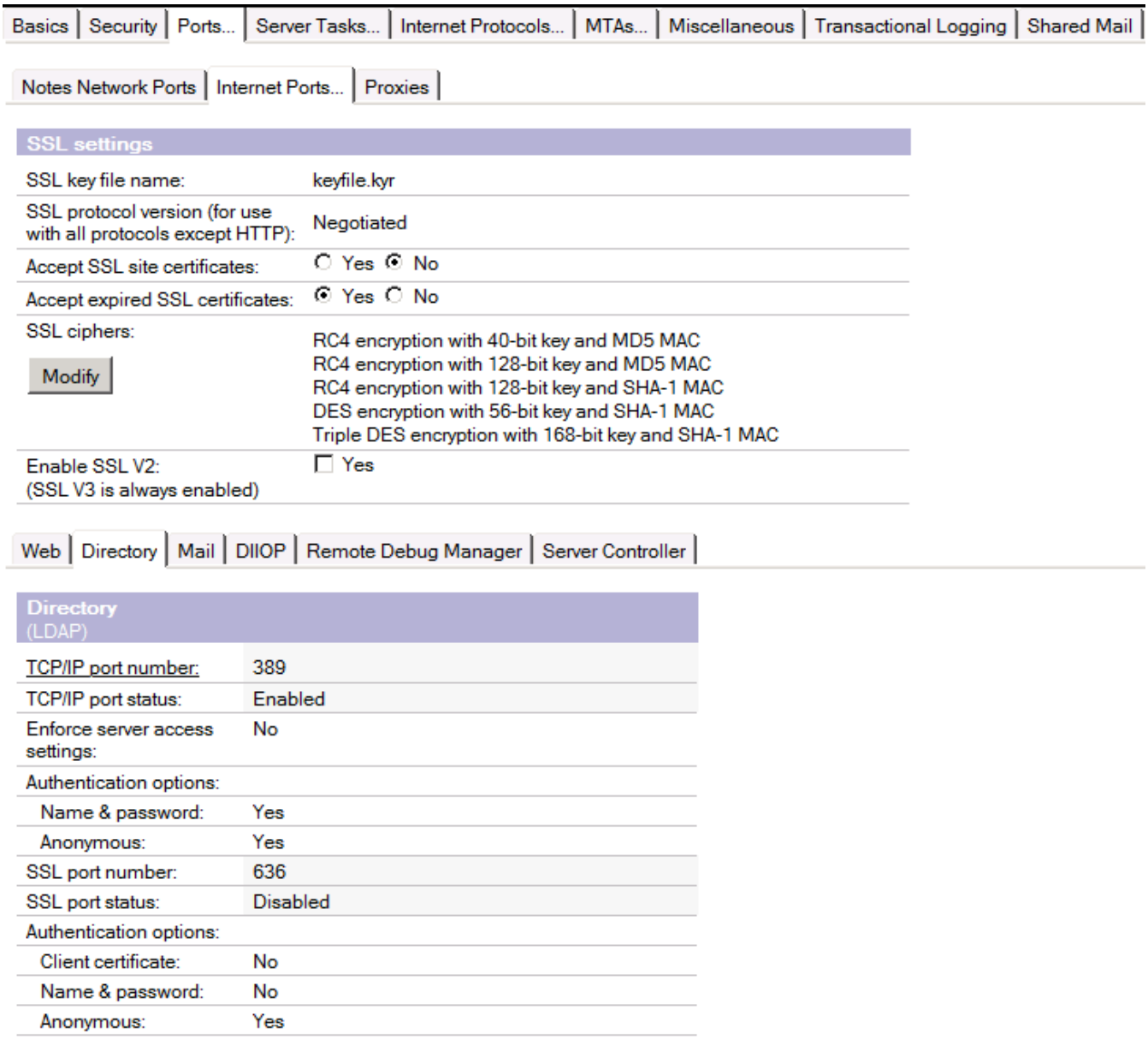
Configurações LDAP do Lotus Domino

No Lotus Domino, habilite Directory Catalog e Directory Assistance. No banco de dados Directory Assistance, clique em **Add Directory Assistance** para criar um novo documento de assistência. No documento, é necessário ativar os clientes LDAP em **Make this domain available to** da seguinte forma:



Screenshot 4: Configurações LDAP do Lotus Domino

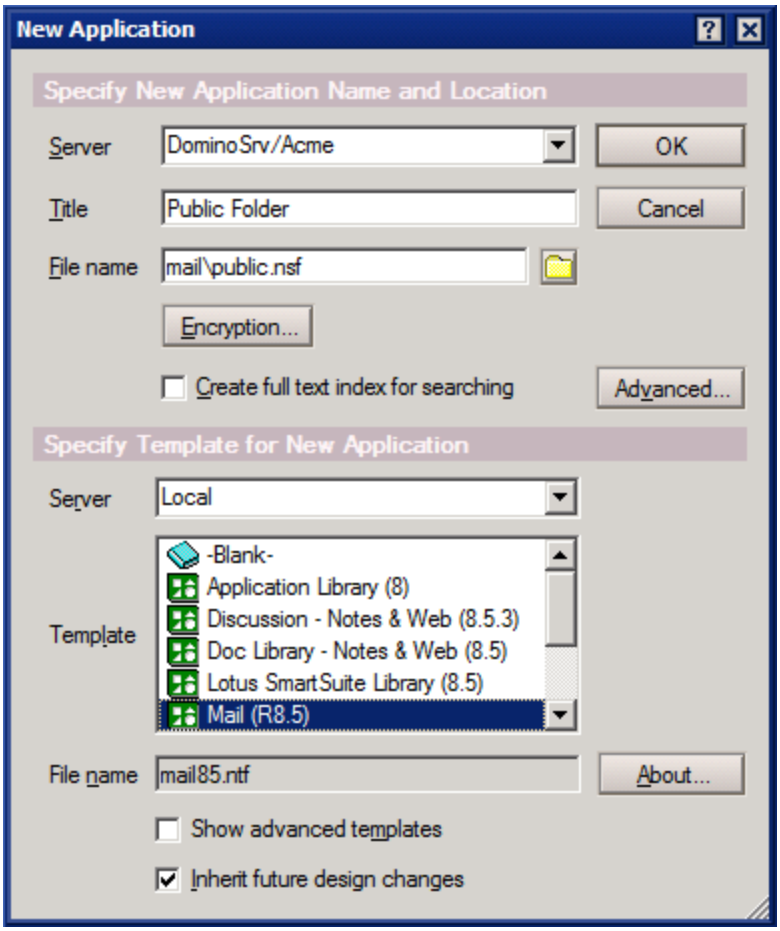
Na configuração do servidor, é necessário editar as credenciais na configuração. A autenticação anônima deve ser habilitada para que o GFI MailEssentials possa acessar o Lotus Domino LDAP.



Screenshot 5: Habilitar a autenticação anônima

Configuração da pasta anti-spam do Lotus Domino

1. No Administrador Lotus Notes, crie um banco de dados com o modelo mail85.ntf normal, que será usado como a pasta pública. Quando o banco de dados for criado, clique com o botão direito do mouse no banco de dados na seção de arquivos e selecione **Access Control**. Configure o usuário ou o grupo ou o servidor para ter acesso ao banco de dados.



Screenshot 6: Criar um novo banco de dados

2. Converta o banco de dados usando o console do servidor digitando:

```
load convert -e -h mail\public.nsf
```

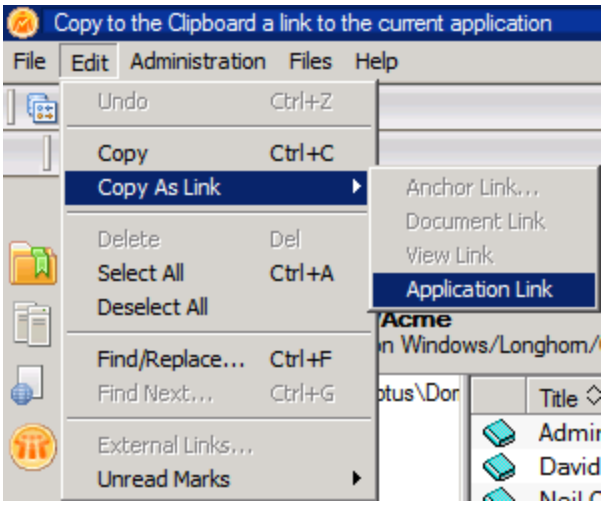
O comando deve exibir os resultados a seguir.

```
load convert -e -h mail\public.nsf

[0A34:0002-06F4] 19/09/2012 16:48:43   Mail Conversion Utility starting
[0A34:0002-06F4] 19/09/2012 16:48:43   Mail Convert: Started enabling NSF support for IMAP
in 'mail\public.nsf'
[0A34:0002-06F4] 19/09/2012 16:48:43   Mail Convert: Finished enabling NSF support for IMAP
in 'mail\public.nsf'
[0A34:0002-06F4] 19/09/2012 16:48:43   Mail Convert: Started adding IMAP specific items in
'mail\public.nsf'
[0A34:0002-06F4] 19/09/2012 16:48:43   Mail Convert: Finished adding IMAP specific items in
'mail\public.nsf'. 0 messages succeeded, 0 messages failed.
[0A34:0002-06F4] 19/09/2012 16:48:43   Mail Conversion Utility shutdown
```

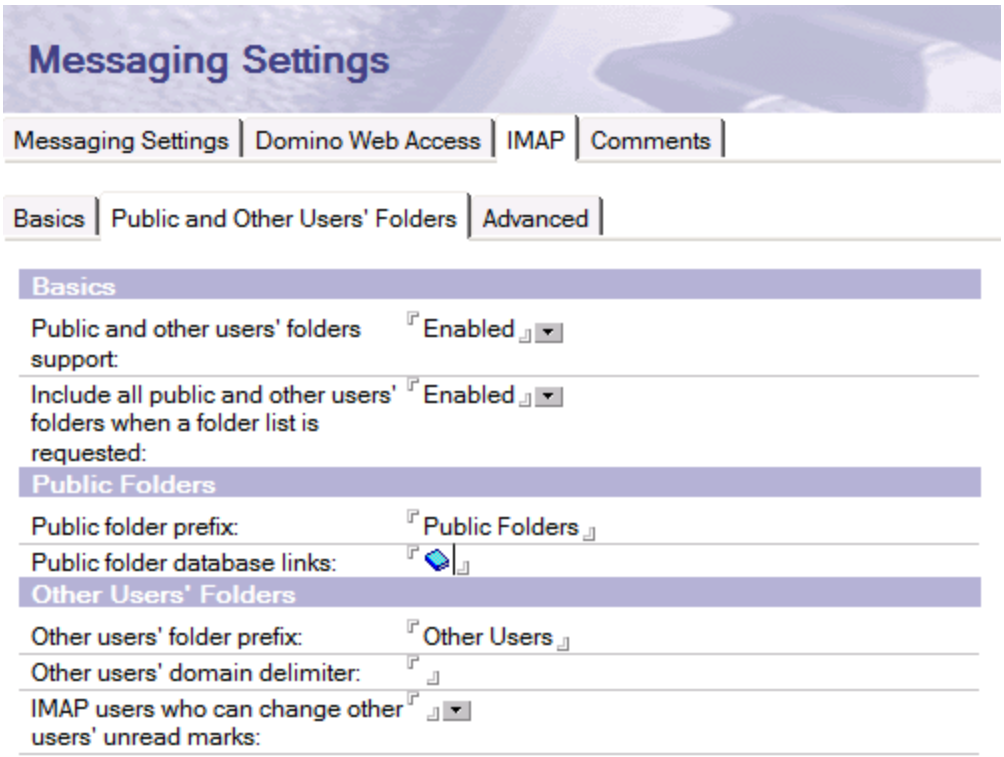
Screenshot 7: Carregar o resultado da conversão

3. Ao concluir, certifique-se de que o banco de dados possa ser acessado a partir do serviço IMAP. No Administrador Lotus Notes, acesse **Configuration** e selecione a guia **Files**. Selecione o banco de dados da pasta pública, clique em **Edit**, selecione **Copy as Link** e clique em **Application Link**.



Screenshot 8: Copie na área de transferência um link para o aplicativo atual

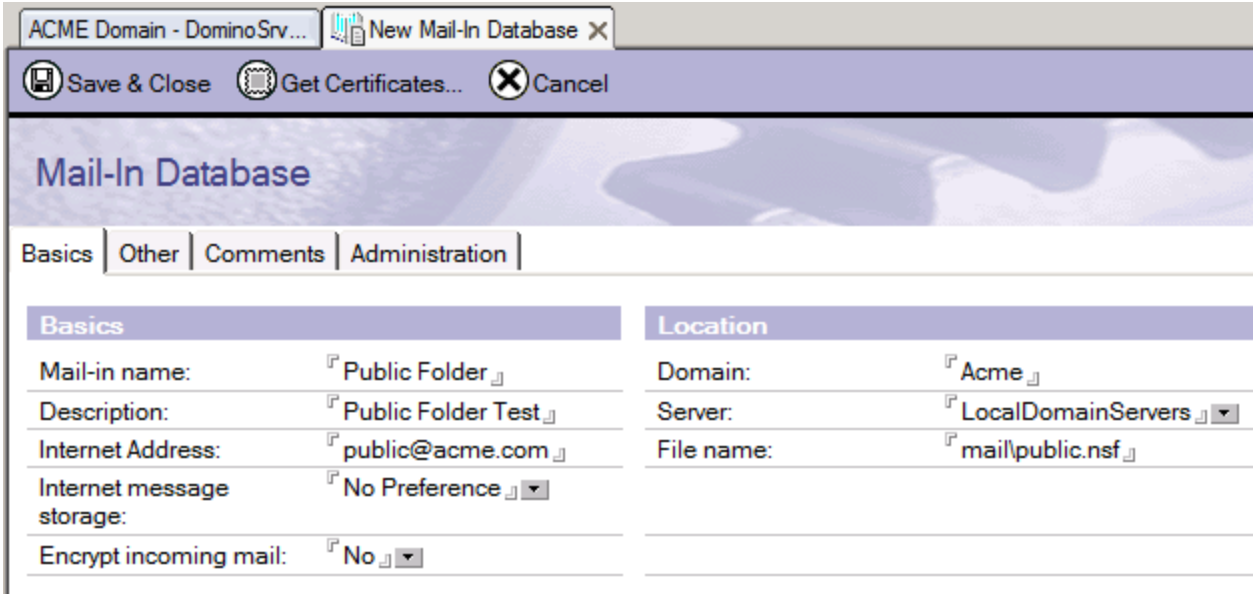
4. Na configuração, acesse **Messaging Settings** e selecione a guia **IMAP**.



Screenshot 9: Inclua todas as pastas públicas e de outros usuários quando uma lista de pastas for solicitada

5. Selecione a guia **Public and Other Users' Folders**. Clique com o botão direito do mouse e cole nos **Public Folders Database Links** e habilite a opção **Include all public and other users folders when a folder list is requested**.

6. Salve e feche o documento.



Screenshot 10: Novo email no banco de dados

7. No Lotus Notes Administrator, configure a pasta a ser usada pelo email. Acesse **People and Groups** e selecione **Mail-In Database**. Crie um novo Mail-in Database e, no caminho completo do diretório, digite o caminho completo (por exemplo, Mail\public.ns).

8. Salve e feche o documento.

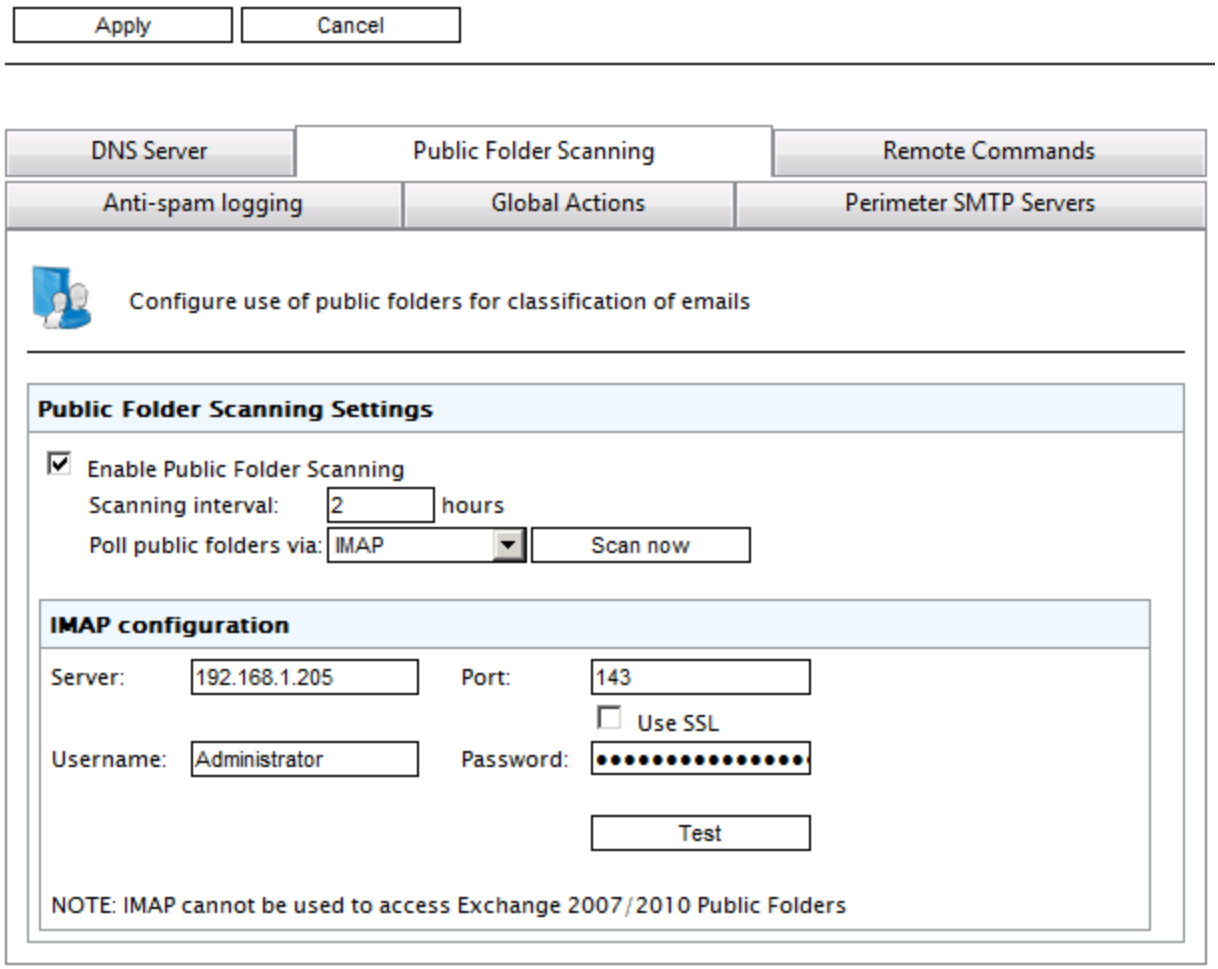
9. Na GFI MailEssentialsinterface da Web, expanda **AntiSpam** e selecione **AntiSpam Settings**.

10. No lado direito, selecione a guia **Public Folder Scanning** e ative **Public Folder Scanning**.

11. Na seção **IMAP configuration**, digite o servidor de IMAP (no servidor Lotus Domino, Port e as credenciais do usuário para acessar a pasta).

> **OBS.**
> O botão de teste não funcionará.

12. Clique em **Apply** para salvar as alterações.



Screenshot 11: Habilitar a verificação de pasta pública

13. No Registro, altere os valores a serem usados nesta função. No Registro, selecione `HKEY_LOCAL_MACHINE\SOFTWARE\GFI\ME12\ATTENDANT\RPFOLDERS:5` e crie o seguinte Key String Value:

```
Nome/Valor
SharedNamespace Public Folders\\Public Folder
FolderDelimiter \\
```

3.3 Procedimento de instalação

Esta seção descreve como executar a instalação do GFI MailEssentials.

3.3.1 Observações importantes

1. Se você estiver utilizando uma versão anterior do GFI MailEssentials, poderá atualizar a instalação atual mantendo todas as definições de configuração existentes. A atualização não é reversível. Você não poderá fazer o downgrade para a versão anterior.Para obter mais informações, consulte Atualização de uma versão anterior (página 49).

2. Se estiver usando SMA e quiser fazer o upgrade, acesse a área do cliente do site da GFI para atualizar a chave de licença.

OBS.
A avaliação não é mais aceita como uma chave de licença. Acesse a área do cliente do site da GFI para atualizar a chave da licença antes de iniciar o processo de atualização.

3. Faça o download da compilação do GFI MailEssentials apropriado para seu tipo de máquina. Use a instalação de 32 bits (x86) do GFI MailEssentials em sistemas de 32 bits e a instalação de 64 bits (x64) em sistemas de 64 bits.

4. Antes de executar o assistente de instalação, certifique-se de que:

» Você efetuou logon com uma conta com privilégios administrativos.

» A máquina na qual GFI MailEssentials será instalado, atende aos requisitos de sistema indicados. Para obter mais informações, consulte Requisitos do sistema (página 23).

» Configure seu firewall para permitir que o GFI MailEssentials estabeleça uma conexão com servidores GFI. Para obter mais informações, consulte Configurações da porta do firewall (página 26).

» Desabilite software antivírus e de backup de terceiros nas pastas de verificação usadas pelo GFI MailEssentials. Para obter mais informações, consulte Software antivírus e de backup (página 25).

» Se estiver instalando o GFI MailEssentials em um gateway de email ou servidor de retransmissão/perímetro, configure a máquina para funcionar como um gateway. Para obter mais informações, consulte Instalar em um gateway de email ou servidor de retransmissão/perímetro (página 27).

» Salve todos os trabalhos em execução e feche todos os aplicativos abertos no computador.

6. A instalação do GFI MailEssentials reiniciará Microsoft® Exchange ou os serviços SMTP do Microsoft IIS®. Isso é necessário para permitir que os componentes do GFI MailEssentials sejam registrados corretamente. É recomendável instalar o GFI MailEssentials em um momento no qual a reinicialização desses serviços tenha impacto mínimo em sua rede.

3.3.2 Como executar o assistente de instalação

1. Execute o programa de instalação do GFI MailEssentials.

2. Selecione o idioma a ser usado na instalação do GFI MailEssentials e clique em **Install**.

OBS.
A seleção de idioma não pode ser desfeita. Será necessário reinstalar o GFI MailEssentials para alterar o idioma selecionado nesta etapa.

3. Clique em **Next** na página **Welcome**.

4. Selecione se deseja verificar novas versões/compilações de GFI MailEssentials e clique em **Next**.

5. Leia o contrato de licença e clique em **I accept the terms in the license agreement** se você aceitar os termos e condições. Clique em **Next**.

Screenshot 12: Especificar o endereço de email do administrador e a chave de licença

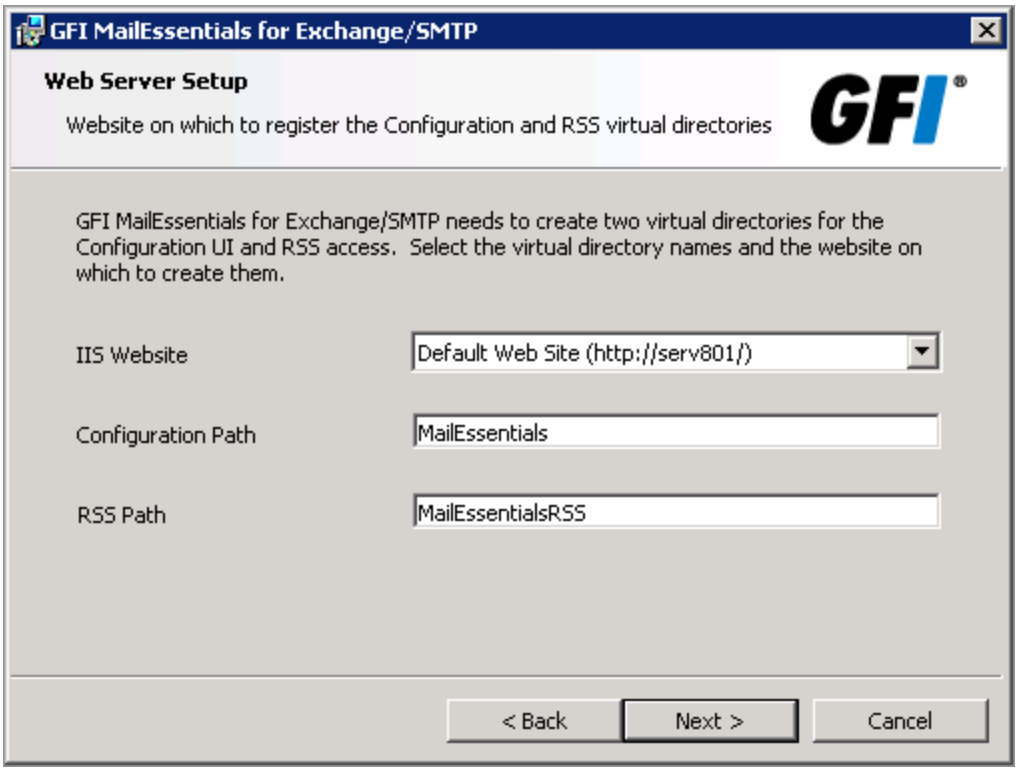
6. Digite o endereço de email do administrador em **Administrator Email** e digite **License Key**. Clique em **Next**.

> **OBS.**
> A avaliação não é mais aceita como uma chave de licença. Acesse a área do cliente do site da GFI para atualizar a chave da licença antes de iniciar o processo de atualização.

7. Selecione o modo que o GFI MailEssentials usará para recuperar a lista de usuários de email.

Opção	Descrição
Yes, all email users are available on Active Directory. As regras serão baseadas em usuários do Active Directory.	**Modo Active Directory** O GFI MailEssentials obterá a lista de usuários do Active Directory. A seleção desta opção significa que o GFI MailEssentials está sendo instalado protegido pelo seu firewall e tem acesso ao Active Directory que contém TODOS os usuários de email.
No, I do not have Active Directory or my network does not have access to Active Directory (DMZ)	**Modo SMTP** Selecione este modo se você estiver instalando o GFI MailEssentials em uma máquina que não tenha acesso ao Active Directory que contém a lista completa de todos os usuários de email. Isso inclui as máquinas em uma DMZ ou as máquinas que não fazem parte do domínio do Active Directory. Nesse modo, o GFI MailEssentials preenche automaticamente a lista de usuários locais usando o endereço de email do remetente nos emails de saída. A lista de usuários também pode ser gerenciada no nó GFI MailEssentials General Settings Para obter mais informações, consulte Gerenciar usuários locais (página 244).

Clique em **Next**.



Screenshot 13: Detalhes do servidor SMTP e do diretório virtual

8. No diálogo **Web Server Setup**, configure as seguintes opções:

> **OBS.**
> As configurações padrão estão normalmente corretas para a maioria das instalações.

Opção	Descrição
The website to create the GFI MailEssentials virtual directory	Selecione o site onde você deseja hospedar os diretórios virtuais do GFI MailEssentials.
The GFI MailEssentials Configuration virtual directory	Especifique um nome para diretório virtual do GFI MailEssentials.
The GFI MailEssentials Quarantine RSS feeds virtual directory	Especifique um nome para o diretório virtual de feeds RSS GFI MailEssentials Quarantine.
SMTP Server Setup	Selecione o servidor SMTP ao qual o GFI MailEssentials se conecta. Por padrão, o GFI MailEssentials se conecta ao seu servidor virtual SMTP padrão. Se você tiver vários servidores virtuais SMTP no domínio, poderá conectar o GFI MailEssentials a qualquer servidor virtual SMTP. **OBSERVAÇÕES** 1. Se você estiver instalando em uma máquina com o Microsoft® Exchange Server 2007/2010/2013, essa opção não será exibida, pois o Microsoft® Exchange tem seu próprio servidor SMTP. 2. Após a instalação, você ainda poderá conectar o GFI MailEssentials a outro servidor virtual SMTP a partir de GFI MailEssentials Configuration. Para obter mais informações, consulte Associações do servidor virtual SMTP (página 245).

Clique em **Next**.

9. Selecione a pasta na qual instalar o GFI MailEssentials e clique em **Next**. Quando a instalação for uma atualização, o GFI MailEssentials será instalado no mesmo local da instalação anterior.

10. Clique em **Install** para iniciar a instalação. Se você for solicitado a reiniciar os serviços SMTP, clique em **Yes**.

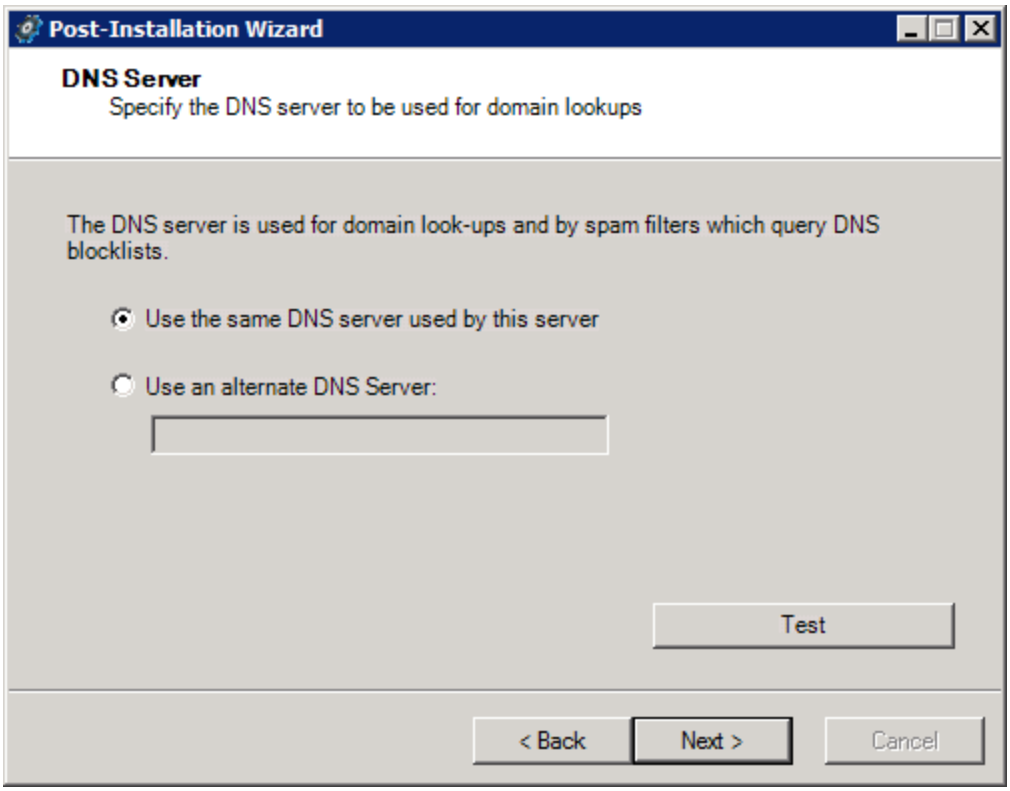
11. Quando terminar, clique em **Finish**.

> **OBS.**
> Para novas instalações, a configuração inicia automaticamente o Assistente pós-instalação. Para obter mais informações, consulte Assistente pós-instalação (página 45)..

3.3.3 Assistente pós-instalação

O Assistente pós-instalação é carregado automaticamente depois que o GFI MailEssentials é instalado pela primeira vez. Ele permite a definição das configurações mais importantes do GFI MailEssentials.

1. Clique em **Next** na página de boas-vindas.

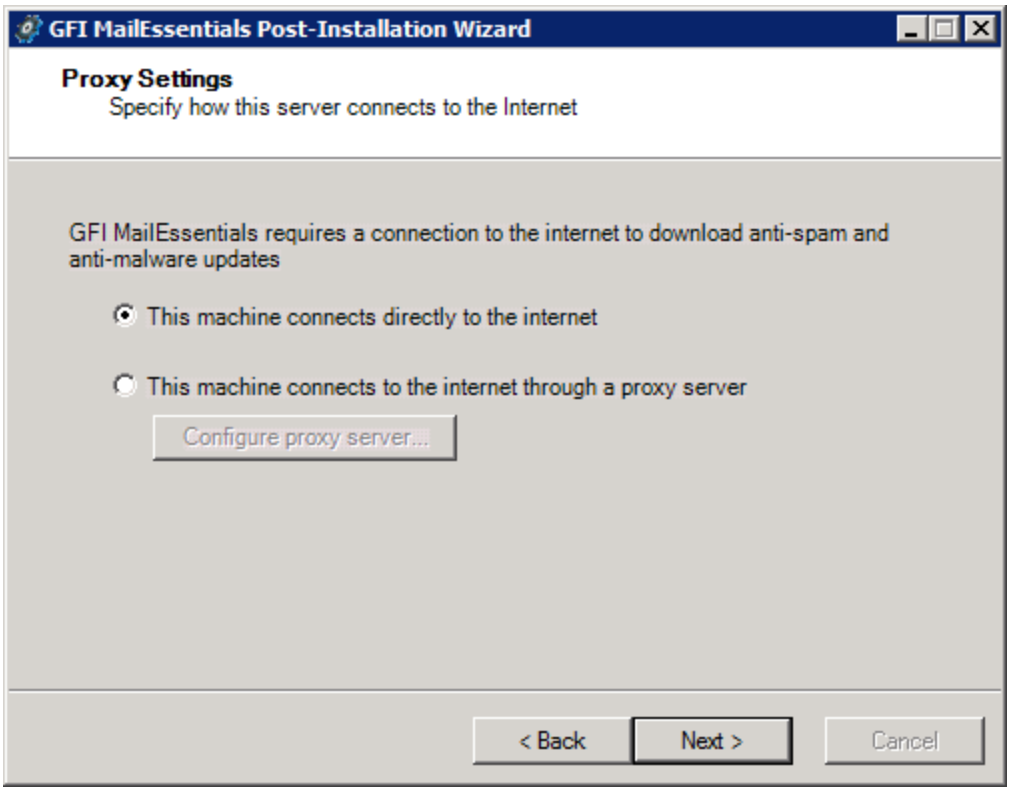


Screenshot 14: Configurações do servidor DNS

2. No diálogo DNS Server, selecione:

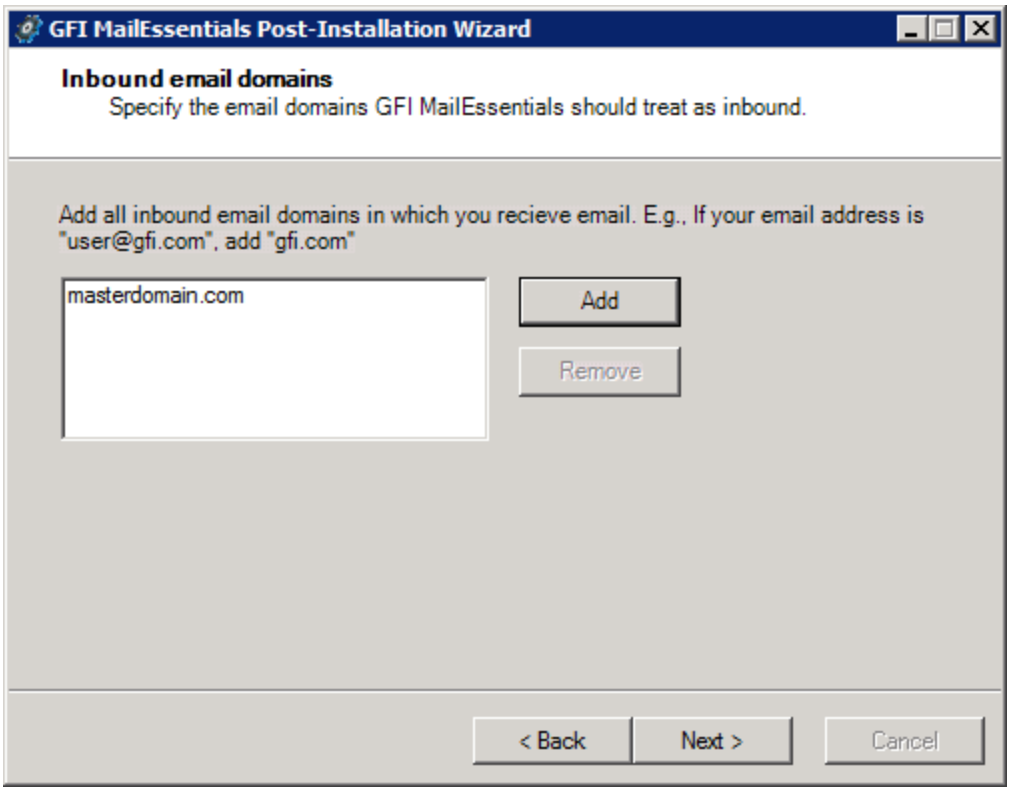
Opção	Descrição
Use the same DNS server used by this server	Selecione esta opção para usar o mesmo servidor DNS usado pelo sistema operacional no qual o GFI MailEssentials está instalado.
Use an alternate DNS server	Selecione esta opção para definir um endereço IP de servidor DNS personalizado.

Clique em **Test** para testar a conexão com o servidor DNS indicado. Se o teste não for bem-sucedido, especifique outro servidor DNS. Clique em **Next**.



Screenshot 15: Configurações de proxy

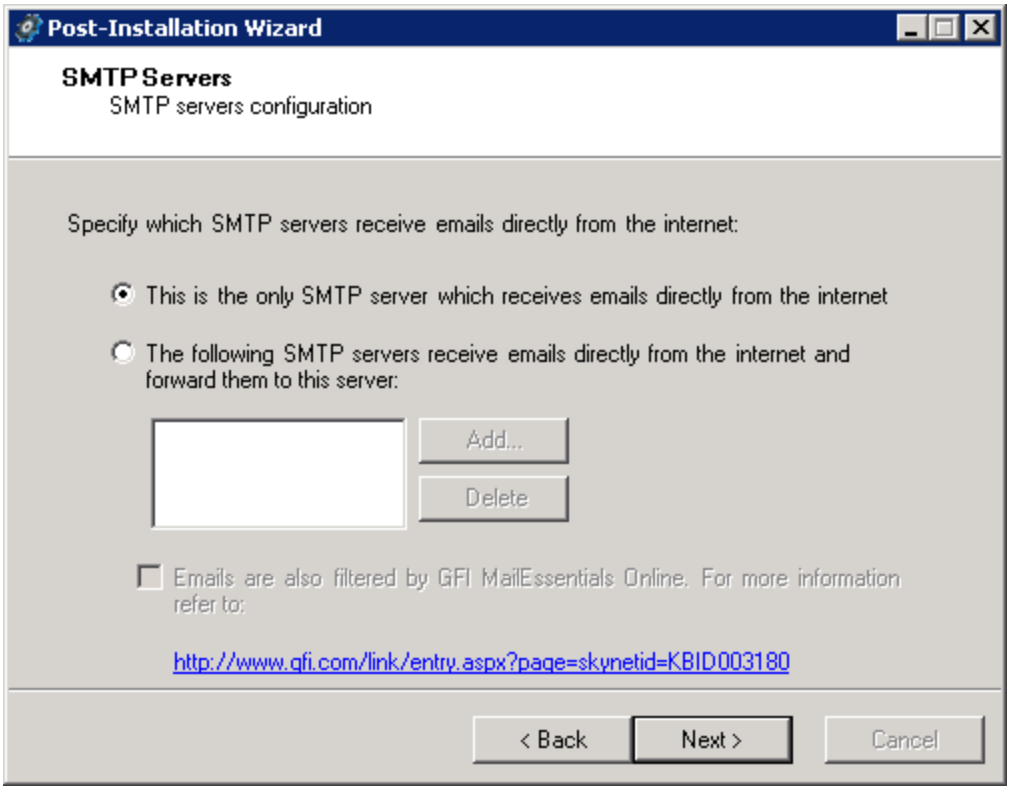
3. No diálogo **Proxy Settings**, especifique como o GFI MailEssentials estabelece uma conexão com a Internet. Se o servidor estabelecer uma conexão com a Internet por meio de um servidor proxy, clique em **Configure proxy server…** e especifique as configurações de proxy. Clique em **Next**.



Screenshot 16: Domínios de email de entrada

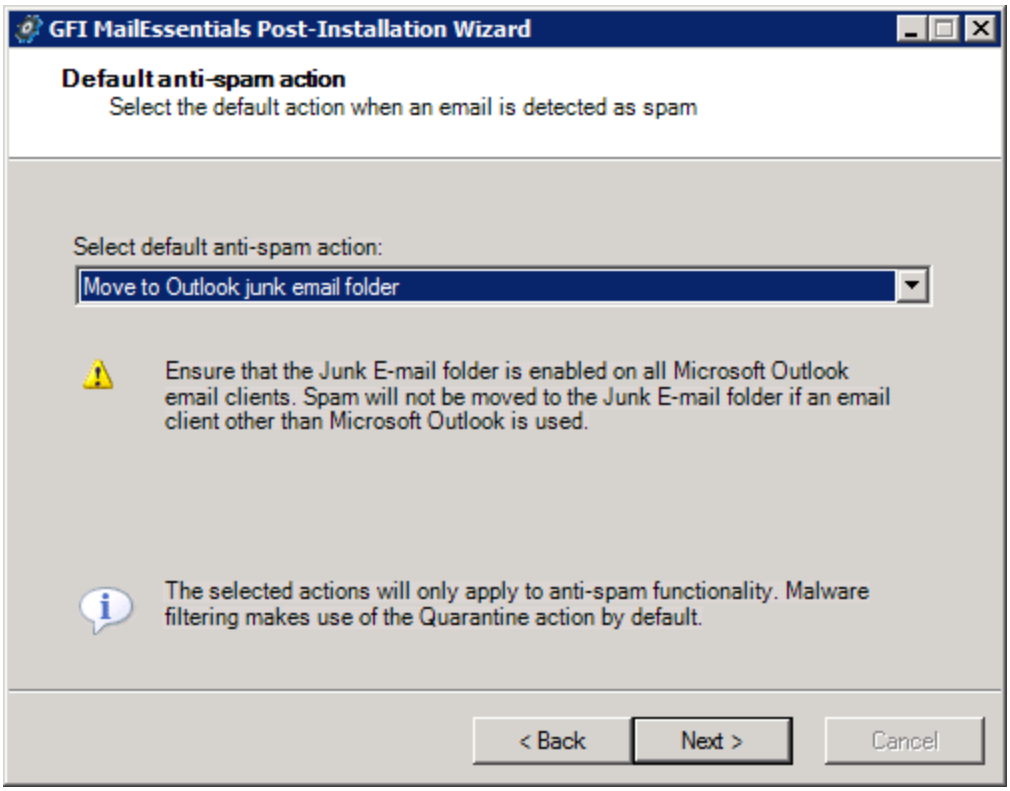
4. No diálogo **Inbound email domains**, especifique os domínios para procurar vírus e spam. Qualquer domínio que não estiver especificado na lista, não será verificado. Clique em **Next**.

> **OBS.**
> Ao adicionar domínios, selecione **Obtain domain's MX records and include in perimeter servers list** para recuperar os registros MX do domínio e adicioná-los automaticamente à lista de servidores SMTP de perímetro (configurada na próxima etapa).



Screenshot 17: Configurações do servidor SMTP

5. No diálogo **SMTP Servers**, especifique como o servidor recebe emails externos. Se os emails forem roteados através de outros servidores antes que serem encaminhados para o GFI MailEssentials, adicione os endereços IP dos outros servidores na lista. Para obter mais informações sobre servidores SMTP de perímetro, consulte http://go.gfi.com/?pageid=ME_PerimeterServer. Ao utilizar os produtos de segurança de email hospedados GFI MailEssentials Online, marque a caixa de seleção **Os emails também são filtrados por...**. Para obter mais informações, consulte: http://go.gfi.com/?pageid=ME_MAXMPME. Clique em **Next**.



Screenshot 18: Como selecionar a ação padrão anti-spam a ser usada

6. No diálogo **Default anti-spam action**, selecione a ação padrão a ser tomada quando emails forem detectados como spam. Esta ação se aplica somente aos filtros anti-spam. Os filtros de malware colocam automaticamente em quarentena os emails bloqueados. Para obter mais informações, consulte Mecanismos de verificação e filtragem de email (página 16).

> **OBS.**
> Quando você instalar o Microsoft® Exchange 2010 e a ação padrão selecionada for **Move to sub folder in recipient's Exchange mailbox**, um usuário com direitos de representação deverá ser criado. Selecione se deseja permitir que o GFI MailEssentialscrie automaticamente o usuário ou especifique automaticamente as credenciais e clique em **Set access rights** para atribuir os direitos exigidos ao usuário especificado. Esse usuário deve ser dedicado somente a esse recurso e as credenciais não devem ser alteradas. Para obter mais informações, consulte http://go.gfi.com/?pageid=ME_SpamExch2010.

Clique em **Next**.

7. Quando você fizer a instalação no Microsoft® Exchange Server 2007/2010, a lista de funções de servidor do Microsoft® Exchange Server detectadas e de componentes necessários do GFI MailEssentials será exibida. Clique em **Next** para instalar os componentes necessários do GFI MailEssentials.

8. Clique em **Finish** para finalizar a instalação.

A instalação doGFI MailEssentials está concluída e o sistema de proteção de email está instalado e funcionando.

Próxima etapa: Otimize seu sistema de proteção para garantir que ele esteja efetivamente instalado e funcionando. Para obter mais informações, consulte Ações pós-instalação (página 50).

OBS.

Para executar novamente o Assistente pós-instalação, no prompt de comando, acesse a pasta de instalação do GFI MailEssentials e execute o seguinte comando:

```
e2kwiz.exe clean
```

3.4 Atualização de uma versão anterior

Atualize para a versão mais recente do GFI MailEssentials do:

» GFI MailEssentials 2012

» GFI MailEssentials 12 e superior e/ou GFI MailSecurity 10.1 e superior.

Observações importantes

1. Antes de atualizar para a versão mais recente do GFI MailEssentials, certifique-se de que o sistema atenda aos requisitos mínimos de sistema. Para obter mais informações, consulte Requisitos do sistema (página 23).

2. A atualização não é reversível. Você não poderá fazer o downgrade para a versão anterior.

3.4.1 Atualização da versão 2012 ou posterior

Para atualizar o GFI MailEssentials 2012 ou posterior para a versão mais recente, inicie o instalador mais recente no servidor no qual o GFI MailEssentials está instalado. Depois de aceitar o Contrato de licença do Usuário Final, o programa de instalação detecta a instalação existente e mostra o caminho de instalação da versão anterior. Clique em **Next** para atualizar e **Finish** quando terminar.

Uma nova chave de licença é necessária ao fazer a atualização de uma versão superior para outra, por exemplo, atualizar da versão GFI MailEssentials 2012 para a GFI MailEssentials 2014 R2. Obtenha sua nova chave na Área de Clientes da GFI.

Microsoft® Exchange 2007 e superior

Para obter atualizações do Microsoft® Exchange 2007 e superior, o Post Installation wizard é exibido após a instalação. Ele exibe a lista de funções de servidor do Microsoft® Exchange detectadas e os componentes do GFI MailEssentialsnecessários. Clique em **Next** para instalar os componentes doGFI MailEssentials necessários e em **Finish** para concluir o Post-Install wizard.

3.4.2 Atualização de versões mais antigas

Informações sobre como atualizar para a versão mais recente do GFI MailEssentials em:

» GFI MailEssentials versões 12, 14, 2010

» Versões 10.1 e 2011 do GFI MailSecurity

As versões 2012 e 2014 do GFI MailEssentials introduziram várias alterações nas funcionalidades disponíveis. Para obter mais informações, consulte o GFI MailEssentials Guia de Atualização. As principais alterações incluem:

» Recursos anti-spam e antivírus serão mesclados em uma única solução

» Uma nova interface de usuário da Web

» Diferença entre os mecanismos antivírus disponíveis

» A geração de relatórios é integrada à interface do usuário

» Outras atualizações

Selecione o ambiente a partir do qual você está fazendo upgrade:

» GFI MailEssentials versões 12, 14, 2010

» GFI MailSecurity versões 10.1, 2011

» O GFI MailEssentials e o GFI MailSecurity

Atualização a partir das versões 12, 14, 2010 do GFI MailEssentials

Recursos anti-spam e anti-phishing são licenciados na atualização. Os recursos antivírus e antimalware são disponibilizados em uma versão de avaliação de 30 dias.

Instale o GFI MailEssentials como se fosse a primeira vez. Para obter mais informações, consulte Procedimento de instalação (página 41).

Para obter atualizações do Microsoft® Exchange 2007 e superior, o Post Installation wizard é exibido após a instalação. Ele exibe a lista de funções de servidor do Microsoft® Exchange detectadas e os componentes do GFI MailEssentialsnecessários. Clique em **Next** para instalar os componentes doGFI MailEssentials necessários e em **Finish** para concluir o Post-Install wizard.

Atualização das versões 10.1, 2011 do GFI MailSecurity

Os recursos antivírus e antimalware são licenciados na atualização. Os recursos anti-spam e antiphishing estão em uma versão de avaliação de 30 dias.

Instale o GFI MailEssentials como se fosse a primeira vez. Para obter mais informações, consulte Procedimento de instalação (página 41).

Após a instalação, conclua o Post Install Wizard do GFI MailEssentials. Para obter mais informações, consulte Assistente pós-instalação (página 45).

Atualização do GFI MailEssentials e do GFI MailSecurity

Quando atualizar um servidor que contenha o GFI MailEssentials e o GFI MailSecurity, todos os recursos antivírus, antimalware, anti-spam e antiphishing serão licenciados na atualização.

Instale o GFI MailEssentials como se fosse a primeira vez. Para obter mais informações, consulte Procedimento de instalação (página 41).

Para obter atualizações do Microsoft® Exchange 2007 e superior, o Post Installation wizard é exibido após a instalação. Ele exibe a lista de funções de servidor do Microsoft® Exchange detectadas e os componentes do GFI MailEssentialsnecessários. Clique em **Next** para instalar os componentes doGFI MailEssentials necessários e em **Finish** para concluir o Post-Install wizard.

3.5 Ações pós-instalação

Para garantir que o sistema de filtragem e verificação do GFI MailEssentials funcione corretamente, execute as seguintes ações pós-instalação:

Table 1: Ações pós-instalação

Ação	Descrição
Adicione os mecanismos de verificação do GFI MailEssentials à Lista de exceções Windows DEP.	O Data Execution Prevention (DEP) é um conjunto das tecnologias de hardware e software que executam verificações de memória para impedir que códigos mal-intencionados sejam executados em um sistema. Se você tiver instalado o GFI MailEssentials em um sistema operacional que inclui o DEP, será necessário adicionar os executáveis do mecanismo de verificação GFI MailEssentials(**GFiScanM.exe**) e do mecanismo de verificação de vírus Kaspersky (**kavss.exe**). **OBS.** Isso só é necessário na instalação no Microsoft Windows® Server 2003 SP 1 ou SP 2. Para obter mais informações, consulte Adicionar mecanismos à Lista de exceções Windows DEP (página 51).
Inicie a configuração do GFI MailEssentials	Acesse **Start > Programs > GFI MailEssentials > GFI MailEssentials Configuration**.
Habilitar o filtro Coleta de diretório	Ataques do tipo Directory harvesting ocorrem quando os remetentes de spam tentam adivinhar endereços de email anexando nomes dos usuários conhecidos a seu domínio. A maioria dos endereços de email é inexistente.Este filtro é ativado por padrão se o GFI MailEssentials estiver instalado em um ambiente do Active Directory. Para obter mais informações, consulte Coleta de diretório (página 115).
Habilitar lista de exclusão temporária	O filtro Lista de exclusão temporária bloqueia temporariamente a entrada de emails recebidos de remetentes desconhecidos. Sistemas de email legítimos normalmente tentam enviar o email após alguns minutos. Os remetentes de spam simplesmente ignoram essas mensagens de erro.Este filtro não é habilitado por padrão. Para obter mais informações, consulte Lista de exclusão temporária (página 130).Para obter mais informações, consulte Lista de exclusão temporária (página 130).
Configurar os filtros Listas de permissão	A lista de permissão contém listas de critérios que identificam um email legítimo. Emails que correspondam a esses critérios não são examinados pelos filtros anti-spam e são sempre entregues ao destinatário. Para obter mais informações, consulte Lista de permissão (página 141).
Testar a instalação	Após a configuração de todas as ações pós-instalação, o GFI MailEssentials está pronto para começar a proteger e filtrar o sistema de emails contra emails mal-intencionados e emails com spam. Teste sua instalação para assegurar que o GFI MailEssentials esteja funcionando corretamente. Para obter mais informações, consulte Testar a instalação (página 52).

3.5.1 Adicionar mecanismos à Lista de exceções Windows DEP

O Data Execution Prevention (DEP) é um conjunto das tecnologias de hardware e software que executam verificações de memória para impedir que códigos mal-intencionados sejam executados em um sistema.

Se você tiver instalado o GFI MailEssentials em um sistema operacional que inclui o DEP, será necessário adicionar os executáveis do mecanismo de verificação GFI MailEssentials(**GFiScanM.exe**) e do mecanismo de verificação de vírus Kaspersky (**kavss.exe**).

> **OBS.**
> Isso só é necessário na instalação no Microsoft Windows® Server 2003 SP 1 ou SP 2.

Para adicionar os executáveis GFI na lista de exceção DEP:

1. No **Control Panel**, abra o miniaplicativo **System**.
2. Na guia **Advanced**, na área **Performance**, clique em **Settings**.
3. Clique na guia **Data Execution Prevention**.
4. Clique em **Turn on DEP for all programs and services except those I select**.

5. Clique em **Add** e, no diálogo, procure: ***<GFI MailEssentials installation path>\GFI\MailEssentials*\EmailSecurity** e escolha **GFiScanM.exe**.

6. Clique em **Add** e, no diálogo, procure: ***<GFI MailEssentials installation path>\GFI\MailEssentials*\AntiVirus\Kaspersky** e escolha **kavss.exe**.

7. Clique em **Apply** e **OK** para aplicar as alterações.

8. Reinicie o serviço **GFI MailEssentialsAutoupdater** e os serviços **GFI MailEssentials AV Scan Engine**.

3.5.2 Testar a instalação

Após a configuração de todas as ações pós-instalação, o GFI MailEssentials está pronto para começar a proteger e filtrar o sistema de emails contra emails mal-intencionados e emails com spam.

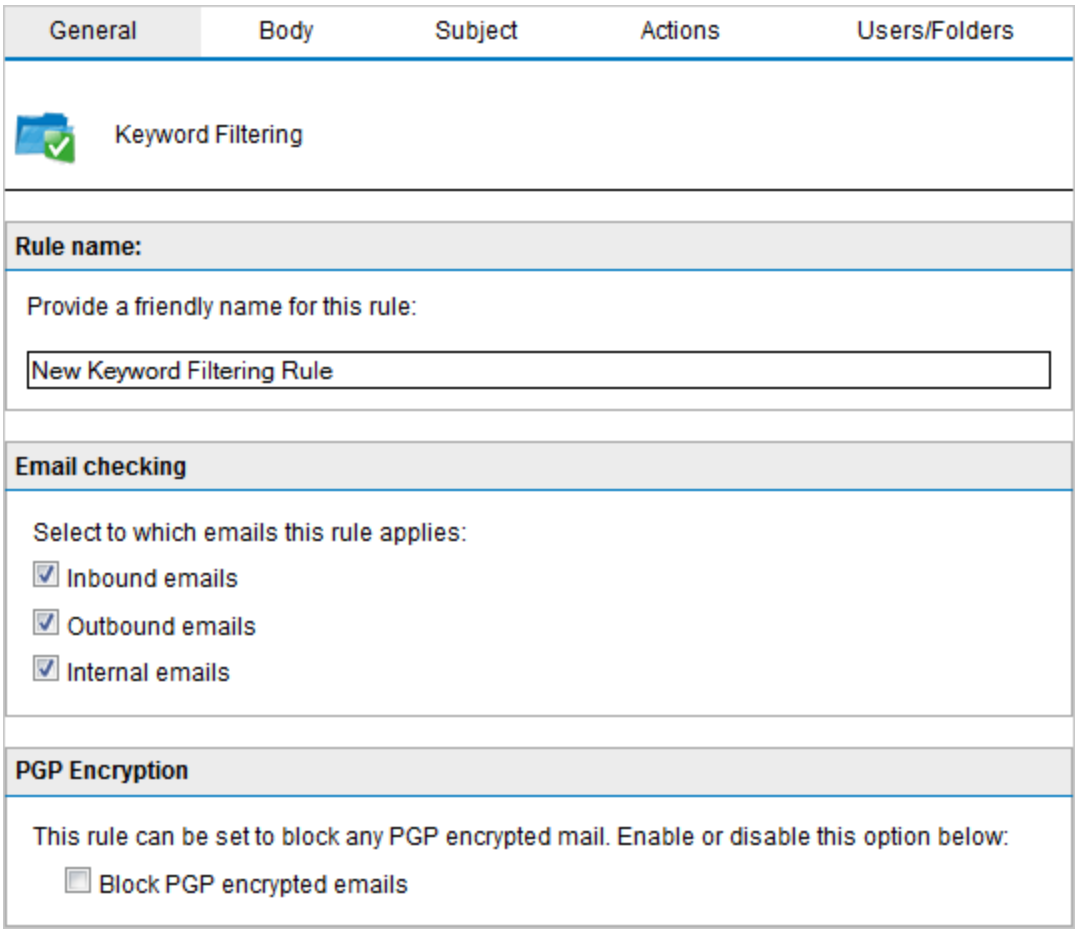
Certifique-se de que o GFI MailEssentials bloqueie emails indesejados. Para fazer isso, envie emails de entrada e de saída escritos intencionalmente de forma que sejam bloqueados pelo GFI MailEssentials.

Etapa 1: Criar uma regra de filtragem de conteúdo

1. Inicie o console do GFI MailEssentials.

2. Acesse o nó **GFI MailEssentials > Content Filtering > Keyword Filtering**.

3. Clique em **Add Rule…**.



Screenshot 19: Criar uma regra de teste da filtragem de palavras-chave

4. Em **Rule name**, digite `Test Rule`.

5. Na guia **Subject**, selecione **Block emails if content is found matching these conditions (message subject)**.

6. Em **Edit Condition**, digite `Threat test` e clique em **Add Condition**.

7. Na guia **Actions**, selecione **Block email and perform this action** e selecione **Quarantine email**.

8. Clique em **Apply** para salvar a regra.

Etapa 2: Enviar um email de teste de entrada

1. Em uma conta de email externa, crie um novo email e digite `Threat test` como o assunto.

2. Envie o email para uma de suas contas de email internas.

Etapa 3: Enviar um email de teste de saída

1. Em uma conta de email interna, crie um novo email e digite `Threat test` no assunto.

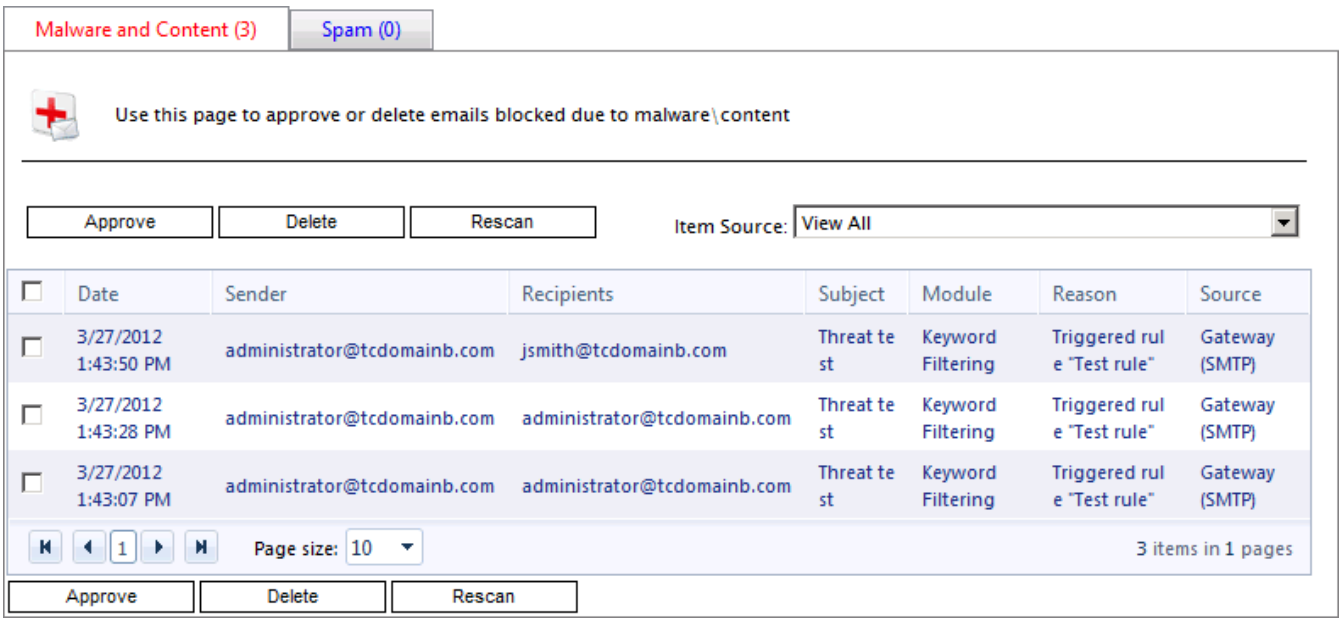
2. Envie o email para uma conta de email externa.

Etapa 4: Confirmar se os emails de teste foram bloqueados

Verifique se os testes de emails de entrada e saída foram bloqueados e colocados em quarentena. Para fazer isso:

1. No GFI MailEssentials, acesse **GFI MailEssentials Configuration > Quarantine > Today**.

2. Certifique-se de que emails de teste de entrada e saída sejam listados na guia **Malware and Content** pelos seguintes motivos: **Triggered rule "Test rule"**.



Screenshot 20: Email de teste bloqueado pela Regra de teste

> **OBS.**
> Quando o teste for concluído, exclua ou desabilite a **Test rule** criada na Etapa 1.

4 Monitorar o status

O GFI MailEssentials permite monitorar a atividade de emails em tempo real ou gerar relatórios de atividade de email para um determinado período de tempo.

Monitoração de módulo	Descrição
Painel	O **Dashboard** do GFI MailEssentials oferece informações em tempo real que permitem monitorar o produto. Para acessar o Painel, acesse **GFI MailEssentials > Painel**. Isso inclui: » Informações estatísticas importantes sobre emails bloqueados. Para obter mais informações, consulte Status e estatísticas (página 55). » Status dos serviços do GFI MailEssentials. Para obter mais informações, consulte Serviços (página 56). » Apresentação gráfica da atividade do email. Para obter mais informações, consulte Charts (página 57). » Lista de emails processados. Para obter mais informações, consulte Registros de processamento de email (página 58). » Status das atualizações de software. Para obter mais informações, consulte Atualizações do mecanismo antivírus e anti-spam (página 60). » Registro de eventos importantes do GFI MailEssentials. Para obter mais informações, consulte Logs de eventos (página 61). » Registro das atividades do POP2Exchange. Para obter mais informações, consulte Atividade do POP2Exchange (página 62).
Relatórios	O GFI MailEssentials permite que você gere relatórios baseados nos dados registrados no banco de dados. Para acessar Reporting, acesse **GFI MailEssentials > Reporting**. » **Enabling reporting** - Para obter mais informações, consulte Habilitar/desabilitar a geração de relatórios (página 62). » **Configure reporting database** - Para obter mais informações, consulte Configurar o banco de dados de relatórios (página 69). » **Generate reports** - Para obter mais informações, consulte Gerar um relatório (página 63). » **Create custom reports** - Para obter mais informações, consulte Relatórios personalizados (página 66). » **Search the reporting database** - Para obter mais informações, consulte Pesquisar no banco de dados de relatórios (página 67).

4.1 Painel

O **Dashboard** do GFI MailEssentials oferece informações em tempo real que permitem monitorar o produto. Para acessar o Painel, acesse **GFI MailEssentials > Painel**. Isso inclui:

» Informações estatísticas importantes sobre emails bloqueados. Para obter mais informações, consulte Status e estatísticas (página 55).

» Status dos serviços do GFI MailEssentials. Para obter mais informações, consulte Serviços (página 56).

» Apresentação gráfica da atividade do email. Para obter mais informações, consulte Charts (página 57).

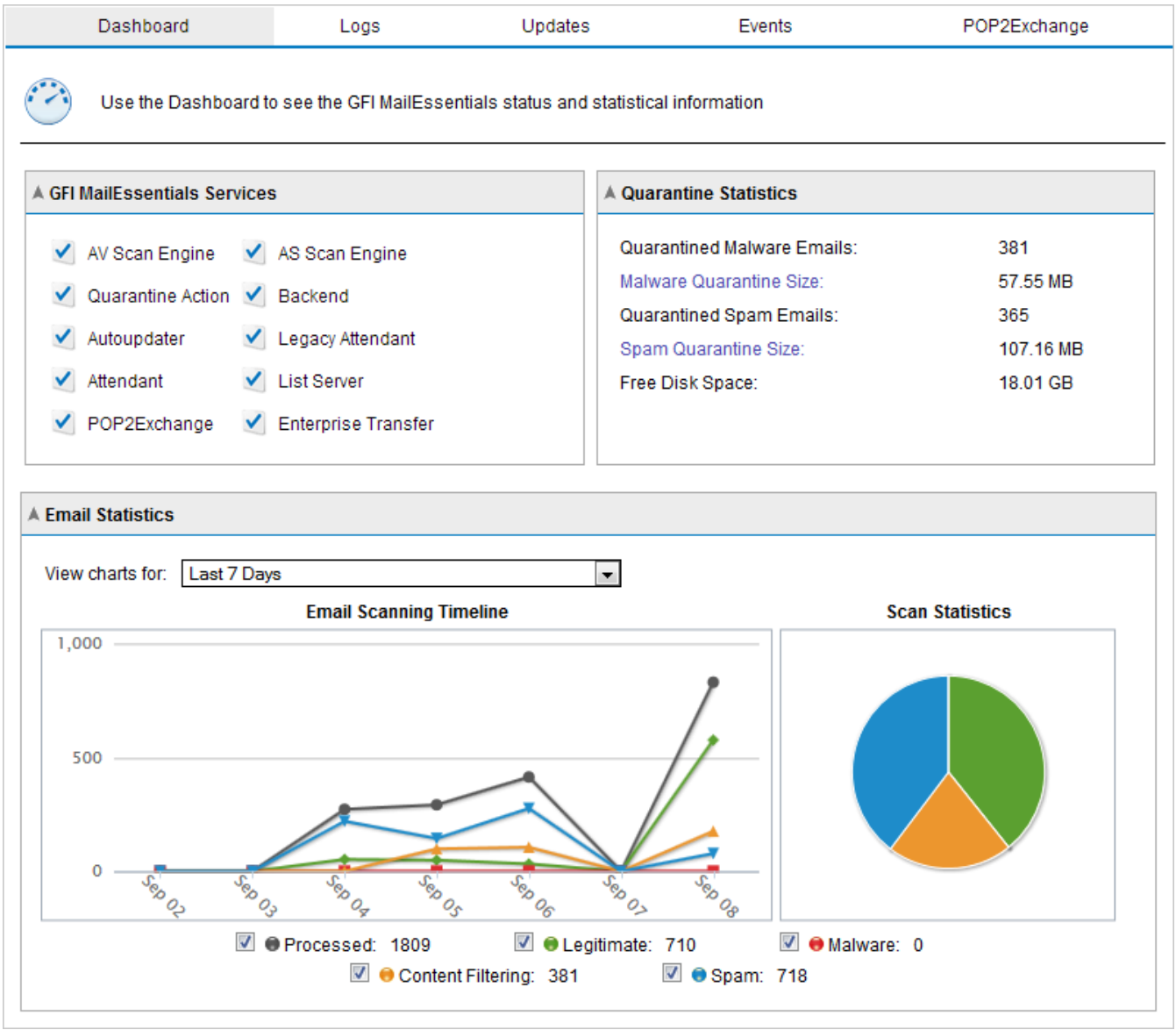
» Lista de emails processados. Para obter mais informações, consulte Registros de processamento de email (página 58).

» Status das atualizações de software. Para obter mais informações, consulte Atualizações do mecanismo antivírus e anti-spam (página 60).

» Registro de eventos importantes do GFI MailEssentials. Para obter mais informações, consulte Logs de eventos (página 61).

» Registro das atividades do POP2Exchange. Para obter mais informações, consulte Atividade do POP2Exchange (página 62).

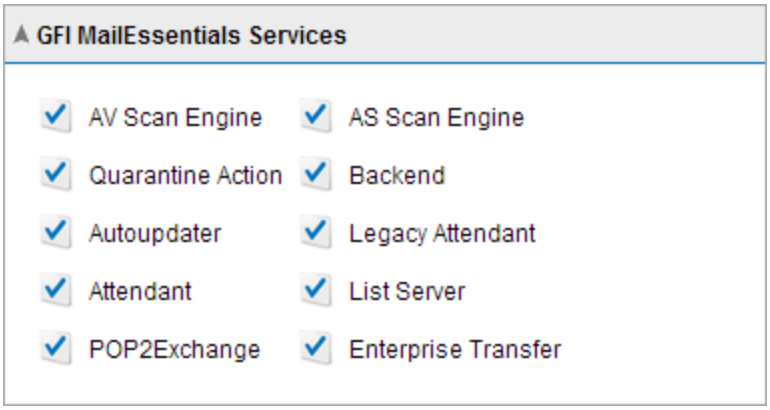
4.1.1 Status e estatísticas



Screenshot 21: O painel do GFI MailEssentials

Para abrir o Painel, acesse **GFI MailEssentials > Dashboard**. Esta página mostra estatísticas, o status de serviços e uma apresentação gráfica da atividade do email. Mais detalhes sobre essas seções são fornecidos a seguir.

Serviços



Screenshot 22: Os serviços do GFI MailEssentials

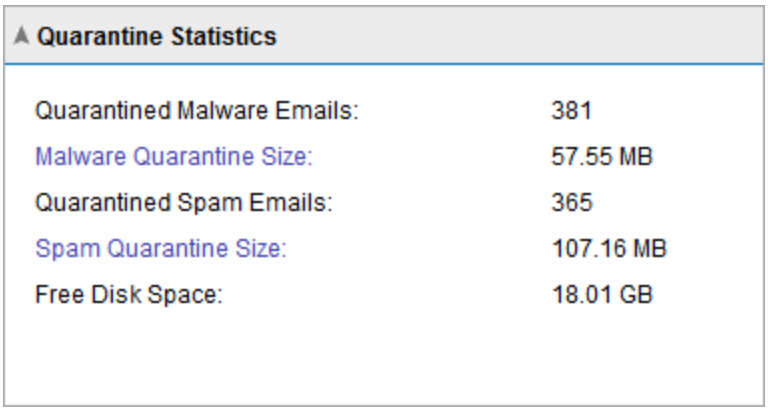
A área **Services** exibe o status dos serviços do GFI MailEssentials.

» - Indica que o serviço foi iniciado. Clique neste ícone para interromper o serviço.

» - Indica que o serviço foi interrompido. Clique neste ícone para iniciar um serviço interrompido.

Você também pode iniciar ou interromper serviços no console de serviços do Microsoft® Windows. Para iniciar o console de serviços, acesse **Start > Run**, digite `services.msc` e clique em **OK**.

Estatísticas da Quarentena

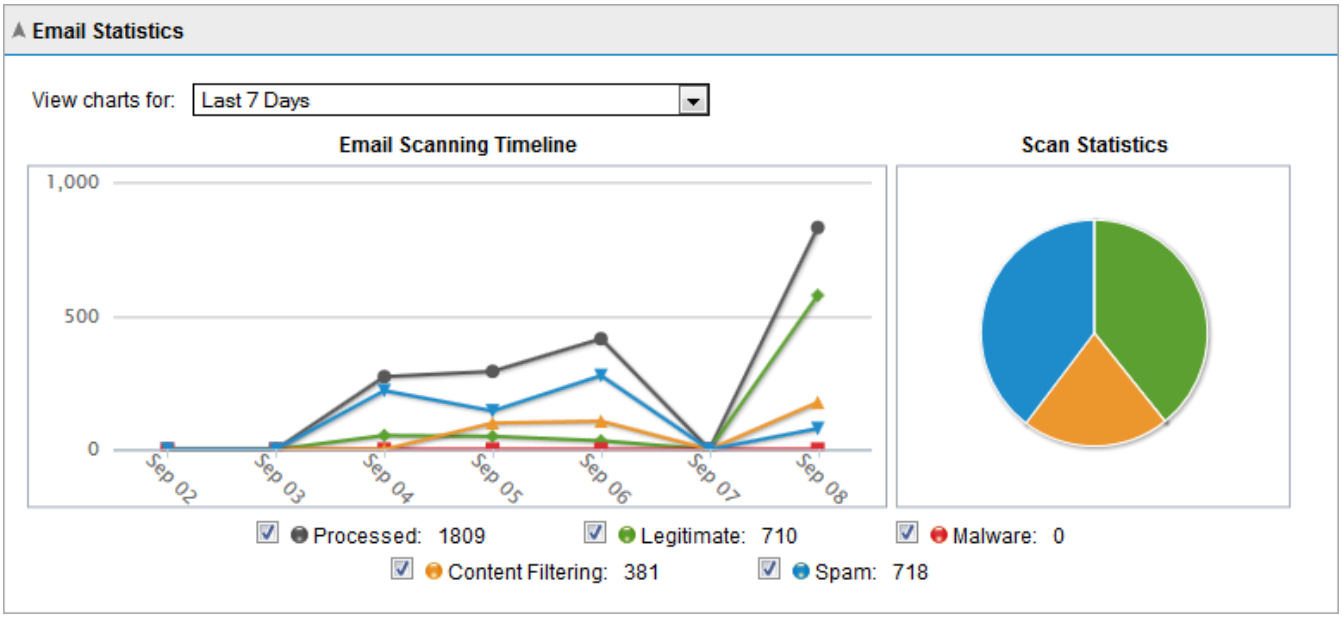


Screenshot 23: Estatísticas da Quarentena

A área **Quarantine Statistics** exibe as seguintes informações estatísticas:

Título da estatística	Descrição
Quarantined Malware Emails	Número de e-mails bloqueados pelos mecanismos Email Security and Content Filtering e armazenados no Malware Quarantine Store.
Malware Quarantine Size	Tamanho no disco do banco de dados Malware Quarantine Store.
Quarantined Spam Emails	Número de emails bloqueados por mecanismos anti-spam e armazenados no Spam Quarantine Store.
Spam Quarantine Size	Tamanho no disco do banco de dados de Spam Quarantine Store.
Free disk space	Espaço livre no disco onde os armazenamentos em quarentena são salvos.

Charts

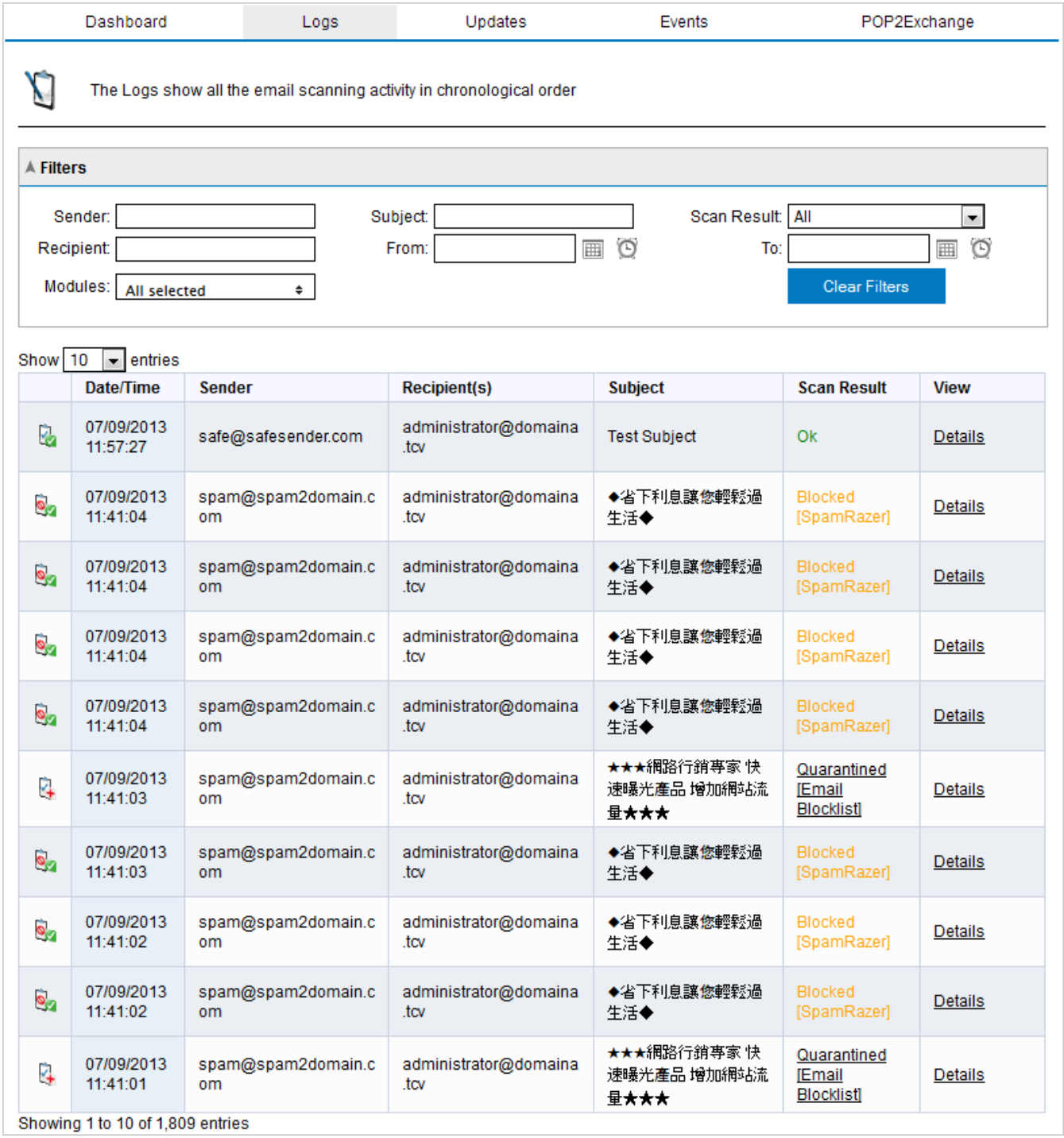


Screenshot 24: Gráficos do Painel

A área **Charts** exibe informações gráficas sobre os emails processados pelo GFI MailEssentials. Selecione o período de tempo na lista suspensa para exibir informações do período nos gráficos.

Área	Descrição
View charts for	Permite que você selecione um período para visualizar gráficos. As opções disponíveis são: » Últimas 6 horas » Últimas 24 horas » Últimas 48 horas » Últimos sete dias
Email scanning timeline (time graph)	Mostra um gráfico de tempo em intervalos para o período selecionado. O gráfico mostra o número de emails processados, legítimos, malware, filtragem de conteúdo e spam.
Scan statistics (pie chart)	Distribuição em um gráfico do número total de emails seguros, colocados em quarentena e com falha no período selecionado.
Legend	A legenda mostra a cor usada nos gráficos e a contagem de cada categoria.

4.1.2 Registros de processamento de email



Screenshot 25: Registros de processamento de email

Em GFI MailEssentials Configuration, você pode monitorar todos os emails processados em tempo real. Acesse **GFI MailEssentials > Painel** e selecione a guia **Logs** para exibir a lista de e-mails processados. As seguintes informações são exibidas para cada email processado:

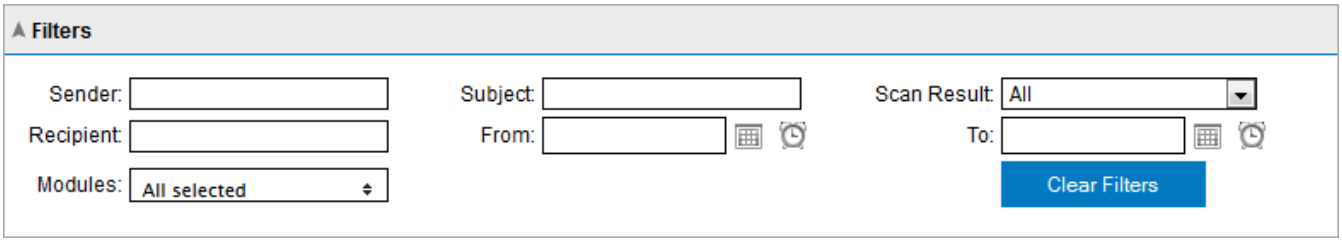
- Data/hora
- Remetente
- Destinatário(s)

» Assunto

» Scan Result: mostra a ação realizada no email.

Ação	Descrição
OK	O email não está bloqueado pelo GFI MailEssentials e é fornecido para os destinatários pretendidos.
Quarantined	O email é bloqueado por um mecanismo ou um filtro com ação definida para quarentena. Clique em **Quarantine** para analisar o email. **OBS.** O email não pode ser visualizado na quarentena se tiver sido excluído manualmente da quarentena.
Blocked	Email está bloqueado por um mecanismo ou filtro. Ação tomada é a ação configurada para o mecanismo específico.
Deleted	O email é bloqueado por um mecanismo ou filtro com ação definida para excluir emails detectados.
Failed	O email que não pode ser verificado pelo GFI MailEssentials. O email é movido para uma das seguintes pastas: *<GFI MailEssentials installation path>*\GFI\MailEssentials\EmailSecurity\FailedMails\ *<GFI MailEssentials installation path>*\GFI\MailEssentials\AntiSpam\FailedMails\ Para obter mais informações, consulte Emails com falha (página 255).

Como filtrar os registros de processamento de email



Screenshot 26: Filtros de registros de processamento de emails

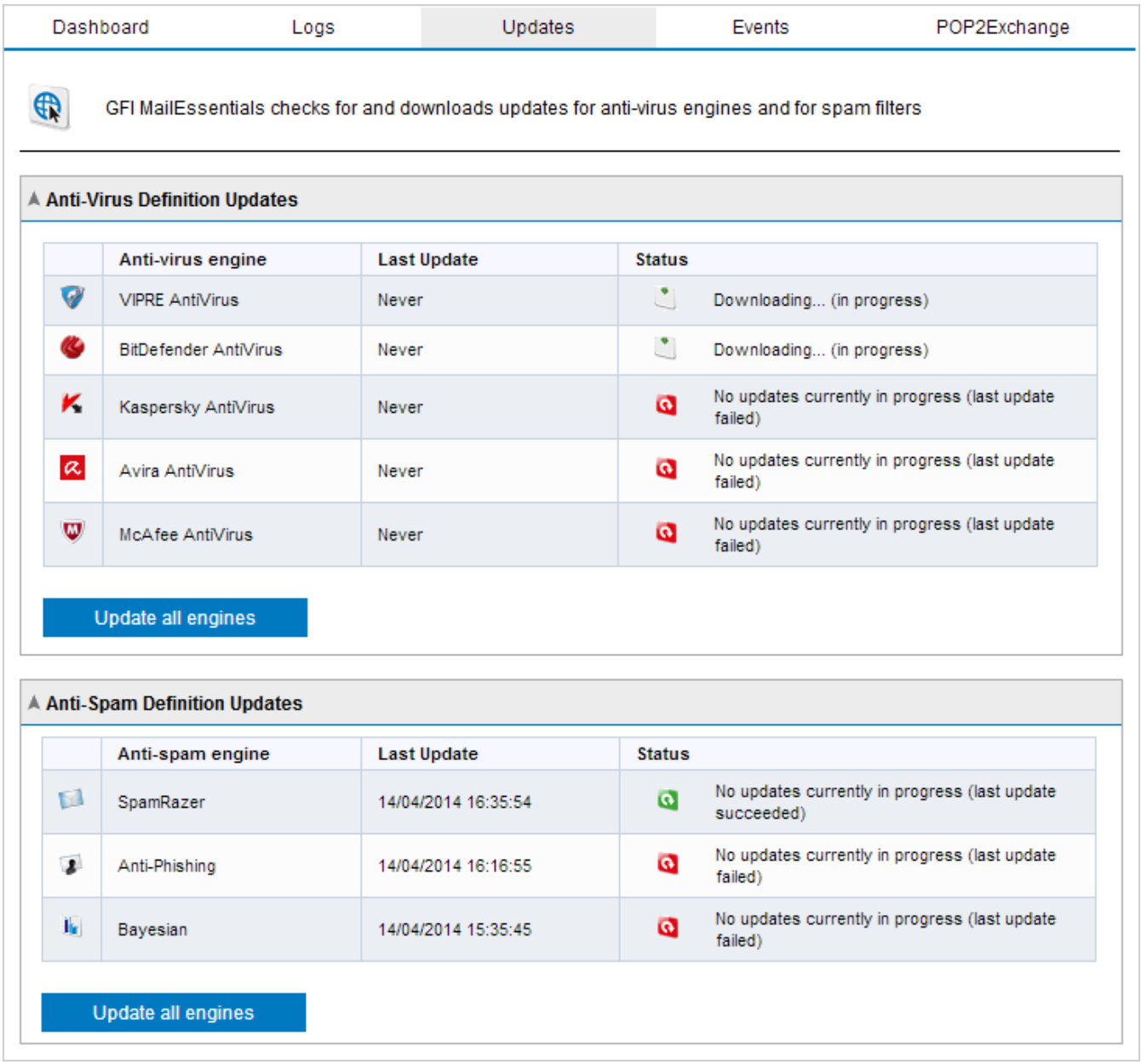
A filtragem de registros de processamento de email simplifica o processo de análise, fornecendo a possibilidade de encontrar emails específicos. Na área **Filter**, especifique um dos seguintes critérios:

Filtro	Descrição
Sender	Especifique se o endereço de email completo ou parcial para exibir apenas os emails enviados por remetentes correspondentes.
Recipient	Especifique se o endereço de email completo ou parcial para exibir apenas os emails enviados para destinatários correspondentes.
Subject	Especifique o assunto completo ou parcial para exibir apenas os emails com um assunto correspondente.
Scan result	Na lista suspensa, selecione se deseja exibir somente emails com uma determinado resultado da verificação (por exemplo, somente emails em quarentena)
From & To	Especifique um intervalo de data e hora para exibir os emails processados durante esse período específico.

OBS.

Clique em **Clear Filters** para remover filtros específicos e mostrar todos os registros de email.

4.1.3 Atualizações do mecanismo antivírus e anti-spam



Screenshot 27: Atualizações de mecanismos de verificação de vírus

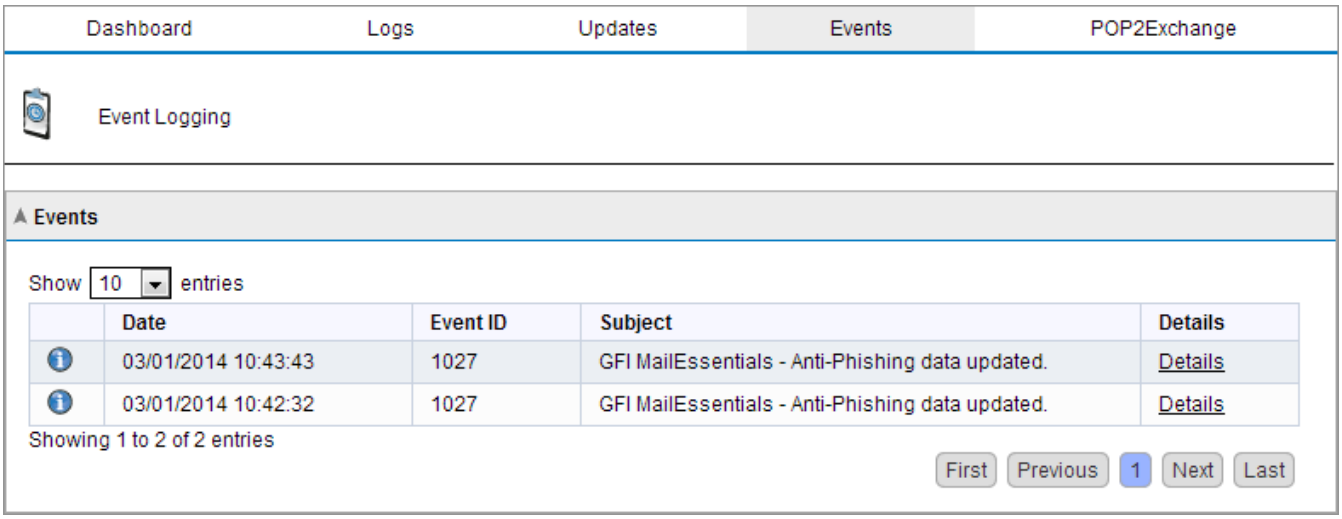
As atualizações dos mecanismos de verificação de antivírus e anti-spam podem ser monitoradas em uma única página. Acesse **GFI MailEssentials > Dashboard** e selecione a guia **Updates** para examinar o status e as datas quando os mecanismos de verificação foram atualizados pela última vez.

Clique em **Update all engines** para verificar e fazer o download de todas as atualizações.

As atualizações são verificadas e obtidas por download, como definido nas páginas de configuração dos mecanismos. Acesse a página de configuração de cada mecanismo e acesse a guia **Updates** para definir as configurações de atualização.

> **OBS.**
> As atualizações de cada mecanismo são verificadas e obtidas por download sequencialmente (uma atualização de mecanismo de cada vez).

4.1.4 Logs de eventos



Screenshot 28: Logs de eventos

Em Configuração do GFI MailEssentials, você pode monitorar eventos importantes relacionados à funcionalidade do GFI MailEssentials. Exemplos de instâncias que acionam eventos:

» conclusão das atualizações do mecanismo anti-spam.

» quando o banco de dados de relatórios atingir 1,7 GB e o GFI MailEssentials passar para um novo banco de dados.

» menos de 1 GB de espaço livre na partição do disco em que a quarentena está armazenada.

Acesse **GFI MailEssentials > Painel** e selecione a guia **Eventos** para exibir a lista de eventos. As seguintes informações são exibidas para cada evento:

» Data/hora

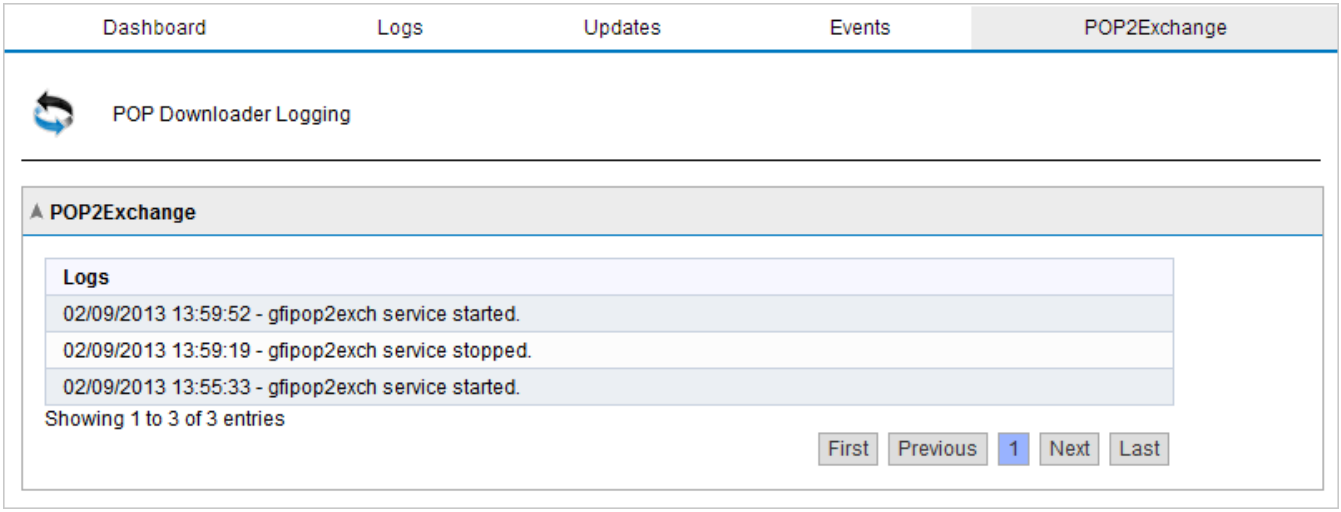
» ID do evento – um identificador é atribuído para cada tipo de evento do GFI MailEssentials.

» Assunto

Clique em **Detalhes** para mostrar mais informações sobre um determinado evento.

Os eventos do GFI MailEssentials também estão disponíveis no Visualizador de Eventos do Windows em **Logs de Aplicativos e Serviços** > GFI MailEssentials.

4.1.5 Atividade do POP2Exchange



Screenshot 29: Registro POP2Exchange

No GFI MailEssentials, você pode monitorar a atividade de POP2Exchange em tempo real. Acesse **GFI MailEssentials > Painel** e selecione a guia **POP2Exchange**.

> **OBS.**
> Para obter mais informações, consulte POP2Exchange - Download de emails do servidor POP3 (página 258).

4.2 Relatórios

O GFI MailEssentials permite que você gere relatórios baseados nos dados registrados no banco de dados.

Para acessar Reporting, acesse **GFI MailEssentials > Reporting**.

» **Enabling reporting** - Para obter mais informações, consulte Habilitar/desabilitar a geração de relatórios (página 62).

» **Configure reporting database** - Para obter mais informações, consulte Configurar o banco de dados de relatórios (página 69).

» **Generate reports** - Para obter mais informações, consulte Gerar um relatório (página 63).

» **Create custom reports** - Para obter mais informações, consulte Relatórios personalizados (página 66).

» **Search the reporting database** - Para obter mais informações, consulte Pesquisar no banco de dados de relatórios (página 67).

4.2.1 Habilitar/desabilitar a geração de relatórios

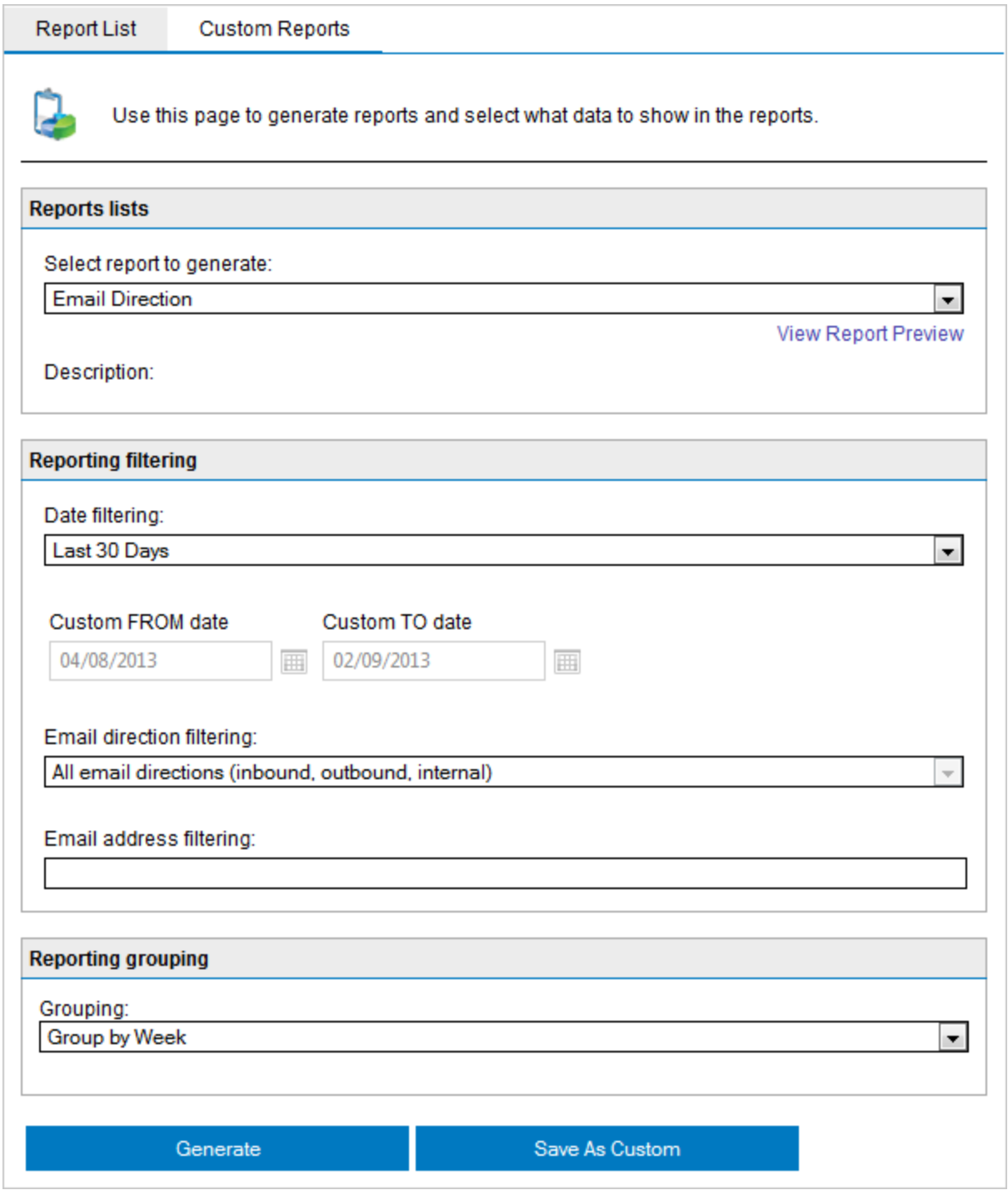
Por padrão, a opção Reporting fica habilitada e os dados de atividade de email são registrados em um banco de dados do Firebird localizado na pasta:

`<GFI MailEssentials installation path>\GFI\MailEssentials\data\`

Acesse o nó **Reporting > Settings** e marque ou desmarque **Enable Reporting** para habilitar ou desabilitar a geração de relatórios, respectivamente.

4.2.2 Gerar um relatório

1. Na configuração do GFI MailEssentials, acesse **GFI MailEssentials > Reporting > Reports**.

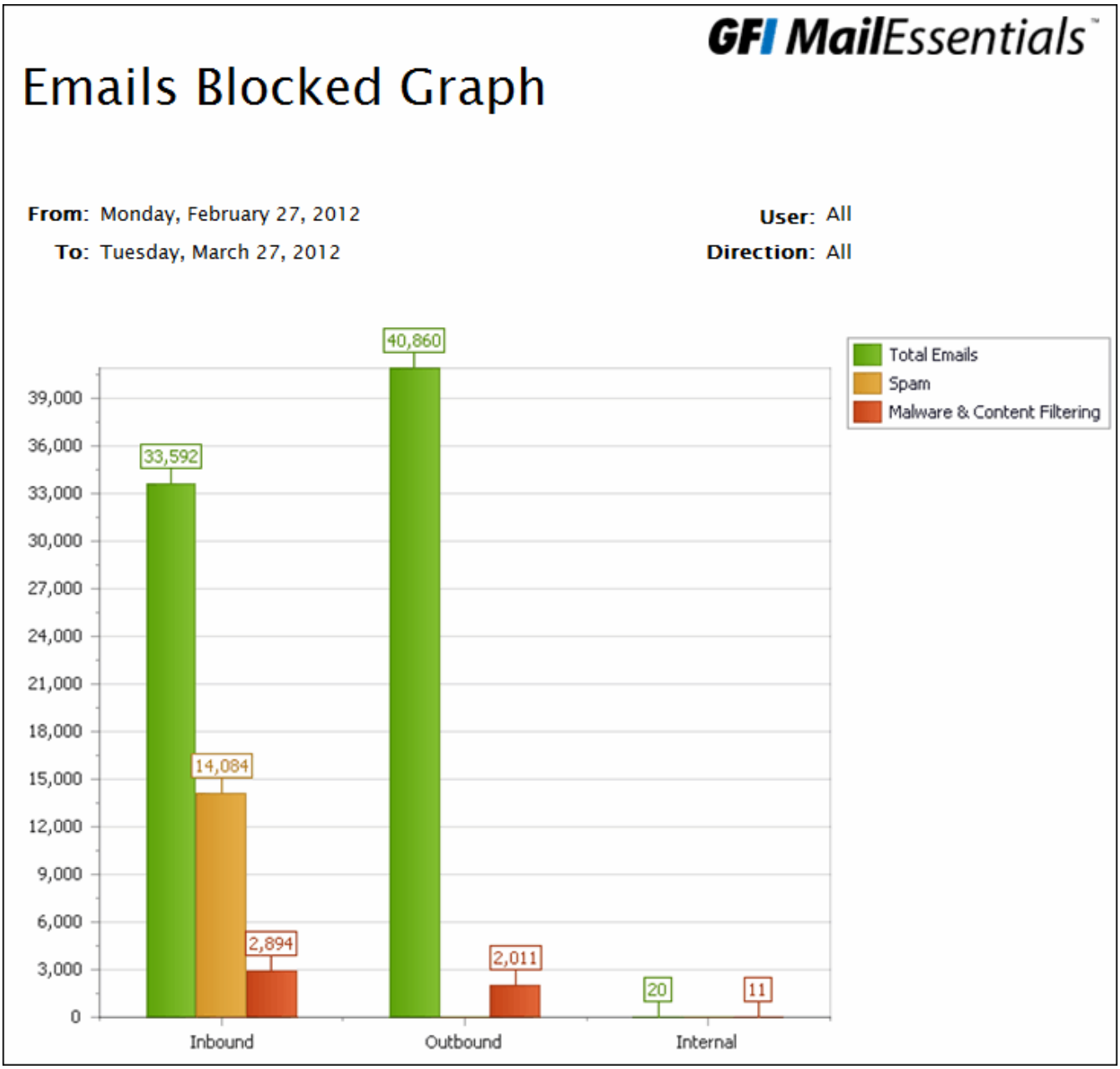


Screenshot 30: Criar um relatório

2. Na guia **Report List**, configure as seguintes opções de relatório:

Opção	Descrição
Report type	Selecione o tipo de relatório a ser gerado: » **Emails Blocked**: mostra o total de emails bloqueados pelos filtros de anti-spam e antimalware para cada direção de email (de entrada, de saída e internos) de todos os emails processados. » **Emails Blocked Graph**: mostra graficamente o total de emails bloqueados pelos filtros anti-spam e antimalware para cada direção de email (de entrada, de saída e internos) de todos os emails processados. » **Email Direction Chart**: mostra graficamente o total de emails processados para cada direção de email (de entrada, de saída e internos). » **Email Direction**: exibe o número total de emails processados para cada direção de email (de entrada, de saída e internos). » **User Report**: mostra o número de emails bloqueados e permitidos para cada endereço de email. » **Spam Filter**: mostra o número total de emails bloqueados por cada filtro anti-spam. » **Spam Filter Graph**: mostra graficamente o número total de emails bloqueados por cada filtro anti-spam. Clique em **View Report Preview** para visualizar a aparência do relatório.
Date filtering	Selecione o intervalo da data do relatório. Quando selecionar **Custom date range**, especifique o período para exibir os dados, nos controles do calendário **Custom From** e **Custom To**.
Email directions filtering	Selecione uma direção de email específica para exibir os dados ou selecione **All email directions (inbound, outbound, internal)** para exibir os dados de todas as direções.
Email address filtering	Digite um endereço de email para mostrar as informações do relatório somente para determinados endereços de email.
Report Grouping	Especifique como agrupar dados. As opções disponíveis são: » **Agrupar por dia** » **Agrupar por semana** » **Agrupar por mês** » **Agrupar por ano**

3. Clique em **Generate** para criar e exibir o relatório ou **Save as Custom** para salvar as configurações do relatório para reutilização futura.



Screenshot 31: Relatório gráfico de emails bloqueados

Relatório de funções

Use a barra de ferramentas na parte superior do relatório para executar as seguintes funções:

Função	Ícone	Descrição
Print		Clique para imprimir o relatório.
Print current page		Clique para imprimir a página que está atualmente visível.
Navigate		Use esta barra de ferramentas para percorrer as páginas do relatório.
Save		Selecione o formato no qual salvar o relatório e clique em **Save**. Especifique o local onde deseja salvar o relatório.

4.2.3 Relatórios personalizados

Relatórios personalizados permitem salvar parâmetros de relatório específicos (por exemplo, um tipo de relatório para um determinado período de data/hora) e programar a geração de relatórios. Use esse recurso para automatizar a geração de relatórios.

Configurar relatórios personalizados

1. Na configuração do GFI MailEssentials, acesse **GFI MailEssentials > Reporting > Reports**.

2. Selecione a guia **Custom Reports** e clique em **New**.

3. Configure as seguintes opções:

Opção	Descrição
Report type	Selecione o tipo de relatório a ser gerado: » **Emails Blocked**: mostra o total de emails bloqueados pelos filtros de anti-spam e antimalware para cada direção de email (de entrada, de saída e internos) de todos os emails processados. » **Emails Blocked Graph**: mostra graficamente o total de emails bloqueados pelos filtros anti-spam e antimalware para cada direção de email (de entrada, de saída e internos) de todos os emails processados. » **Email Direction Chart**: mostra graficamente o total de emails processados para cada direção de email (de entrada, de saída e internos). » **Email Direction**: exibe o número total de emails processados para cada direção de email (de entrada, de saída e internos). » **User Report**: mostra o número de emails bloqueados e permitidos para cada endereço de email. » **Spam Filter**: mostra o número total de emails bloqueados por cada filtro anti-spam. » **Spam Filter Graph**: mostra graficamente o número total de emails bloqueados por cada filtro anti-spam. Clique em **View Report Preview** para visualizar a aparência do relatório.
Date filtering	Selecione o intervalo da data do relatório. Quando selecionar **Custom date range**, especifique o período para exibir os dados, nos controles do calendário **Custom From** e **Custom To**.
Email directions filtering	Selecione uma direção de email específica para exibir os dados ou selecione **All email directions (inbound, outbound, internal)** para exibir os dados de todas as direções.
Email address filtering	Digite um endereço de email para mostrar as informações do relatório somente para determinados endereços de email.
Report Grouping	Especifique como agrupar dados. As opções disponíveis são: » **Agrupar por dia** » **Agrupar por semana** » **Agrupar por mês** » **Agrupar por ano**

4. Opcionalmente, marque a caixa de seleção **Send every** e configure a combinação data/hora para que o relatório seja gerado em uma data e hora específicas. Clique em **Add Rule** para salvar a hora de geração de relatório.

> **OBS.**
> Para excluir uma regra, selecione uma hora de geração de relatório existente e clique em **Delete**.

5. Selecione se deseja enviar o relatório por email ou salvá-lo no disco. Para enviar o relatório por email, selecione **Send by email** e forneça o endereço de email para onde o email deve ser enviado. Para salvar o relatório em disco, selecione **Save to Disk**, forneça uma localização onde o arquivo será salvo e o formato do arquivo.

6. Clique em **Save** para salvar o relatório recém-criado.

4.2.4 Como gerar relatórios personalizados

Para gerar um relatório personalizado:

1. Na configuração do GFI MailEssentials, acesse **GFI MailEssentials > Reporting > Reports**.

2. Na guia **Custom Reports**, selecione um relatório para gerar.

3. Clique em **Generate**.

4.2.5 Como excluir relatórios personalizados

Para excluir um relatório personalizado:

1. Na configuração do GFI MailEssentials, acesse **GFI MailEssentials > Reporting > Reports**.

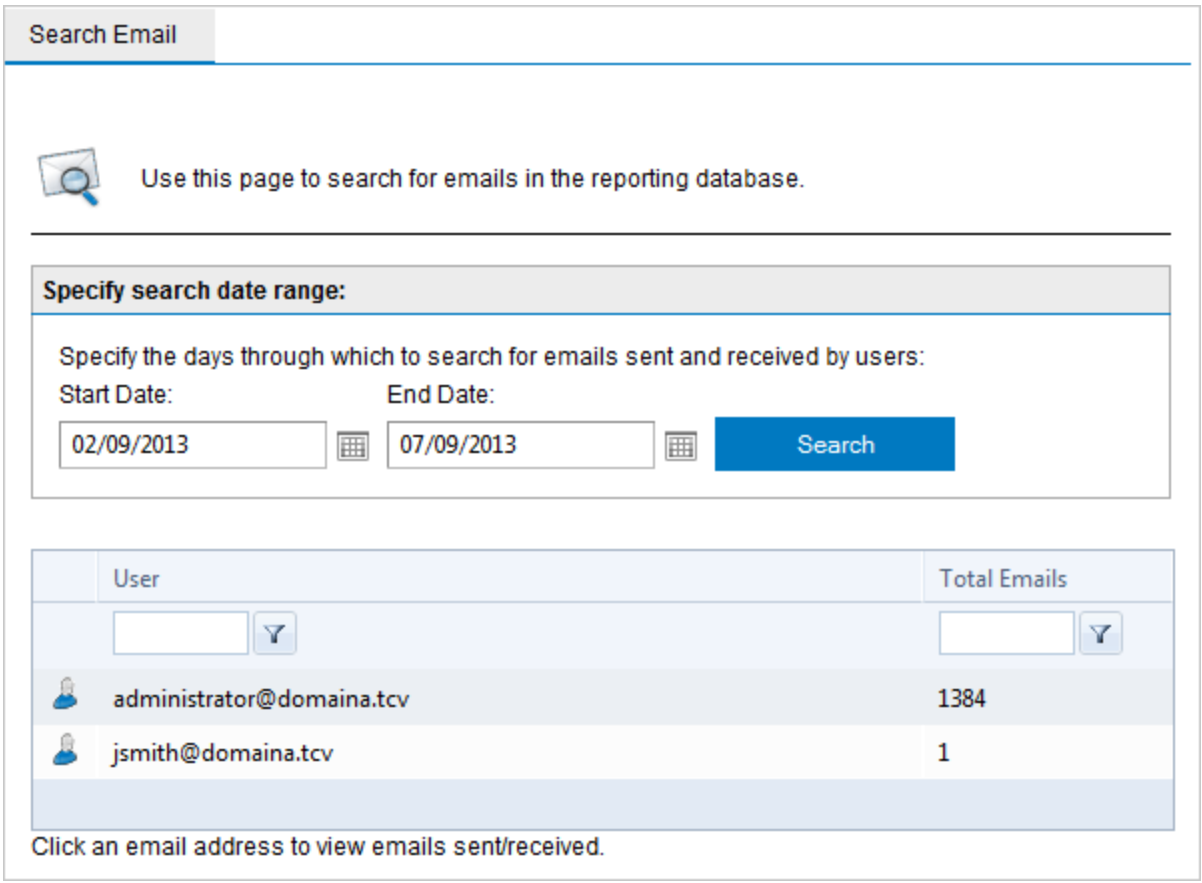
2. Na guia **Custom Reports**, selecione um relatório para excluir.

3. Clique em **Delete**.

4.2.6 Pesquisar no banco de dados de relatórios

O GFI MailEssentials armazena algumas propriedades de todos os emails processados no banco de dados de relatórios. GFI MailEssentials permite pesquisar no banco de dados de relatórios para encontrar emails processados. Para pesquisar no banco de dados de relatórios:

1. Em GFI MailEssentials Configuration, acesse **GFI MailEssentials > Reporting > Search**.

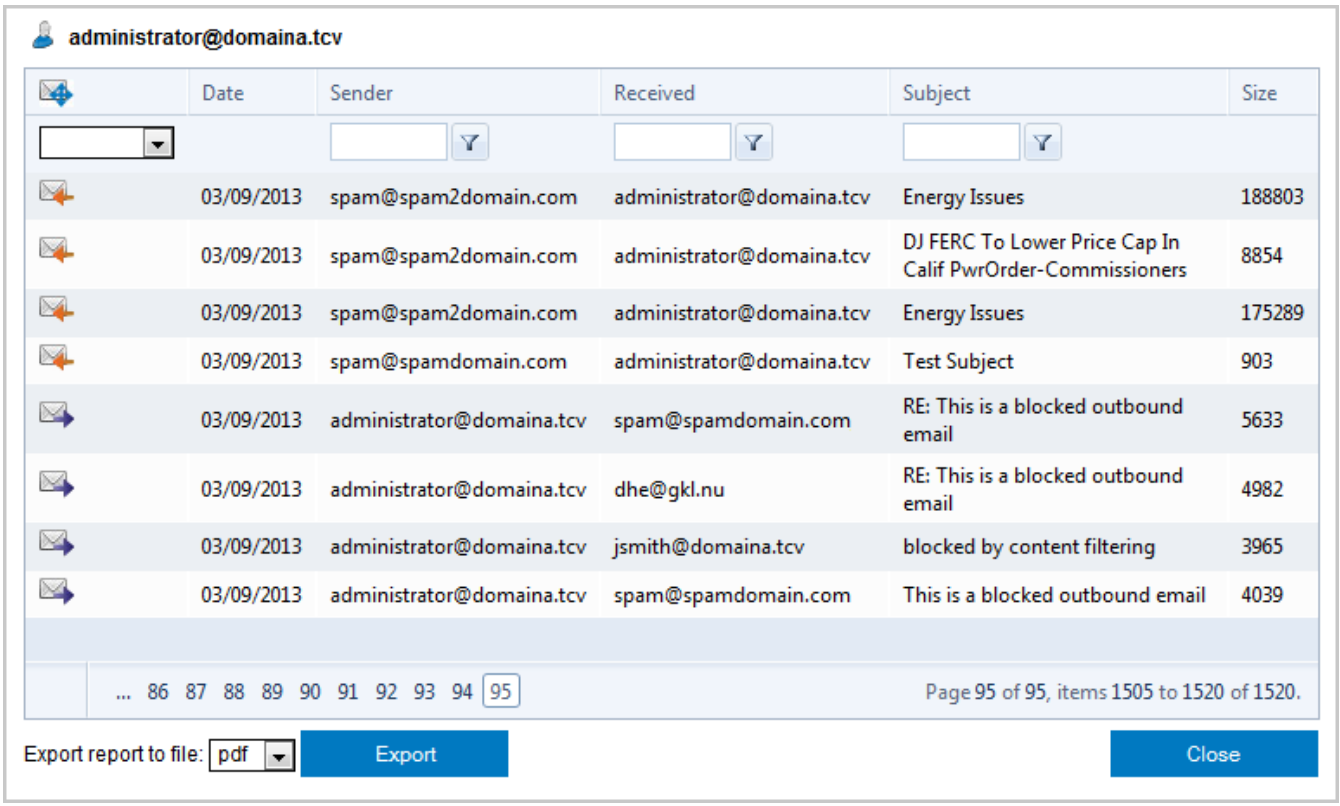


Screenshot 32: Pesquisar no banco de dados de relatórios

2. Especifique os critérios de pesquisa:

Critérios de pesquisa	Descrição
Start date e **End date**	Selecione o intervalo de datas para filtrar emails desse período. Clique em **Search**.
User	Filtrar os resultados de endereços de email. Digite o número e clique em para especificar as condições.
Total emails	Filtrar os usuários de acordo com a quantidade de emails processados. Digite o número e clique em para especificar as condições.

3. A lista de usuários correspondentes é exibida. Clique em um endereço de email para exibir o relatório detalhado dos emails processados para esse endereço de email.



Screenshot 33: Resultados da pesquisa do banco de dados de relatórios

4. (Opcional) No relatório, filtre os dados por direção de email, remetente, destinatário ou assunto.

5. Para exportar o relatório para outro formato, selecione o formato e clique em **Export**.

4.2.7 Configurar o banco de dados de relatórios

Por padrão, o GFI MailEssentials usa um banco de dados Firebird **reports.fdb** localizado em:

`<GFI MailEssentials installation path>\GFI\MailEssentials\data\`

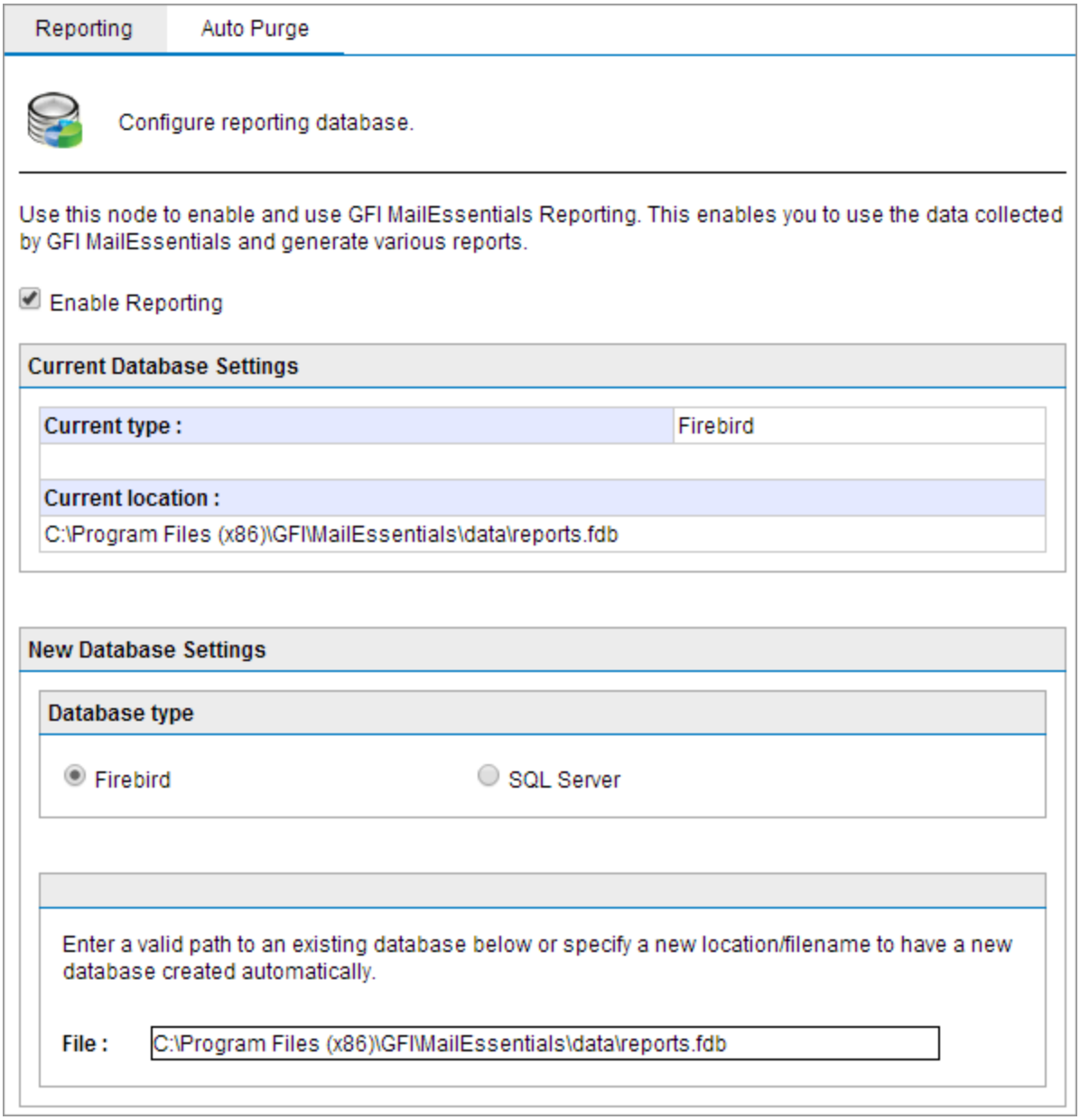
Você também pode usar um banco de dados do Microsoft® SQL Server para relatórios.

» Configurar um back-end do banco de dados Firebird

» Configurar um back-end do banco de dados do Microsoft® SQL Server

» Configurar a limpeza automática do banco de dados

Configurar um back-end do banco de dados Firebird



Screenshot 34: Configurar um back-end do banco de dados Firebird

1. Acesse **Reporting > Settings**.

2. Selecione **Firebird**.

3. Digite o caminho completo, incluindo o nome de arquivo (e a extensão .fdb), do arquivo do banco de dados. Se você especificar apenas um nome de arquivo, o arquivo de banco de dados será criado no seguinte caminho padrão:

`<GFI MailEssentials installation path>\GFI\MailEssentials\data\`

4. Clique em **Apply**.

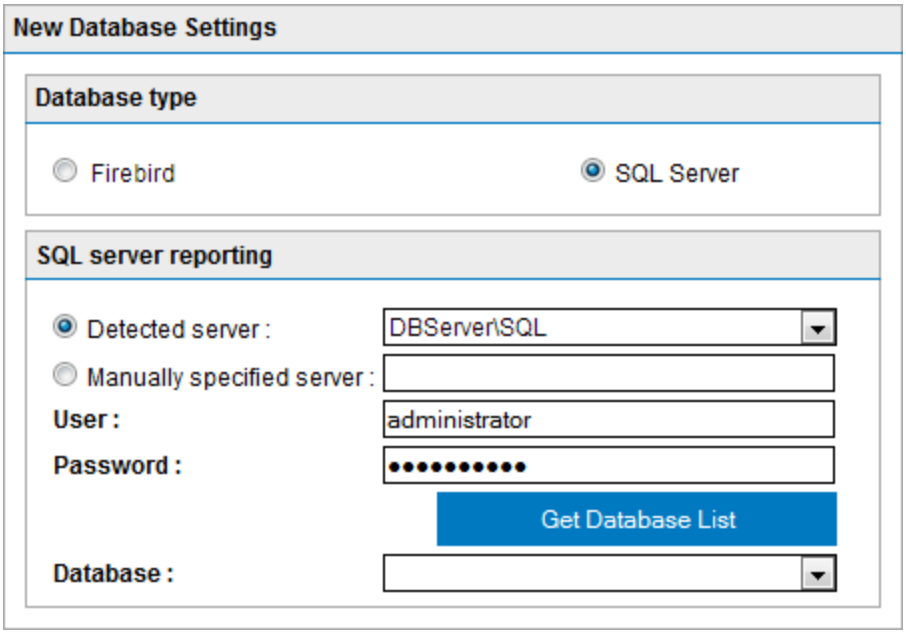
OBS.
Uma notificação de email é enviada para o administrador quando o banco de dados atinge 7 GB desde que isso possa ter um impacto no desempenho. Se for o caso é recomendado utilizar o Auto-Purging para remover emails anteriores a uma certa data.

Configurar um back-end de banco de dados do Microsoft® SQL Server

1. Crie um novo banco de dados no Microsoft® SQL Server.

2. Crie um usuário/logon dedicado no Microsoft® SQL Server, mapeado para o recém criado banco de dados. Garante o acesso completo a todos os servidores e funções e permissões do banco de dados.

3. Em GFI MailEssentials acesse **Reporting > Settings**.



Screenshot 35: Configurar o back-end do banco de dados do SQL Server

4. Selecione **SQL Server**.

5. Selecione **Detected server** e selecione o SQL Server detectado automaticamente na lista. Se o servidor não for detectado, selecione **Manually specified server** e digite o endereço IP ou o nome do servidor do Microsoft® SQL Server.

6. Digite as credenciais com permissões de gravação/leitura para o banco de dados.

7. Clique em **Get Database List** para extrair a lista de bancos de dados do servidor.

8. Na lista **Database**, selecione o banco de dados criado para a geração de relatórios do GFI MailEssentials.

9. Clique em **Apply**.

Configurar a limpeza automática do banco de dados

Você pode configurar o GFI MailEssentials para excluir automaticamente (limpeza automática) os registros do banco de dados que forem mais antigos do que um determinado período.

Por padrão o Auto-Purging é configurado para excluir dados com mais de 12 meses.

Para habilitar a limpeza automática:

1. Acesse **Reporting > Settings** e selecione **Auto-purge**.

2. Selecione **Enable Auto-Purging** e especificar por quanto tempo os itens no banco de dados deve ser armazenado em meses.

3. Clique em **Apply**.

> **OBS.**
> A limpeza automática é aplicada apenas ao banco de dados atual configurado na guia Reporting.

4.2.8 Relatório do MailInsights®

O MailInsights® é um recurso para gerar relatórios que usa os dados do banco de dados de relatórios para fornecer informações relacionadas às tendências e ao uso do email.

O GFI MailEssentials fornece o relatório Fluxo de comunicação que oferece uma representação gráfica dos emails trocados entre os usuários/grupos selecionados e seus contatos. Outros relatórios do MailInsights® podem ser gerados com o GFI MailArchiver.

Relatório Fluxo de comunicação

O relatório Fluxo de comunicação mostra os 20 principais contatos com os quais um usuário se comunicou nos 30 dias anteriores.

1. Navegue para **Relatórios > MailInsights** e selecione a guia **Fluxo de comunicação**.

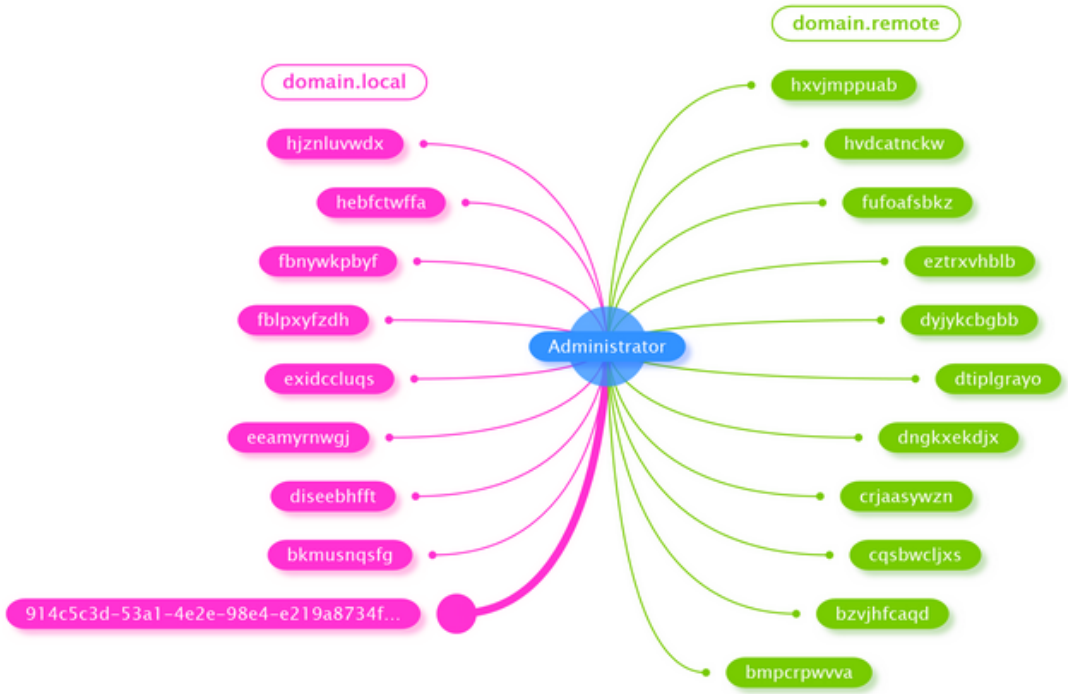
2. O administrador pode gerar o relatório para qualquer usuário de email. Clique em **Pesquisar** para selecionar um usuário de email e clique em **Gerar** para começar a criar o relatório.

O relatório gerado exibe os dados do usuário selecionado da seguinte forma:

Totais	A área superior do relatório mostra o total das estatísticas do fluxo de comunicação nos 30 dias anteriores. » **Total de contatos** - o número total de endereços de email com os quais o usuário se comunicou. » **Total interno** - o número total de usuários internos com quem o usuário se comunicou. » **Principal interno** - o endereço de email interno com o qual o usuário selecionado se comunicou mais. » **Total externo** - o número total de usuários externos com quem o usuário se comunicou. » **Principal externo** - o endereço de email externo com o qual o usuário selecionado se comunicou mais.
Gráfico	O usuário selecionado é exibido como uma entidade única na área central do gráfico. Os contatos são separados por domínios. Cada cluster de domínio é mostrado em uma cor diferente. A largura da margem entre os nós mostra a força da relação dos emails entre as diferentes entidades.
20 principais contatos	Os 20 principais contatos com quem o usuário selecionado mais se comunicou. Os códigos de cores indicam os domínios dos diferentes contatos. A tabela indica o número total de emails enviados e recebidos com aquele contato, junto com a data e a hora da última comunicação.

Top 20 Contacts - Last 30 days

Total Contacts	Total Internal	Top Internal	Total External	Top External
20	20	914c5c3d-53a1-4e2e-98e4-e219a8734f78@domain.local	0	
100% of Total Contacts	100% of Total Contacts	5	0% of Total Contacts	0



Screenshot 36: Relatório de fluxo de comunicação do MailInsights®

5 Segurança de email

Os filtros de segurança do GFI MailEssentials oferecem proteção contra vírus e outros emails mal-intencionados.

Tópicos deste capítulo:

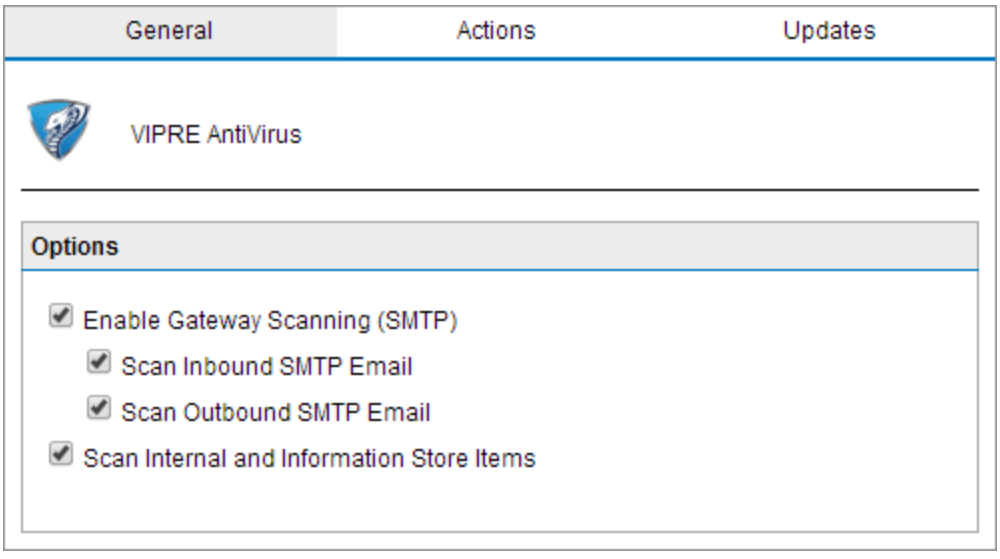
5.1 Mecanismos de verificação de vírus

O GFI MailEssentials utiliza vários mecanismos antivírus para verificar a presença de vírus em emails de entrada, de saída e internos. GFI MailEssentials é fornecido com os mecanismos de verificação de vírus Vipre and BitDefender. Você também pode adquirir uma licença do Kaspersky, Avira e McAfee.

Este capítulo descreve como configurar mecanismos de verificação de vírus, atualizações, ações e a sequência de verificação.

5.1.1 Vipre

1. Acesse **Email Security > Virus Scanning Engines > Vipre**.



Screenshot 37: Configuração do Vipre

2. Selecione a caixa de seleção **Enable Gateway Scanning (SMTP)** para fazer a verificação de mensagens utilizando o Mecanismo de verificação de vírus.

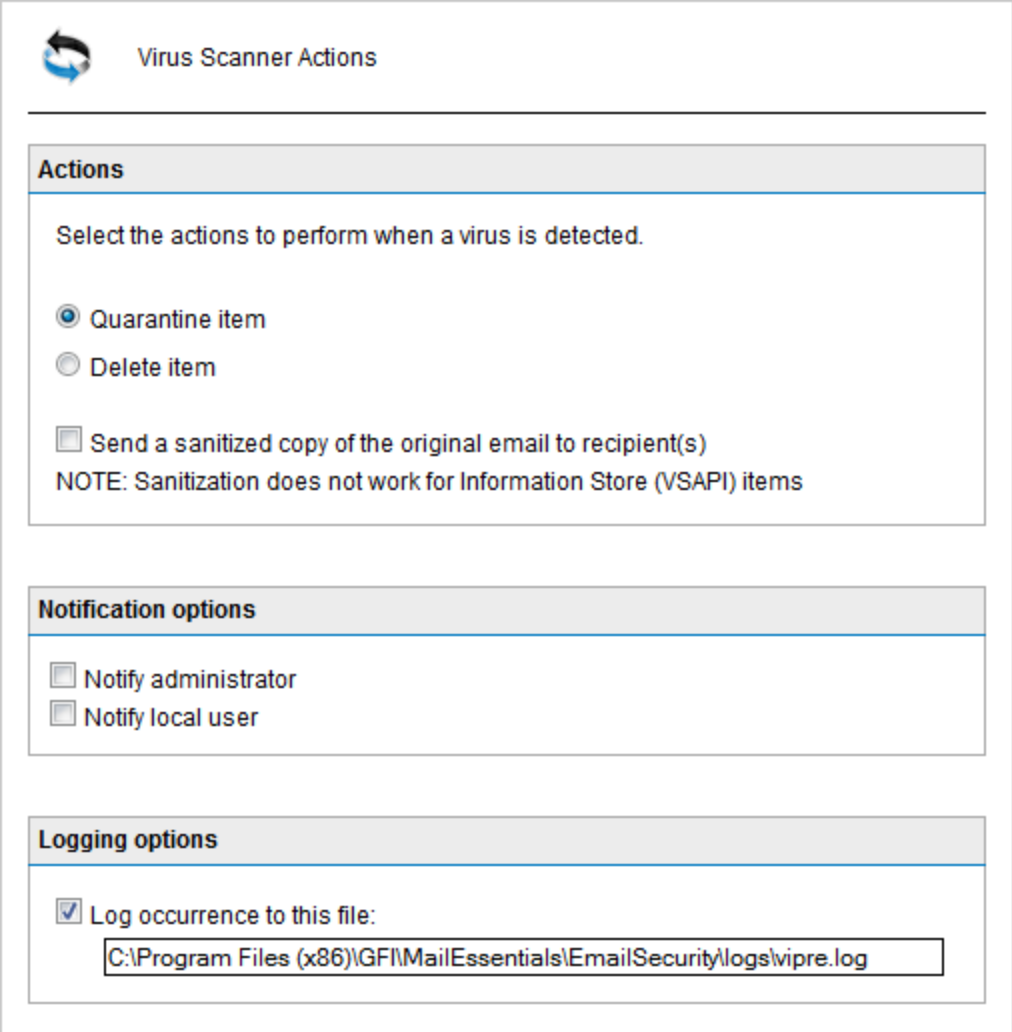
3. Selecione se deseja fazer a verificação de emails de entrada e/ou saída usando o mecanismo de verificação de vírus.

Opção	Descrição
Verificar emails SMTP de entrada	Selecione esta opção para verificar emails de entrada
Verificar emails SMTP de saída	Selecione esta opção para verificar emails de saída

4. Se você instalou o GFI MailEssentials em uma máquina com o Microsoft® Exchange, também terá a opção de verificar os emails internos e o Information Store. Selecione **Scan Internal and Information Store Items**.

OBS.
Para usar o recurso Verificação antivírus do armazenamento de informações, é necessário ativar a opção no nó **Information Store Protection**. Para obter mais informações, consulte Proteção de armazenamento de informações (página 94).

OBS.
Nessa página, você também pode analisar a licença do mecanismo antivírus e as informações da versão.



Screenshot 38: Ações do mecanismo de verificação de vírus

5. Na guia **Actions**, escolha a ação a ser executada quando um email for bloqueado:

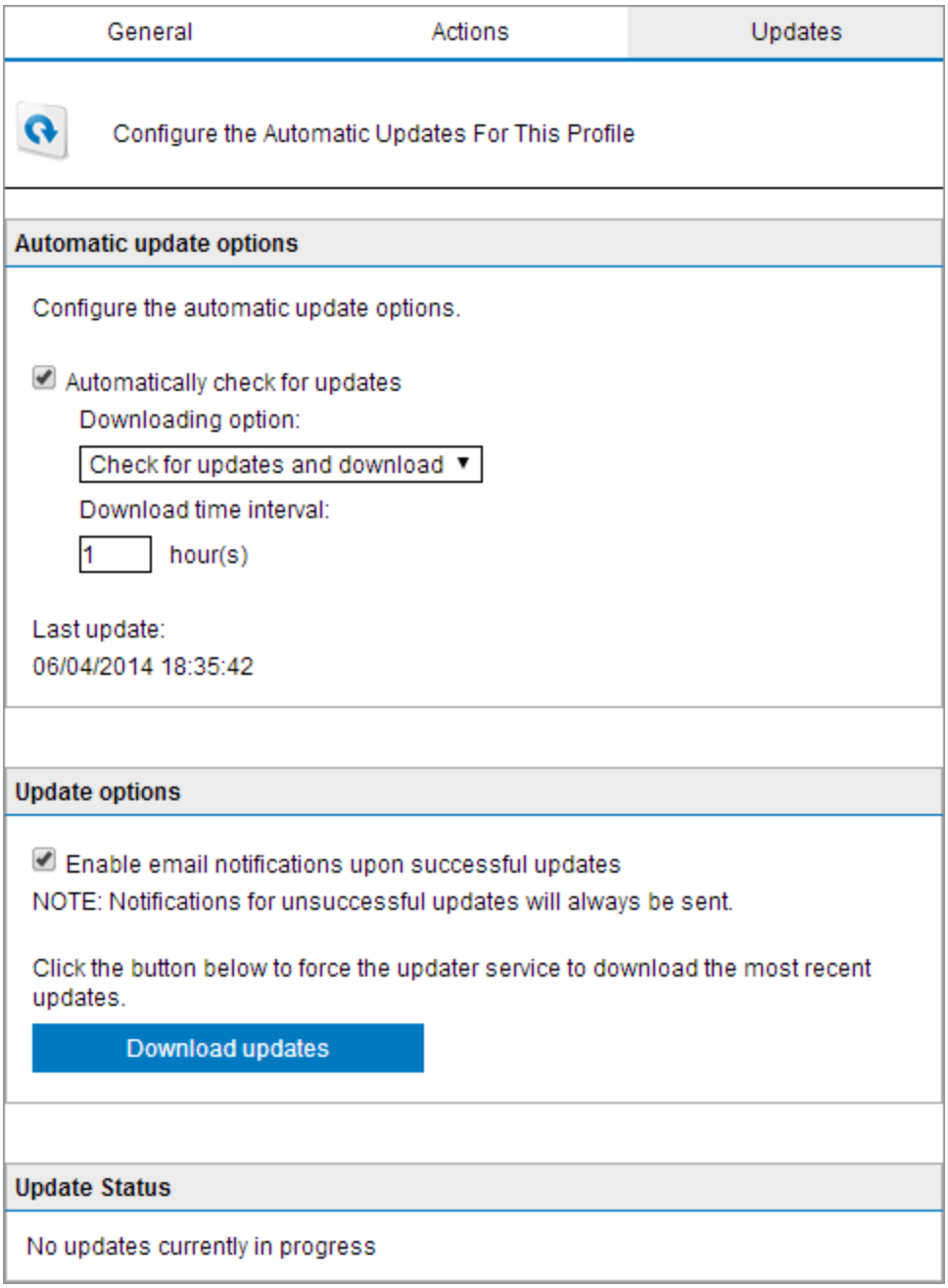
Ação	Descrição
Quarantine email	Armazena todos os emails infectados detectados pelo mecanismo de verificação de vírus selecionado no armazenamento de quarentena. Em seguida, você pode analisar (aprovar/excluir) todos os emails em quarentena. Para obter mais informações, consulte Quarentena (página 203).
Delete email	Exclui emails infectados.
Send a sanitized copy of the original email to recipient(s)	Escolha se deseja enviar uma cópia limpa do email bloqueado para os destinatários.

6. O GFI MailEssentials pode enviar notificações por email quando um email acionar esse filtro. Para ativar esse recurso, selecione uma das seguintes opções:

Opção	Descrição
Notify administrator	Notifique o administrador sempre que esse mecanismo bloquear uma mensagem de email. Para obter mais informações, consulte Endereço de email do administrador (página 240).
Notify local user	Notifique os destinatários locais de email sobre o email bloqueado.

7. Para registrar a atividade deste mecanismo em um arquivo de registro, selecione **Log occurrence to this file**. Na caixa de texto, especifique o caminho e o nome do arquivo para um local personalizado no disco onde armazenar o arquivo de registro. Por padrão, os arquivos de registro são armazenados em:

<GFI MailEssentials installation path>\GFI\MailEssentials\EmailSecurity\Logs\<Nome do mecanismo>.log



Screenshot 39: Guia de atualização do mecanismo

8. Na guia **Updates**, selecione **Automatically check for updates** para ativar a atualização automática do mecanismo selecionado.

9. Na lista **Downloading option**, selecione uma das seguintes opções:

Opção	Descrição
Only check for updates	Selecione esta opção se você deseja que o GFI MailEssentials apenas verifique e notifique o administrador quando atualizações estiverem disponíveis para esse mecanismo. Esta opção NÃO fará o download das atualizações disponíveis automaticamente.
Check for updates and download	Selecione esta opção se você deseja que o GFI MailEssentials verifique e faça o download automaticamente das atualizações disponíveis para este mecanismo.

10. Especifique a frequência com que você deseja que o GFI MailEssentials verifique/faça o download das atualizações para este mecanismo, especificando um valor de intervalo em horas.

11. Na área **Update options**, selecione **Enable email notifications upon successful updates** para enviar uma notificação por email ao administrador quando a atualização do mecanismo for concluída.

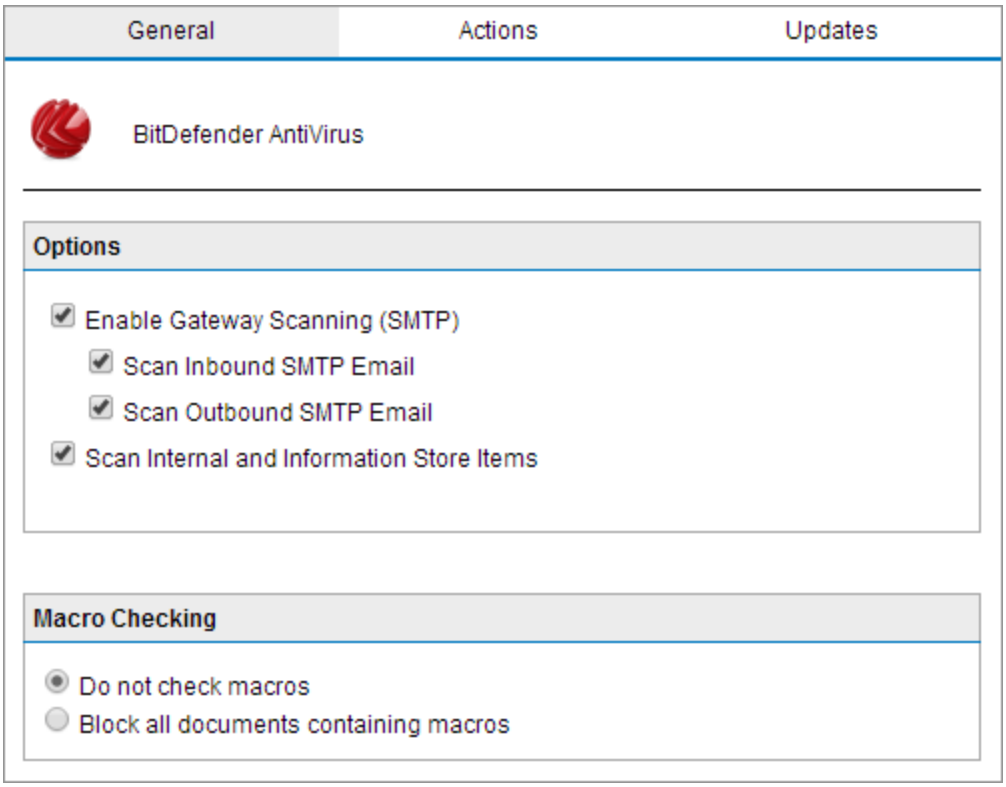
> **OBS.**
> Uma notificação por email será enviada quando uma atualização falhar.

12. Para verificar e baixar as atualizações imediatamente, clique em **Download updates**.

13. Clique em **Apply**.

5.1.2 BitDefender

1. Acesse **Email Security > Virus Scanning Engines > BitDefender**.



Screenshot 40: Configuração do Bitdefender

2. Selecione a caixa de seleção **Enable Gateway Scanning (SMTP)** para fazer a verificação de mensagens utilizando o Mecanismo de verificação de vírus.

3. Selecione se deseja fazer a verificação de emails de entrada e/ou saída usando o mecanismo de verificação de vírus.

Opção	Descrição
Verificar emails SMTP de entrada	Selecione esta opção para verificar emails de entrada
Verificar emails SMTP de saída	Selecione esta opção para verificar emails de saída

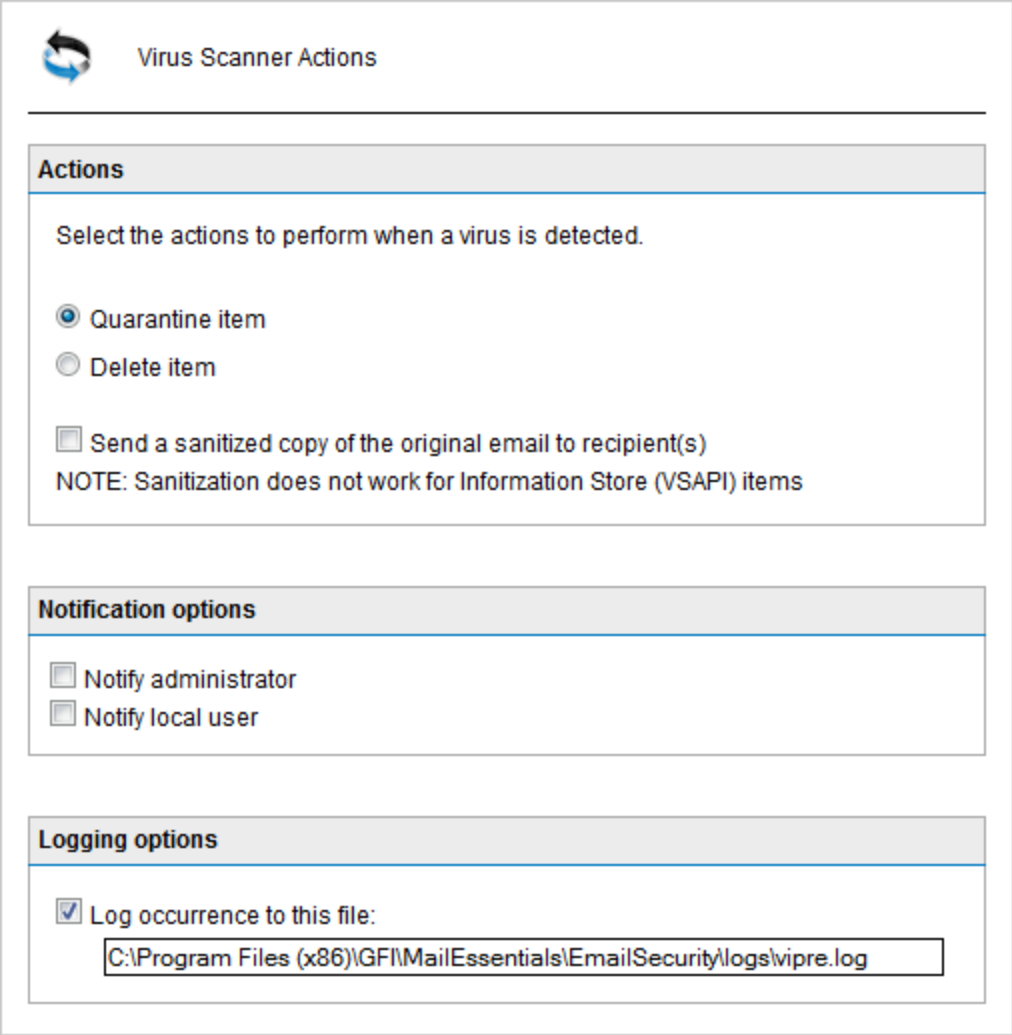
4. Se você instalou o GFI MailEssentials em uma máquina com o Microsoft® Exchange, também terá a opção de verificar os emails internos e o Information Store. Selecione **Scan Internal and Information Store Items**.

> **OBS.**
> Para usar o recurso Verificação antivírus do armazenamento de informações, é necessário ativar a opção no nó **Information Store Protection**. Para obter mais informações, consulte Proteção de armazenamento de informações (página 94).

> **OBS.**
> Nessa página, você também pode analisar a licença do mecanismo antivírus e as informações da versão.

5. O Bitdefender também pode ser usado para bloquear emails com anexos que contenham macros. Para habilitar esse recurso na área **Macro Checking**, selecione **Block all documents containing macros**.

> **OBS.**
> Se a verificação de macro estiver desabilitada, o GFI MailEssentials ainda poderá verificar e bloquear vírus de macro.



Screenshot 41: Ações do mecanismo de verificação de vírus

6. Na guia **Actions**, escolha a ação a ser executada quando um email for bloqueado:

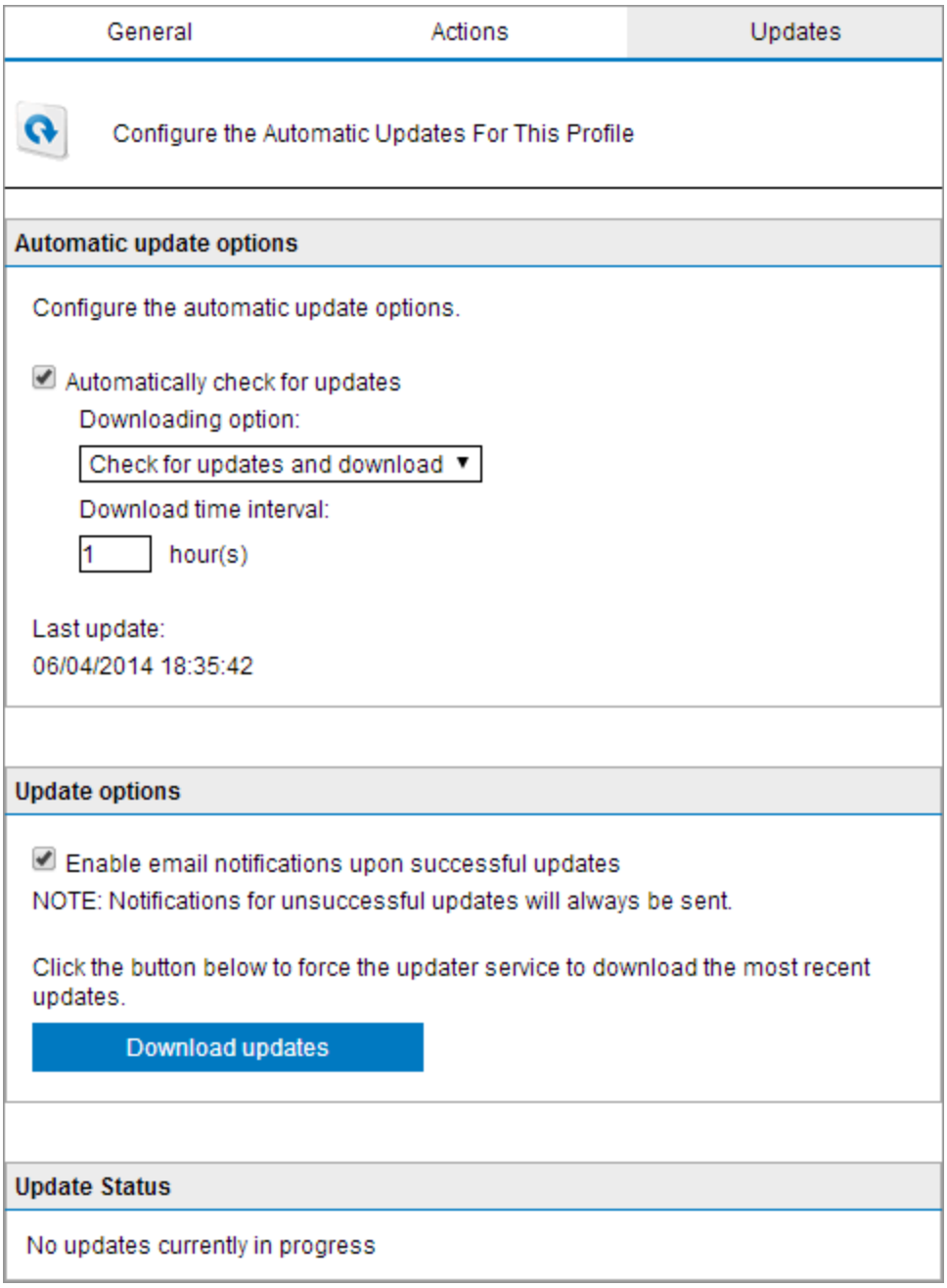
Ação	Descrição
Quarantine email	Armazena todos os emails infectados detectados pelo mecanismo de verificação de vírus selecionado no armazenamento de quarentena. Em seguida, você pode analisar (aprovar/excluir) todos os emails em quarentena. Para obter mais informações, consulte Quarentena (página 203).
Delete email	Exclui emails infectados.
Send a sanitized copy of the original email to recipient(s)	Escolha se deseja enviar uma cópia limpa do email bloqueado para os destinatários.

7. O GFI MailEssentials pode enviar notificações por email quando um email acionar esse filtro. Para ativar esse recurso, selecione uma das seguintes opções:

Opção	Descrição
Notify administrator	Notifique o administrador sempre que esse mecanismo bloquear uma mensagem de email. Para obter mais informações, consulte Endereço de email do administrador (página 240).
Notify local user	Notifique os destinatários locais de email sobre o email bloqueado.

8. Para registrar a atividade deste mecanismo em um arquivo de registro, selecione **Log occurrence to this file**. Na caixa de texto, especifique o caminho e o nome do arquivo para um local personalizado no disco onde armazenar o arquivo de registro. Por padrão, os arquivos de registro são armazenados em:

<GFI MailEssentials installation path>\GFI\MailEssentials\EmailSecurity\Logs\<Nome do mecanismo>.log



Screenshot 42: Guia de atualização do mecanismo

9. Na guia **Updates**, selecione **Automatically check for updates** para ativar a atualização automática do mecanismo selecionado.

10. Na lista **Downloading option**, selecione uma das seguintes opções:

Opção	Descrição
Only check for updates	Selecione esta opção se você deseja que o GFI MailEssentials apenas verifique e notifique o administrador quando atualizações estiverem disponíveis para esse mecanismo. Esta opção NÃO fará o download das atualizações disponíveis automaticamente.
Check for updates and download	Selecione esta opção se você deseja que o GFI MailEssentials verifique e faça o download automaticamente das atualizações disponíveis para este mecanismo.

11. Especifique a frequência com que você deseja que o GFI MailEssentials verifique/faça o download das atualizações para este mecanismo, especificando um valor de intervalo em horas.

12. Na área **Update options**, selecione **Enable email notifications upon successful updates** para enviar uma notificação por email ao administrador quando a atualização do mecanismo for concluída.

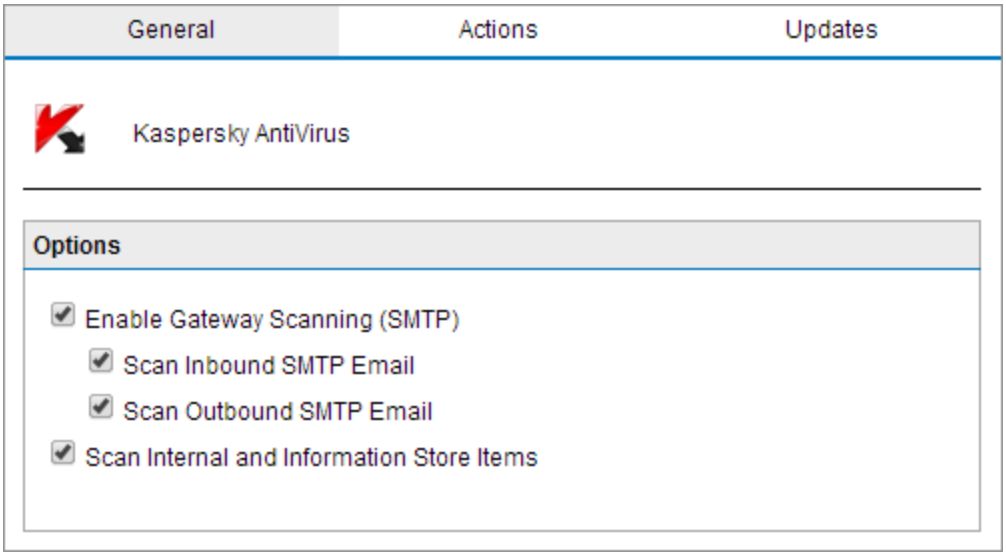
> **OBS.**
> Uma notificação por email será enviada quando uma atualização falhar.

13. Para verificar e baixar as atualizações imediatamente, clique em **Download updates**.

14. Clique em **Apply**.

5.1.3 Kaspersky

1. Acesse **Email Security > Virus Scanning Engines > Kaspersky**.



Screenshot 43: Configuração do Kaspersky

2. Selecione a caixa de seleção **Enable Gateway Scanning (SMTP)** para fazer a verificação de mensagens utilizando o Mecanismo de verificação de vírus.

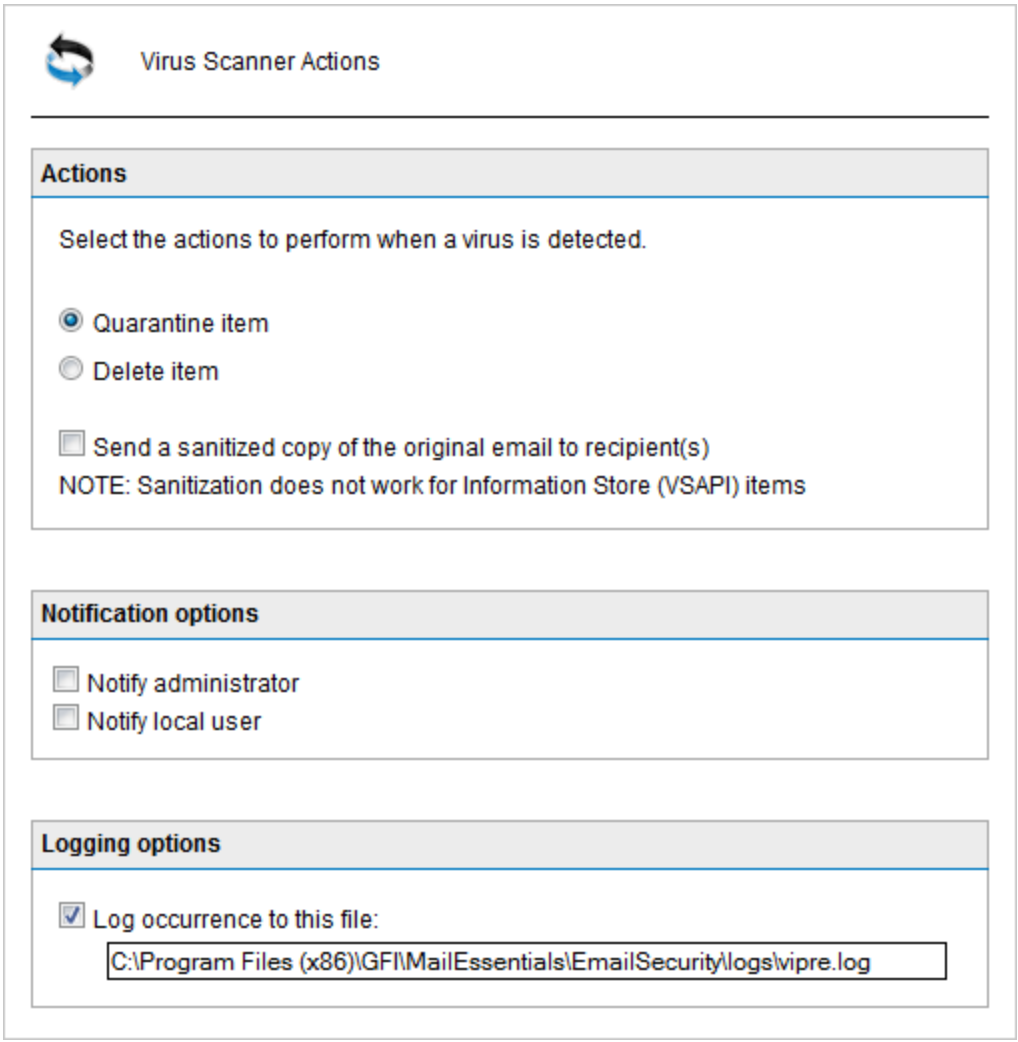
3. Selecione se deseja fazer a verificação de emails de entrada e/ou saída usando o mecanismo de verificação de vírus.

Opção	Descrição
Verificar emails SMTP de entrada	Selecione esta opção para verificar emails de entrada
Verificar emails SMTP de saída	Selecione esta opção para verificar emails de saída

4. Se você instalou o GFI MailEssentials em uma máquina com o Microsoft® Exchange, também terá a opção de verificar os emails internos e o Information Store. Selecione **Scan Internal and Information Store Items**.

OBS.
Para usar o recurso Verificação antivírus do armazenamento de informações, é necessário ativar a opção no nó **Information Store Protection**. Para obter mais informações, consulte Proteção de armazenamento de informações (página 94).

OBS.
Nessa página, você também pode analisar a licença do mecanismo antivírus e as informações da versão.



Screenshot 44: Ações do mecanismo de verificação de vírus

5. Na guia **Actions**, escolha a ação a ser executada quando um email for bloqueado:

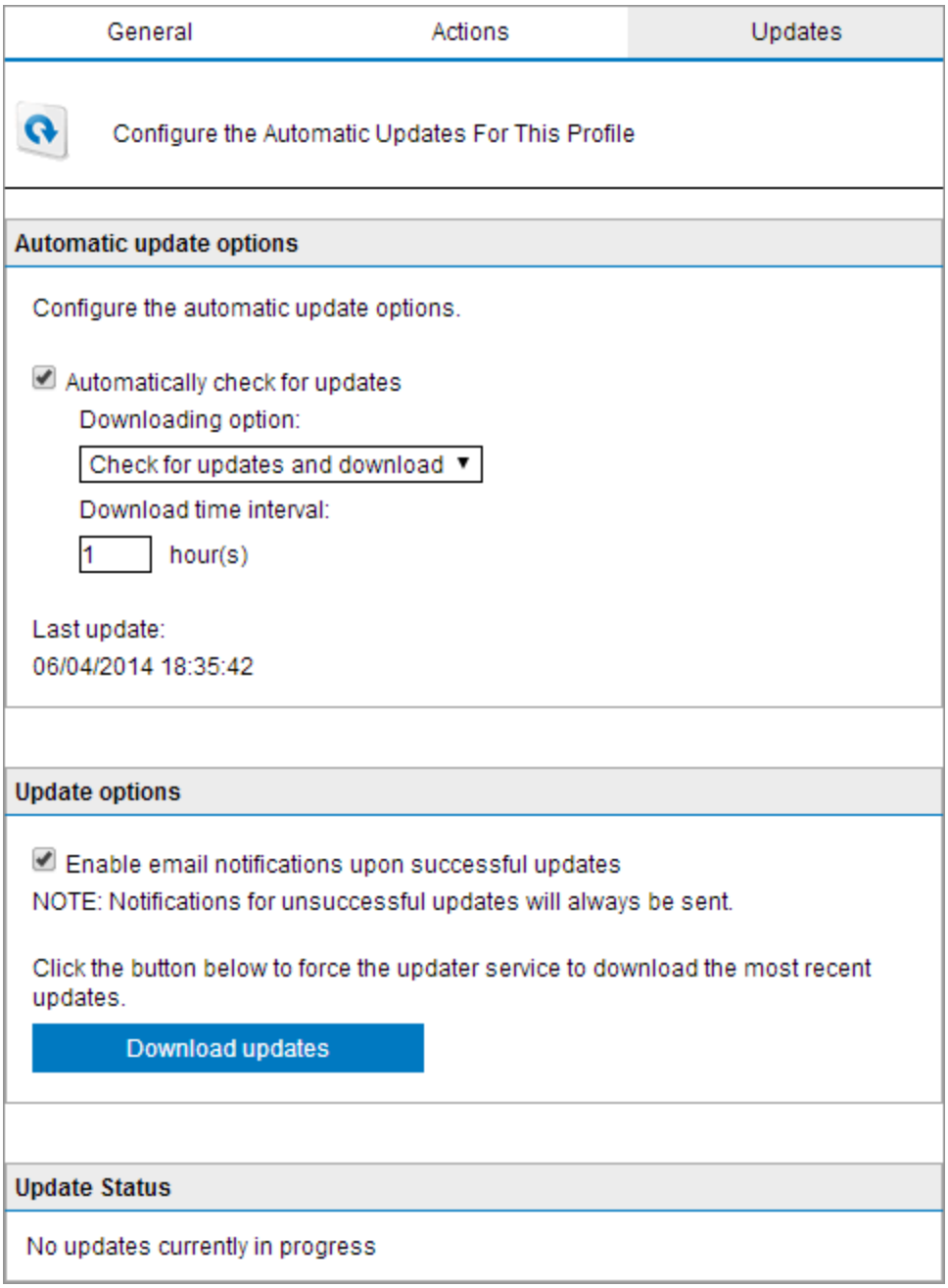
Ação	Descrição
Quarantine email	Armazena todos os emails infectados detectados pelo mecanismo de verificação de vírus selecionado no armazenamento de quarentena. Em seguida, você pode analisar (aprovar/excluir) todos os emails em quarentena. Para obter mais informações, consulte Quarentena (página 203).
Delete email	Exclui emails infectados.
Send a sanitized copy of the original email to recipient(s)	Escolha se deseja enviar uma cópia limpa do email bloqueado para os destinatários.

6. O GFI MailEssentials pode enviar notificações por email quando um email acionar esse filtro. Para ativar esse recurso, selecione uma das seguintes opções:

Opção	Descrição
Notify administrator	Notifique o administrador sempre que esse mecanismo bloquear uma mensagem de email. Para obter mais informações, consulte Endereço de email do administrador (página 240).
Notify local user	Notifique os destinatários locais de email sobre o email bloqueado.

7. Para registrar a atividade deste mecanismo em um arquivo de registro, selecione **Log occurrence to this file**. Na caixa de texto, especifique o caminho e o nome do arquivo para um local personalizado no disco onde armazenar o arquivo de registro. Por padrão, os arquivos de registro são armazenados em:

<GFI MailEssentials installation path>\GFI\MailEssentials\EmailSecurity\Logs\<Nome do mecanismo>.log



Screenshot 45: Guia de atualização do mecanismo

8. Na guia **Updates**, selecione **Automatically check for updates** para ativar a atualização automática do mecanismo selecionado.

9. Na lista **Downloading option**, selecione uma das seguintes opções:

Opção	Descrição
Only check for updates	Selecione esta opção se você deseja que o GFI MailEssentials apenas verifique e notifique o administrador quando atualizações estiverem disponíveis para esse mecanismo. Esta opção NÃO fará o download das atualizações disponíveis automaticamente.
Check for updates and download	Selecione esta opção se você deseja que o GFI MailEssentials verifique e faça o download automaticamente das atualizações disponíveis para este mecanismo.

10. Especifique a frequência com que você deseja que o GFI MailEssentials verifique/faça o download das atualizações para este mecanismo, especificando um valor de intervalo em horas.

11. Na área **Update options**, selecione **Enable email notifications upon successful updates** para enviar uma notificação por email ao administrador quando a atualização do mecanismo for concluída.

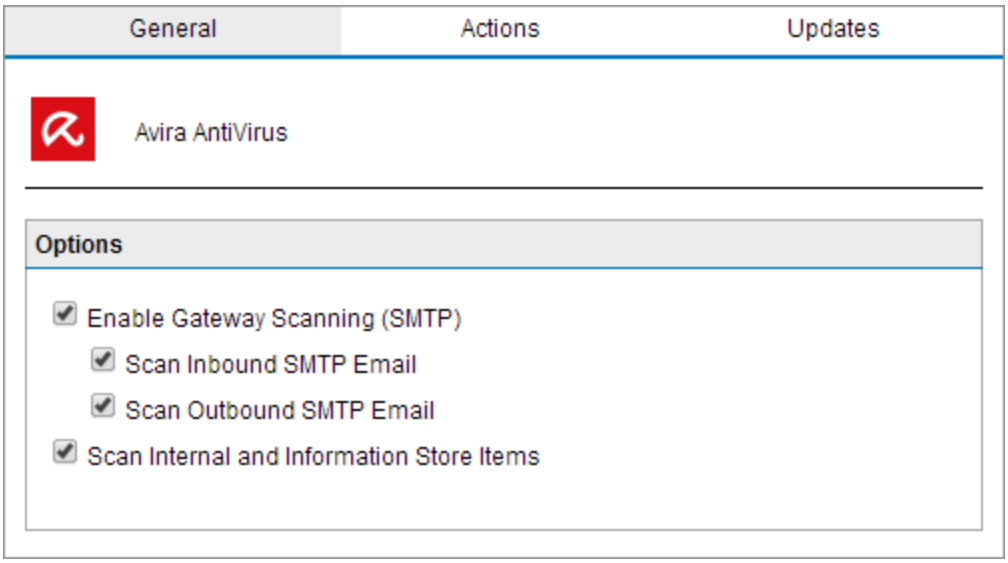
> **OBS.**
> Uma notificação por email será enviada quando uma atualização falhar.

12. Para verificar e baixar as atualizações imediatamente, clique em **Download updates**.

13. Clique em **Apply**.

5.1.4 Avira

1. Acesse **Email Security > Virus Scanning Engines > Avira**.



Screenshot 46: Configuração Avira

2. Selecione a caixa de seleção **Enable Gateway Scanning (SMTP)** para fazer a verificação de mensagens utilizando o Mecanismo de verificação de vírus.

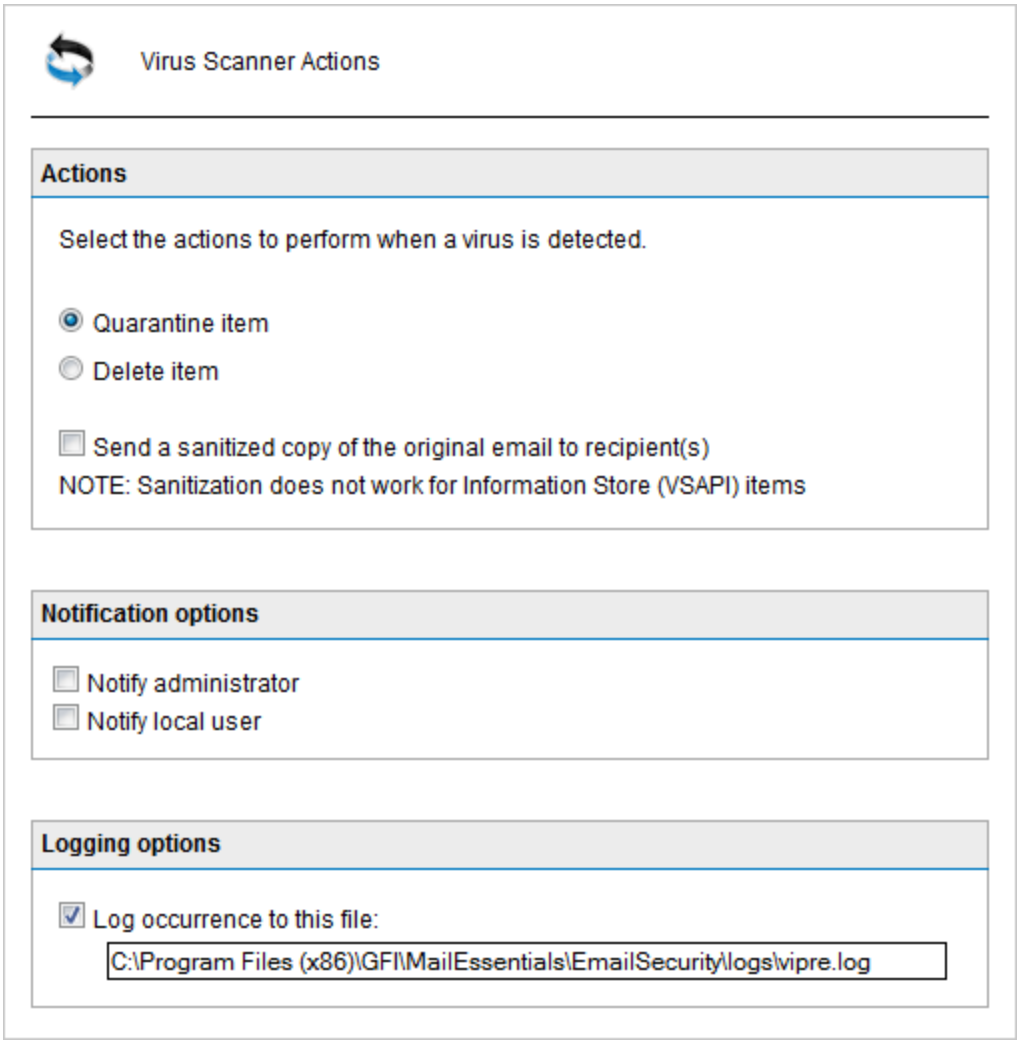
3. Selecione se deseja fazer a verificação de emails de entrada e/ou saída usando o mecanismo de verificação de vírus.

Opção	Descrição
Verificar emails SMTP de entrada	Selecione esta opção para verificar emails de entrada
Verificar emails SMTP de saída	Selecione esta opção para verificar emails de saída

4. Se você instalou o GFI MailEssentials em uma máquina com o Microsoft® Exchange, também terá a opção de verificar os emails internos e o Information Store. Selecione **Scan Internal and Information Store Items**.

OBS.
Para usar o recurso Verificação antivírus do armazenamento de informações, é necessário ativar a opção no nó **Information Store Protection**. Para obter mais informações, consulte Proteção de armazenamento de informações (página 94).

OBS.
Nessa página, você também pode analisar a licença do mecanismo antivírus e as informações da versão.



Screenshot 47: Ações do mecanismo de verificação de vírus

5. Na guia **Actions**, escolha a ação a ser executada quando um email for bloqueado:

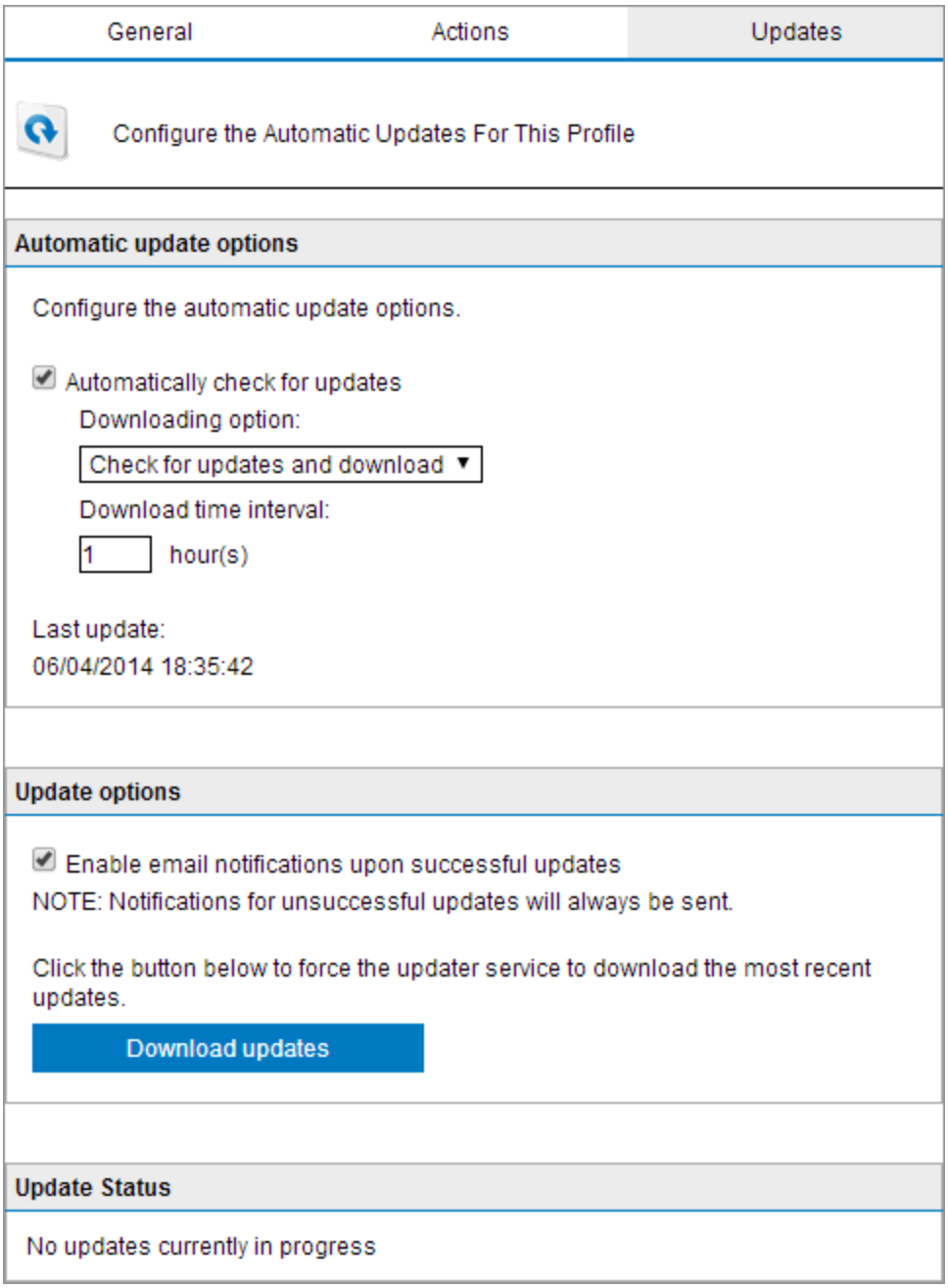
Ação	Descrição
Quarantine email	Armazena todos os emails infectados detectados pelo mecanismo de verificação de vírus selecionado no armazenamento de quarentena. Em seguida, você pode analisar (aprovar/excluir) todos os emails em quarentena. Para obter mais informações, consulte Quarentena (página 203).
Delete email	Exclui emails infectados.
Send a sanitized copy of the original email to recipient(s)	Escolha se deseja enviar uma cópia limpa do email bloqueado para os destinatários.

6. O GFI MailEssentials pode enviar notificações por email quando um email acionar esse filtro. Para ativar esse recurso, selecione uma das seguintes opções:

Opção	Descrição
Notify administrator	Notifique o administrador sempre que esse mecanismo bloquear uma mensagem de email. Para obter mais informações, consulte Endereço de email do administrador (página 240).
Notify local user	Notifique os destinatários locais de email sobre o email bloqueado.

7. Para registrar a atividade deste mecanismo em um arquivo de registro, selecione **Log occurrence to this file**. Na caixa de texto, especifique o caminho e o nome do arquivo para um local personalizado no disco onde armazenar o arquivo de registro. Por padrão, os arquivos de registro são armazenados em:

<GFI MailEssentials installation path>\GFI\MailEssentials\EmailSecurity\Logs\<Nome do mecanismo>.log



Screenshot 48: Guia de atualização do mecanismo

8. Na guia **Updates**, selecione **Automatically check for updates** para ativar a atualização automática do mecanismo selecionado.

9. Na lista **Downloading option**, selecione uma das seguintes opções:

Opção	Descrição
Only check for updates	Selecione esta opção se você deseja que o GFI MailEssentials apenas verifique e notifique o administrador quando atualizações estiverem disponíveis para esse mecanismo. Esta opção NÃO fará o download das atualizações disponíveis automaticamente.
Check for updates and download	Selecione esta opção se você deseja que o GFI MailEssentials verifique e faça o download automaticamente das atualizações disponíveis para este mecanismo.

10. Especifique a frequência com que você deseja que o GFI MailEssentials verifique/faça o download das atualizações para este mecanismo, especificando um valor de intervalo em horas.

11. Na área **Update options**, selecione **Enable email notifications upon successful updates** para enviar uma notificação por email ao administrador quando a atualização do mecanismo for concluída.

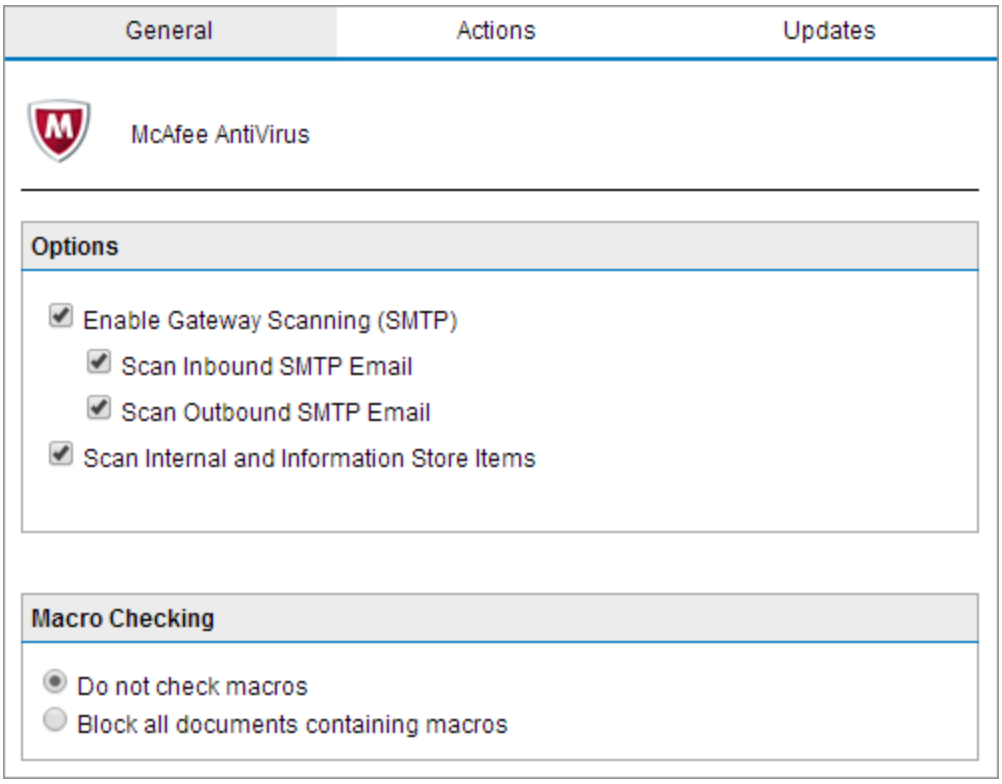
> **OBS.**
> Uma notificação por email será enviada quando uma atualização falhar.

12. Para verificar e baixar as atualizações imediatamente, clique em **Download updates**.

13. Clique em **Apply**.

5.1.5 McAfee

1. Acesse **Email Security > Virus Scanning Engines > McAfee**.



Screenshot 49: Configuração da McAfee

2. Selecione a caixa de seleção **Enable Gateway Scanning (SMTP)** para fazer a verificação de mensagens utilizando o Mecanismo de verificação de vírus.

3. Selecione se deseja fazer a verificação de emails de entrada e/ou saída usando o mecanismo de verificação de vírus.

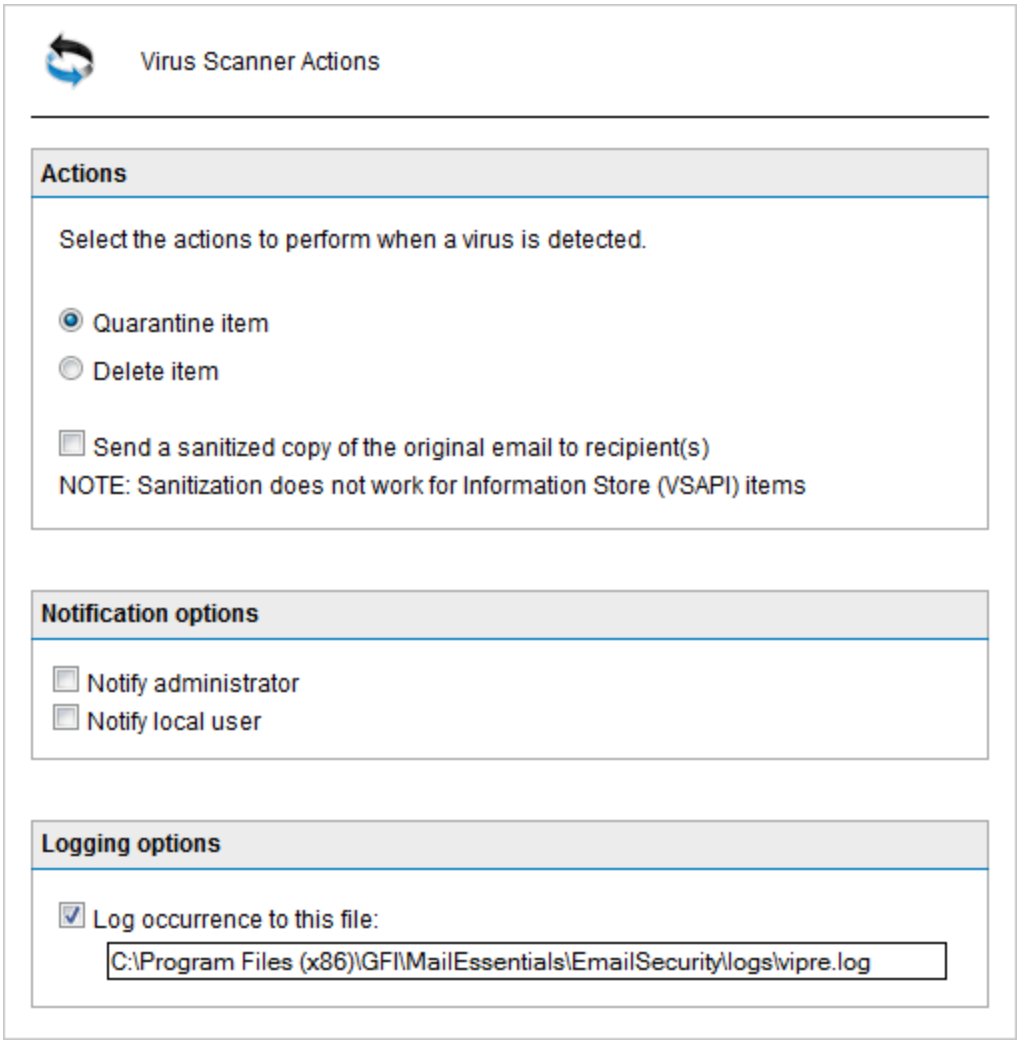
Opção	Descrição
Verificar emails SMTP de entrada	Selecione esta opção para verificar emails de entrada
Verificar emails SMTP de saída	Selecione esta opção para verificar emails de saída

4. Se você instalou o GFI MailEssentials em uma máquina com o Microsoft® Exchange, também terá a opção de verificar os emails internos e o Information Store. Selecione **Scan Internal and Information Store Items**.

> **OBS.**
> Para usar o recurso Verificação antivírus do armazenamento de informações, é necessário ativar a opção no nó **Information Store Protection**. Para obter mais informações, consulte Proteção de armazenamento de informações (página 94).

> **OBS.**
> Nessa página, você também pode analisar a licença do mecanismo antivírus e as informações da versão.

5. O antivírus da McAfee também pode ser usado para bloquear emails com anexos que contenham macros. Para habilitar esse recurso na área **Macro Checking**, selecione **Block all documents containing macros**.



Screenshot 50: Ações do mecanismo de verificação de vírus

6. Na guia **Actions**, escolha a ação a ser executada quando um email for bloqueado:

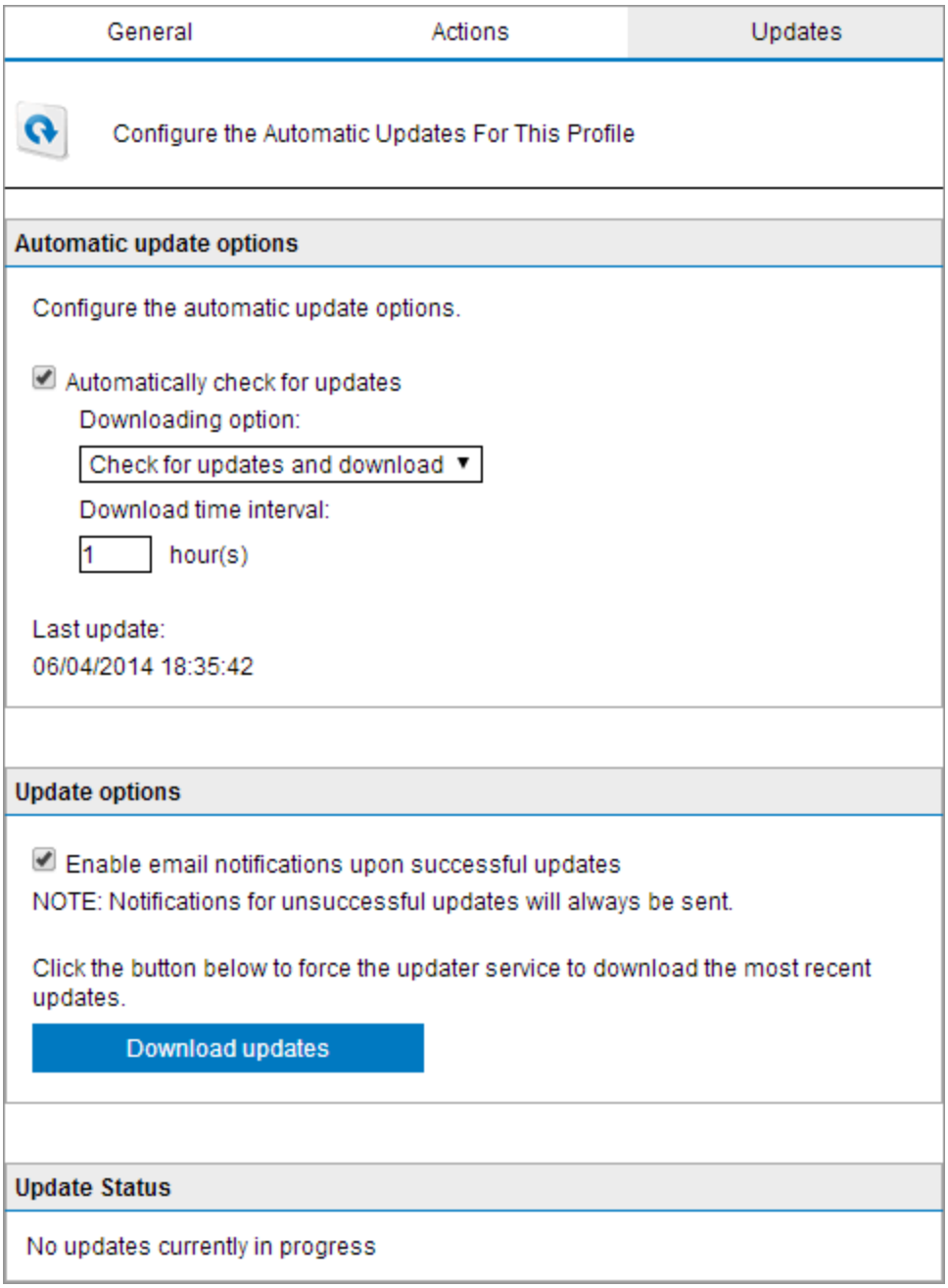
Ação	Descrição
Quarantine email	Armazena todos os emails infectados detectados pelo mecanismo de verificação de vírus selecionado no armazenamento de quarentena. Em seguida, você pode analisar (aprovar/excluir) todos os emails em quarentena. Para obter mais informações, consulte Quarentena (página 203).
Delete email	Exclui emails infectados.
Send a sanitized copy of the original email to recipient(s)	Escolha se deseja enviar uma cópia limpa do email bloqueado para os destinatários.

7. O GFI MailEssentials pode enviar notificações por email quando um email acionar esse filtro. Para ativar esse recurso, selecione uma das seguintes opções:

Opção	Descrição
Notify administrator	Notifique o administrador sempre que esse mecanismo bloquear uma mensagem de email. Para obter mais informações, consulte Endereço de email do administrador (página 240).
Notify local user	Notifique os destinatários locais de email sobre o email bloqueado.

8. Para registrar a atividade deste mecanismo em um arquivo de registro, selecione **Log occurrence to this file**. Na caixa de texto, especifique o caminho e o nome do arquivo para um local personalizado no disco onde armazenar o arquivo de registro. Por padrão, os arquivos de registro são armazenados em:

```
<GFI MailEssentials installation path>\GFI\MailEssentials\EmailSecurity\Logs\<Nome do mecanismo>.log
```



Screenshot 51: Guia de atualização do mecanismo

9. Na guia **Updates**, selecione **Automatically check for updates** para ativar a atualização automática do mecanismo selecionado.

10. Na lista **Downloading option**, selecione uma das seguintes opções:

Opção	Descrição
Only check for updates	Selecione esta opção se você deseja que o GFI MailEssentials apenas verifique e notifique o administrador quando atualizações estiverem disponíveis para esse mecanismo. Esta opção NÃO fará o download das atualizações disponíveis automaticamente.
Check for updates and download	Selecione esta opção se você deseja que o GFI MailEssentials verifique e faça o download automaticamente das atualizações disponíveis para este mecanismo.

11. Especifique a frequência com que você deseja que o GFI MailEssentials verifique/faça o download das atualizações para este mecanismo, especificando um valor de intervalo em horas.

12. Na área **Update options**, selecione **Enable email notifications upon successful updates** para enviar uma notificação por email ao administrador quando a atualização do mecanismo for concluída.

> **OBS.**
> Uma notificação por email será enviada quando uma atualização falhar.

13. Para verificar e baixar as atualizações imediatamente, clique em **Download updates**.

14. Clique em **Apply**.

5.2 Proteção de armazenamento de informações

Quando o GFI MailEssentials estiver instalado na máquina do servidor Microsoft® Exchange, o Information Store Protection permite que você use os Virus Scanning Engines para fazer a verificação de vírus no Microsoft® Exchange Information Store.

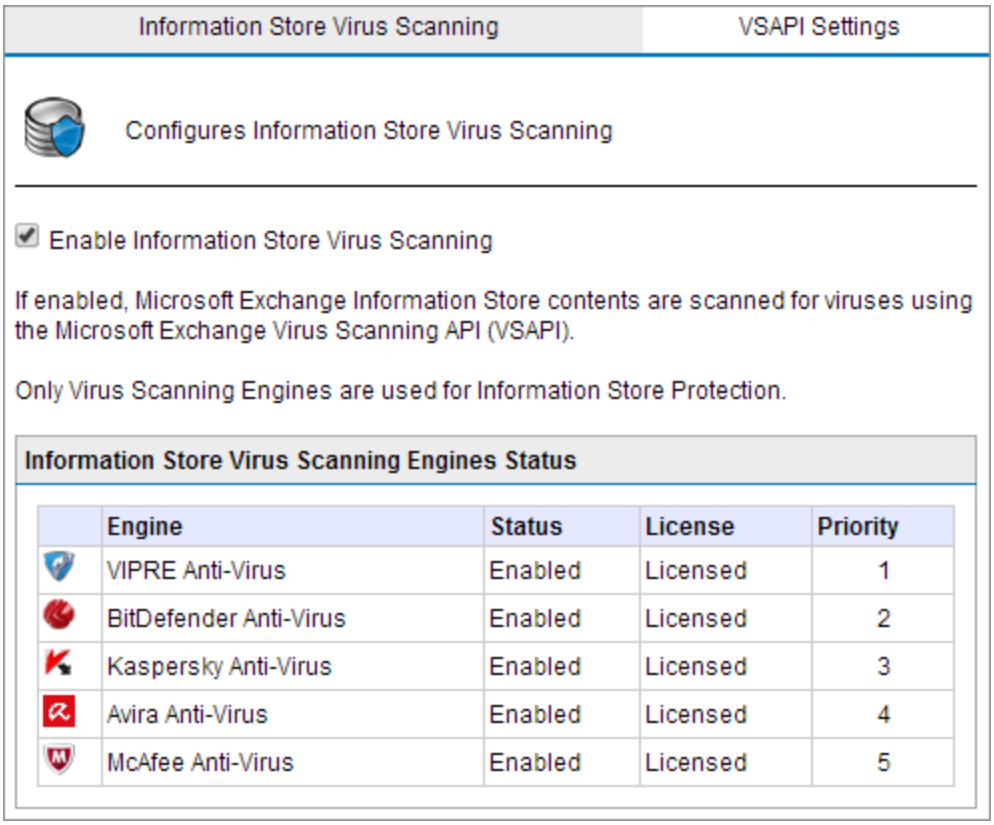
> **OBS.**
> Quando o GFI MailEssentials estiver instalado em uma máquina com o Microsoft®Exchange Server 2007/2010, o recurso Information Store Protection só estará disponível quando as funções de servidor Caixa de Correio e Transporte de Hub estiverem instaladas.

> **OBS.**
> O Information Store Protection (VSAPI) não é compatível com o Microsoft® Exchange Server 2013 porque o VSAPI foi removido do Microsoft® Exchange Server 2013.

Esta seção mostrará como habilitar o recurso Information Store Scanning e selecionar o método usado pela VSAPI (API de Verificação de Vírus).

5.2.1 Verificação do armazenamento de informações

1. Acesse **Email Security > Information Store Protection**.



Screenshot 52: Nó de proteção do armazenamento de informações

2. Na guia **Information Store Virus Scanning**, selecione **Enable Information Store Virus Scanning**.

3. Clique em **Apply**.

O status dos mecanismos de verificação de vírus usados para verificar o armazenamento de informações é exibido na tabela.

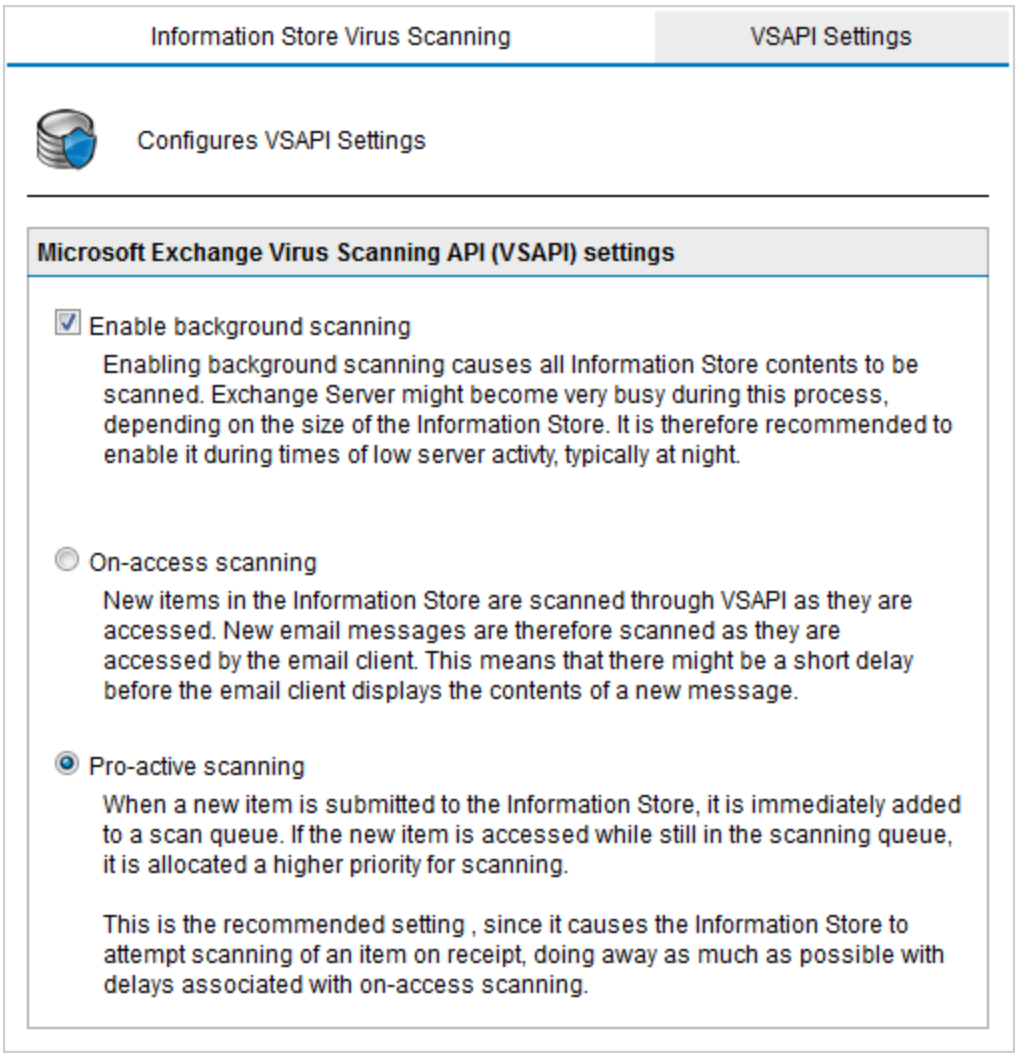
Você também pode desabilitar um determinado mecanismo antivírus em Information Store Scanning. Acesse a página Virus Scanning Engines, selecione o mecanismo antivírus e desabilite **Scan Internal and Information Store Items**.

5.2.2 Configurações do VSAPI

O método usado pelo GFI MailEssentials para acessar emails e anexos no Microsoft® Exchange Information Store é VSAPI (API de Verificação de Vírus).GFI MailEssentials permite que você especifique o método a usar para verificar o armazenamento de informações.

1. Acesse **Email Security > Information Store Protection**.

2. Selecione a guia **VSAPI Settings**



Screenshot 53: Configurações do VSAPI

3. (Opcional) Selecione **Enable background scanning** para executar a Information Store Scanning em segundo plano.

AVISO
A verificação segundo plano faz com que todos os dados do armazenamento de informações sejam examinados. Isso pode resultar em uma alta carga de processamento no Microsoft® Exchange Server de acordo com a quantidade de itens armazenados no armazenamento de informações. Recomenda-se habilitar esta opção somente durante períodos de pouca atividade do servidor, como durante a noite.

4. Selecione um método de verificação VSAPI:

Método de verificação	Descrição
Verificação durante o acesso	Novos itens no armazenamento de informações são examinados assim que são acessados pelo cliente de email. Essa opção gera um pequeno atraso antes de o cliente de email exibir o conteúdo de uma nova mensagem.

Método de verificação	Descrição
Verificação proativa	Novos itens adicionados ao armazenamento de informações são adicionados a uma fila para verificação. Esta é a opção padrão e o modo de operação recomendado, pois, em geral, o atraso associado com a verificação ao acessar é evitado. **OBS.** Caso um cliente de email tente acessar um item que ainda está na fila, será alocada uma maior prioridade para a verificação, para que ele seja examinado imediatamente.

5. Clique em **Apply**.

5.3 Verificador de Cavalo de Troia e executáveis

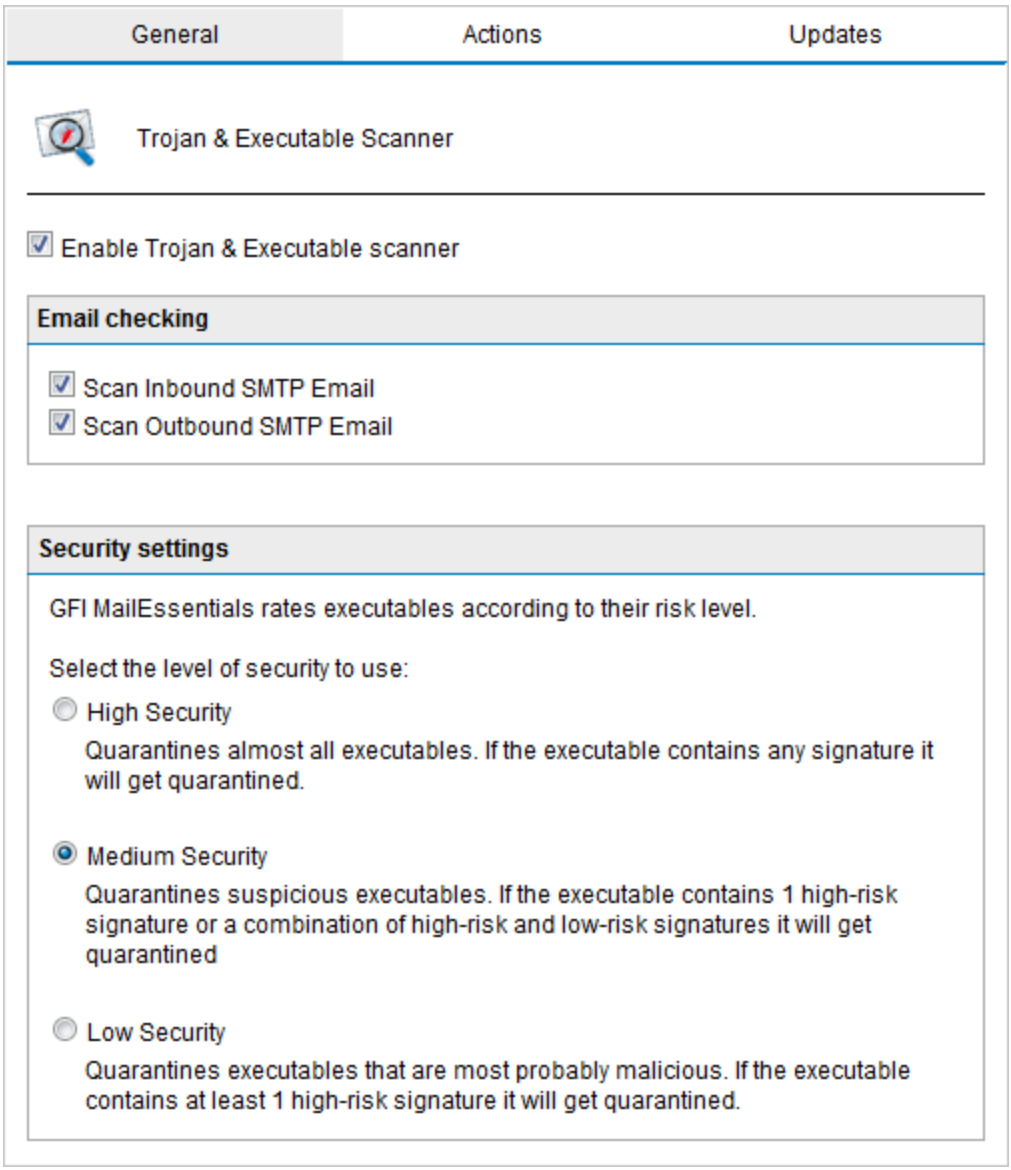
O Verificador de Cavalo de Troia e executáveis analisa e determina a função de arquivos executáveis anexados a emails. O mecanismo de verificação pode colocar posteriormente em quarentena quaisquer atividades executáveis que realizam atividades suspeitas (como Cavalos de Troia).

Como funciona o Verificador de Cavalo de Troia e executáveis?

O GFI MailEssentials classifica o nível de risco de um arquivo executável descompilando o executável e detectando em tempo real o que ele pode fazer. Subsequentemente, ele compara os recursos do executável a um banco de dados de ações mal-intencionadas e classifica o nível de risco do arquivo. Com o Verificador de Cavalo de Troia e executáveis, você pode detectar e bloquear Cavalos de Troia potencialmente perigosos, desconhecidos ou pontuais antes que eles comprometam sua rede.

5.3.1 Configurar o Verificador de Cavalo de Troia e executáveis

1. Acesse **Email Security > Trojan & Executable Scanner**.



Screenshot 54: Verificador de Cavalo de Troia e Executáveis: Guia Geral

2. Selecione **Enable Trojan & Executable Scanner** para ativar este filtro.

3. Na área **Email checking**, especifique os emails nos quais verificar a existência de Cavalos de Troia e outros códigos executáveis mal-intencionados, selecionando:

Opção	Descrição
Check inbound emails	Verifica emails de entrada em busca de Cavalos de Troia e arquivos executáveis mal-intencionados.
Check outbound emails	Verifica emails de saída em busca de Cavalos de Troia e arquivos executáveis mal-intencionados.

4. Na área **Configurações de segurança**, escolha o nível de segurança:

Nível de segurança	Descrição
High Security	Bloqueia todos os executáveis que contenham qualquer assinatura mal-intencionada conhecida

Nível de segurança	Descrição
Medium Security	Bloqueia executáveis suspeitos. Emails são bloqueados se um executável contiver uma assinatura de alto risco ou uma combinação de assinaturas de alto e baixo risco.
Low Security	Bloqueia somente os executáveis mal-intencionados. Emails são bloqueados se um executável contiver pelo menos uma assinatura de alto risco.

5. Na guia **Actions**, configure as ações que você deseja que o GFI MailEssentials execute nos emails que contenham um executável mal-intencionado.

> **OBS.**
> Emails bloqueados pelo Verificador de Cavalo de Troia e executáveis são sempre colocados em quarentena.

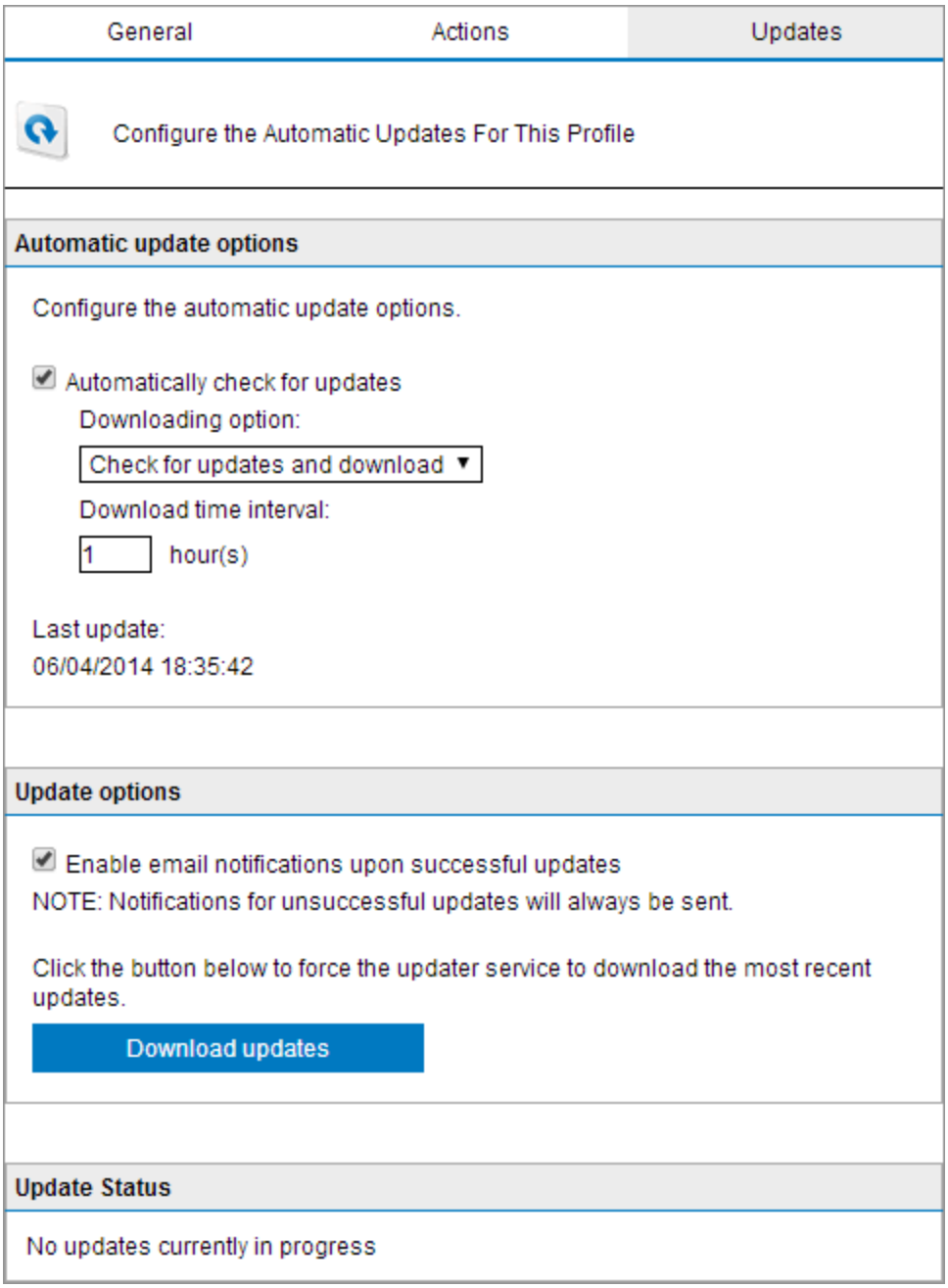
> **OBS.**
> Quando o GFI MailEssentials estiver instalado na mesma máquina do Microsoft® Exchange 2003, o GFI MailEssentials pode não ser capaz de bloquear emails de saída. Em vez disso, ele substitui o conteúdo bloqueado por um relatório de ameaça.

6. O GFI MailEssentials pode enviar notificações por email quando um email acionar esse filtro. Para ativar esse recurso, selecione uma das seguintes opções:

Opção	Descrição
Notify administrator	Notifique o administrador sempre que esse mecanismo bloquear uma mensagem de email. Para obter mais informações, consulte Endereço de email do administrador (página 240).
Notify local user	Notifique os destinatários locais de email sobre o email bloqueado.

7. Para registrar a atividade deste mecanismo em um arquivo de registro, selecione **Log occurrence to this file**. Na caixa de texto, especifique o caminho e o nome do arquivo para um local personalizado no disco onde armazenar o arquivo de registro. Por padrão, os arquivos de registro são armazenados em:

```
<GFI MailEssentials installation path>\GFI\MailEssentials\EmailSecurity\Logs\<Nome do mecanismo>.log
```



Screenshot 55: Guia de atualização do mecanismo

8. Na guia **Updates**, selecione **Automatically check for updates** para ativar a atualização automática do mecanismo selecionado.

9. Na lista **Downloading option**, selecione uma das seguintes opções:

Opção	Descrição
Only check for updates	Selecione esta opção se você deseja que o GFI MailEssentials apenas verifique e notifique o administrador quando atualizações estiverem disponíveis para esse mecanismo. Esta opção NÃO fará o download das atualizações disponíveis automaticamente.
Check for updates and download	Selecione esta opção se você deseja que o GFI MailEssentials verifique e faça o download automaticamente das atualizações disponíveis para este mecanismo.

10. Especifique a frequência com que você deseja que o GFI MailEssentials verifique/faça o download das atualizações para este mecanismo, especificando um valor de intervalo em horas.

11. Na área **Update options**, selecione **Enable email notifications upon successful updates** para enviar uma notificação por email ao administrador quando a atualização do mecanismo for concluída.

> **OBS.**
> Uma notificação por email será enviada quando uma atualização falhar.

12. Para verificar e baixar as atualizações imediatamente, clique em **Download updates**.

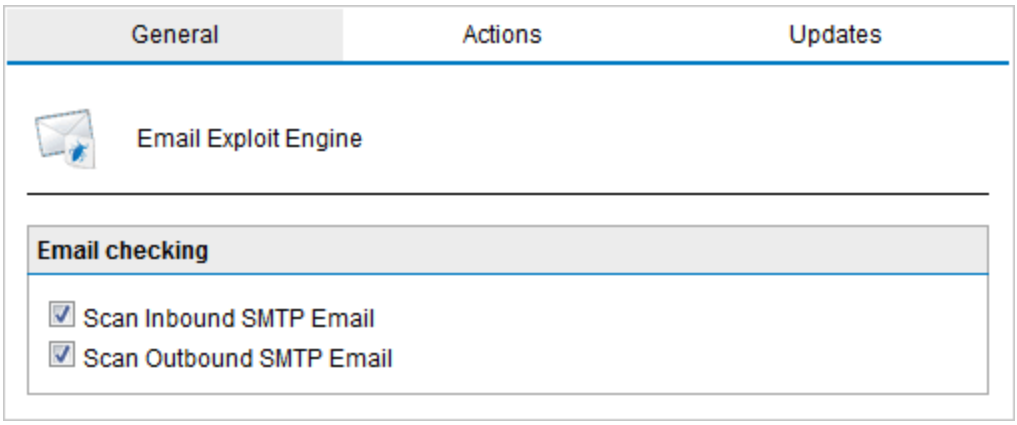
13. Clique em **Apply**.

5.4 Mecanismo de exploração de email

O Mecanismo de exploração de email bloqueia explorações incorporadas em um email que podem ser executadas na máquina do destinatário quando o usuário receber ou abrir o email. Uma exploração utiliza vulnerabilidades conhecidas em aplicativos ou sistemas operacionais para comprometer a segurança de um sistema. Por exemplo, executar um programa ou comando ou instalar um backdoor.

5.4.1 Configurar o mecanismo de exploração de email

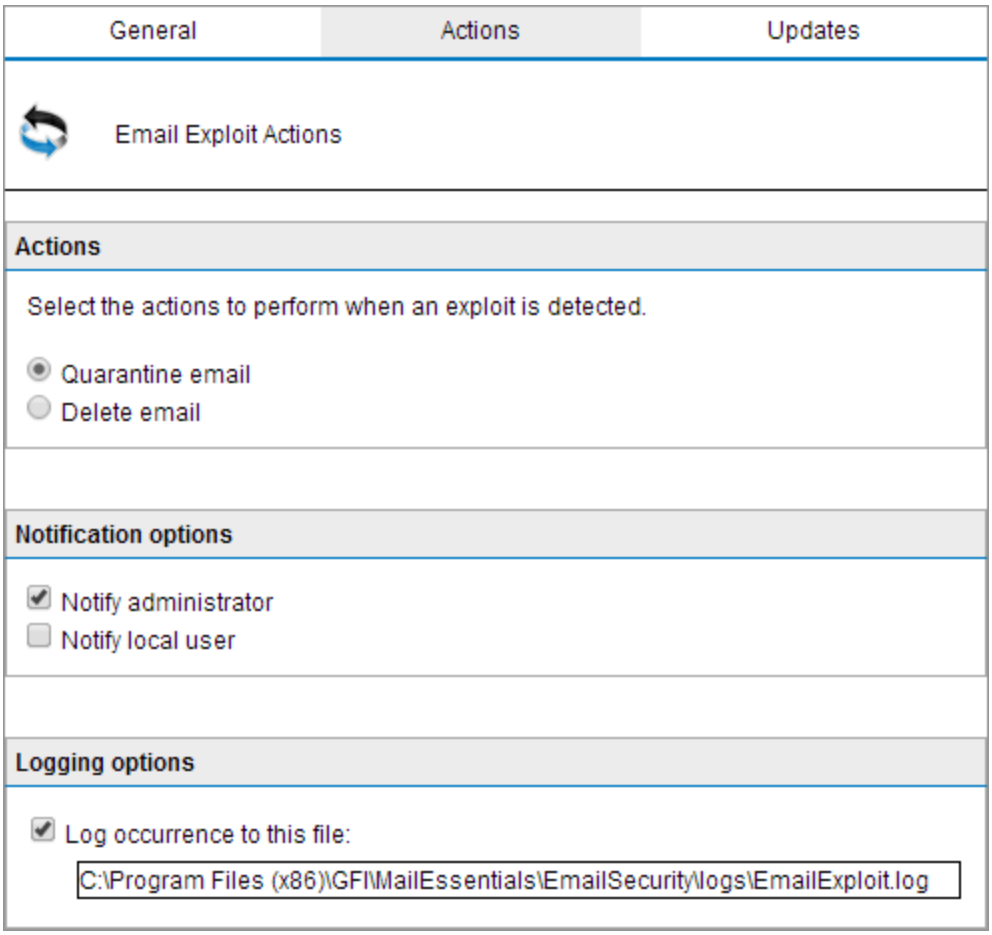
1. Acesse **Email Security > Email Exploit Engine**.



Screenshot 56: Configuração da exploração de email

2. Na guia **General**, selecione se deseja fazer a verificação de emails de entrada e/ou de saída.

Opção	Descrição
Scan inbound SMTP emails	Selecione esta opção para verificar emails de entrada
Scan outbound SMTP emails	Selecione esta opção para verificar emails de saída



Screenshot 57: Ações de exploração de email

3. Na guia **Actions**, escolha a ação a ser executada quando um email for bloqueado:

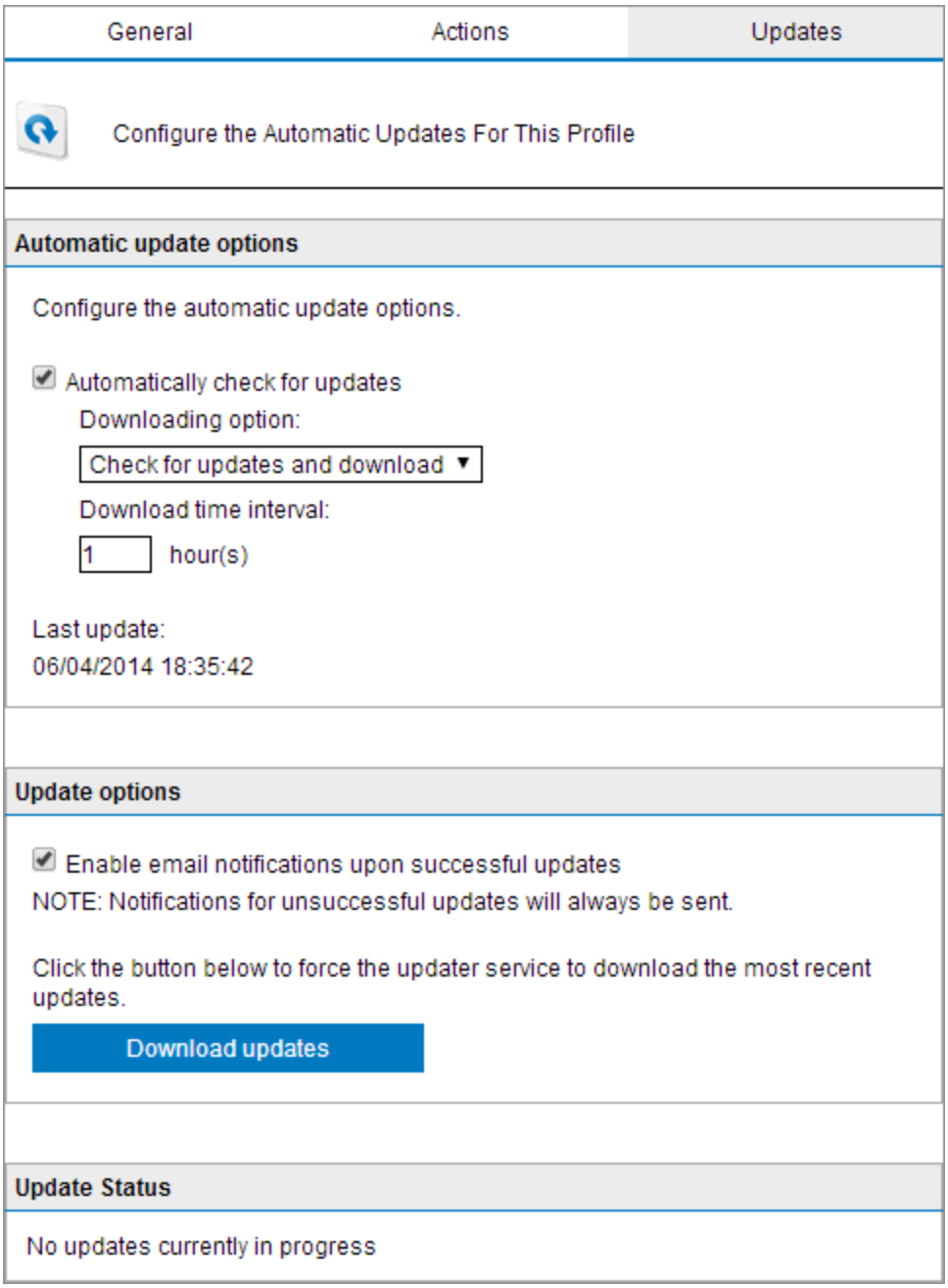
Ação	Descrição
Quarantine item	Armazena todos os emails infectados detectados pelo mecanismo de exploração de emails no armazenamento da quarentena. Em seguida, você pode analisar (aprovar/excluir) todos os emails em quarentena. Para obter mais informações, consulte Trabalhar com emails em quarentena (página 211).
Delete item	Exclui emails infectados.

4. O GFI MailEssentials pode enviar notificações por email quando um email acionar esse filtro. Para ativar esse recurso, selecione uma das seguintes opções:

Opção	Descrição
Notify administrator	Notifique o administrador sempre que esse mecanismo bloquear uma mensagem de email. Para obter mais informações, consulte Endereço de email do administrador (página 240).
Notify local user	Notifique os destinatários locais de email sobre o email bloqueado.

5. Para registrar a atividade deste mecanismo em um arquivo de registro, selecione **Log occurrence to this file**. Na caixa de texto, especifique o caminho e o nome do arquivo para um local personalizado no disco onde armazenar o arquivo de registro. Por padrão, os arquivos de registro são armazenados em:

```
<GFI MailEssentials installation path>\GFI\MailEssentials\EmailSecurity\Logs\<Nome do mecanismo>.log
```



Screenshot 58: Guia de atualização do mecanismo

6. Na guia **Updates**, selecione **Automatically check for updates** para ativar a atualização automática do mecanismo selecionado.

7. Na lista **Downloading option**, selecione uma das seguintes opções:

Opção	Descrição
Only check for updates	Selecione esta opção se você deseja que o GFI MailEssentials apenas verifique e notifique o administrador quando atualizações estiverem disponíveis para esse mecanismo. Esta opção NÃO fará o download das atualizações disponíveis automaticamente.
Check for updates and download	Selecione esta opção se você deseja que o GFI MailEssentials verifique e faça o download automaticamente das atualizações disponíveis para este mecanismo.

8. Especifique a frequência com que você deseja que o GFI MailEssentials verifique/faça o download das atualizações para este mecanismo, especificando um valor de intervalo em horas.

9. Na área **Update options**, selecione **Enable email notifications upon successful updates** para enviar uma notificação por email ao administrador quando a atualização do mecanismo for concluída.

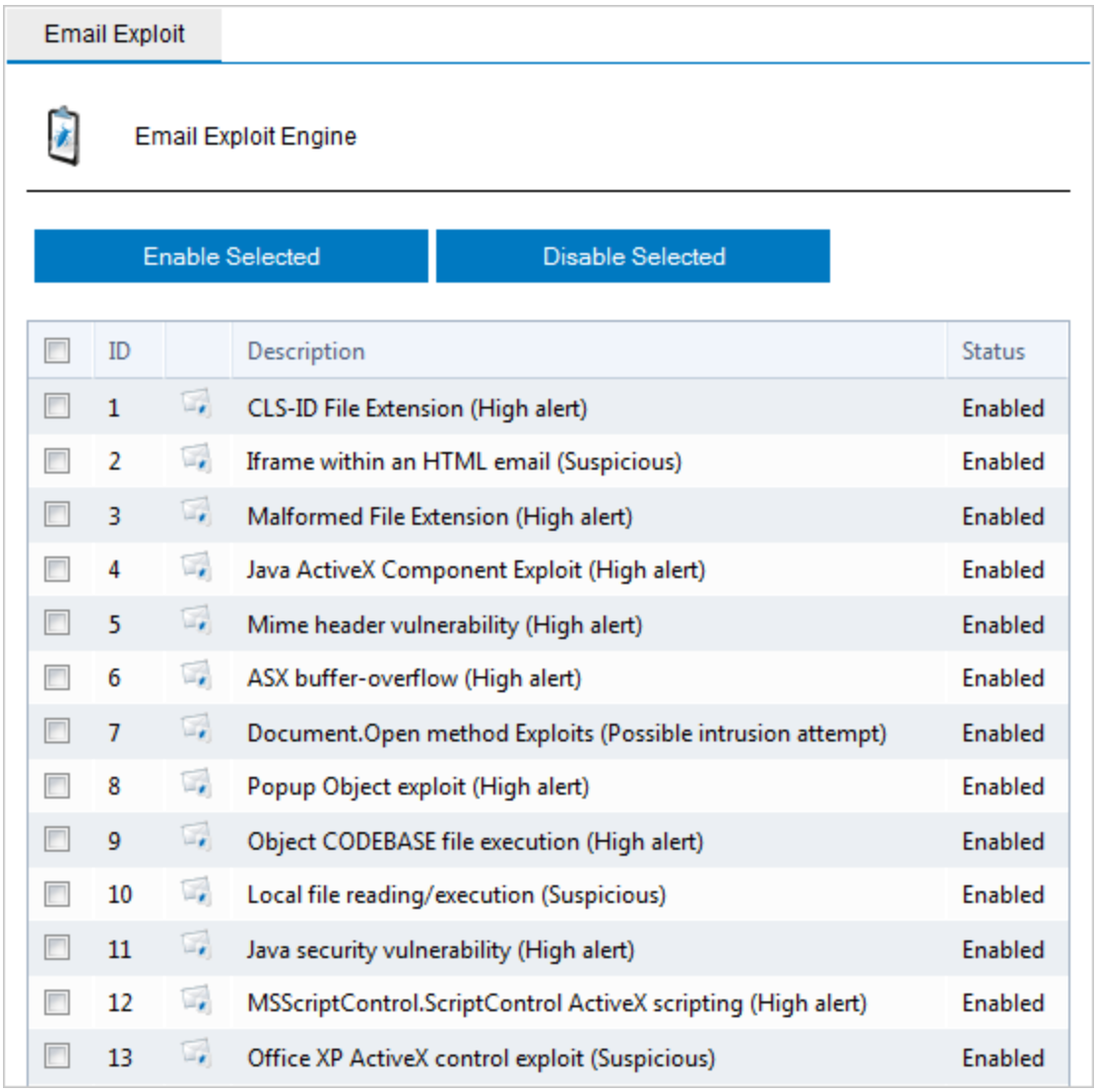
> **OBS.**
> Uma notificação por email será enviada quando uma atualização falhar.

10. Para verificar e baixar as atualizações imediatamente, clique em **Download updates**.

11. Clique em **Apply**.

5.4.2 Habilitar/desabilitar explorações de email

1. Acesse **Email Security > Email Exploit Engine > Exploit List**



Screenshot 59: Lista de exploração de email

2. Marque a caixa de seleção das explorações a serem habilitadas ou desabilitadas.

3. Clique em **Enable Selected** ou **Disable Selected**.

5.5 HTML Sanitizer

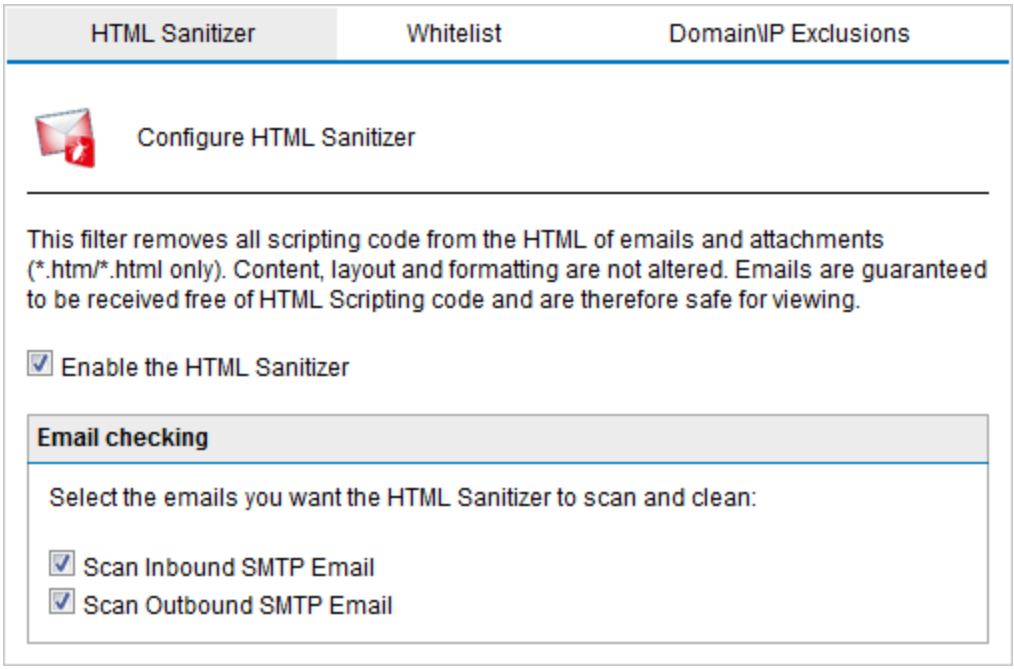
O HTML Sanitizer verifica e remove código de scripts no corpo do email e de anexos. Ele verifica:

» o corpo das mensagens de email que têm o tipo MIME definido como "text/html"

» todos os anexos do tipo **.htm** ou **.html**.

5.5.1 Como configurar o Recuperador de HTML

1. Acesse **Email Security > HTML Sanitizer**.



Screenshot 60: Página de configuração do HTML Sanitizer

2. Para habilitar o HTML Sanitizer, selecione **Enable the HTML Sanitizer**.

3. Selecionar a direção dos emails:

Opção	Descrição
Scan inbound SMTP emails	Verificar e sanitizar scripts HTML de todos os emails de entrada.
Scan outbound SMTP emails	Verificar e sanitizar scripts HTML de todos os emails de saída.

4. Clique em **Apply**.

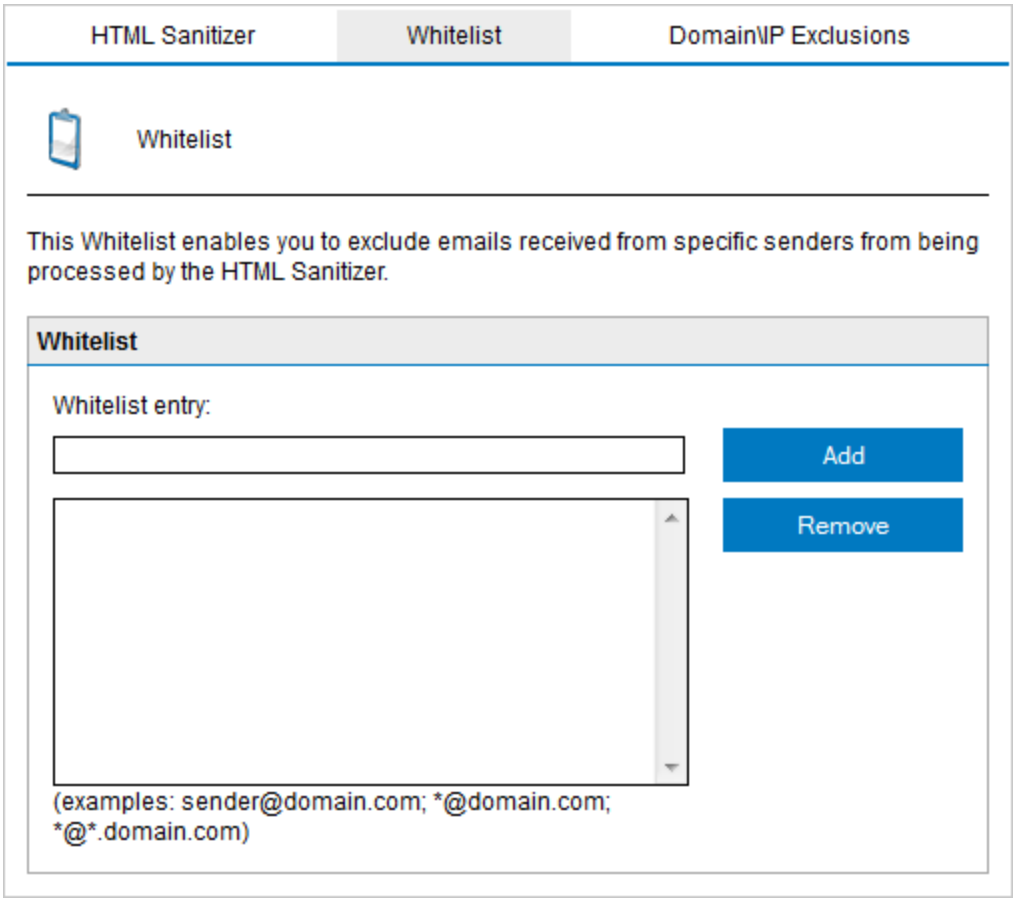
5.5.2 Lista de permissão do HTML Sanitizer

A Lista de permissão do HTML Sanitizer pode ser configurada para excluir mensagens recebidas de remetentes específicos.

OBS.
Para excluir domínios ou endereços IP específicos, use o recurso HTML Sanitizer Domain\IP Exclusions. Para obter mais informações, consulte HTML Sanitizer (página 105).

Para gerenciar remetentes na Lista de permissão do HTML Sanitizer:

1. Acesse **Email Security > HTML Sanitizer** e selecione a guia **Whitelist**.



Screenshot 61: Página da Lista de permissão do HTML Sanitizer

2. Em **Whitelist entry**, digite um endereço de email, um domínio de email (por exemplo, *@dominio.com) ou um subdomínio de email (por exemplo, *@*.dominio.com) e clique em **Add**.

OBS.
Para remover uma entrada da Lista de permissão do HTML Sanitizer, selecione uma entrada e clique em **Remove**.

3. Clique em **Apply**.

5.5.3 HTML Sanitizer Domain\IP Exclusions

O recurso HTML Sanitizer Domain\IP Exclusions permite que os administradores especifiquem os endereços IP ou domínios a serem excluídos do HTML Sanitizer. Esse recurso não usará simplesmente uma lista de endereços IP. Ele também pode oferecer suporte a endereços de domínio, que são resolvidos no tempo de execução, para que todos os endereços IP do domínio em questão sejam obtidos. Isso é feito de duas maneiras:

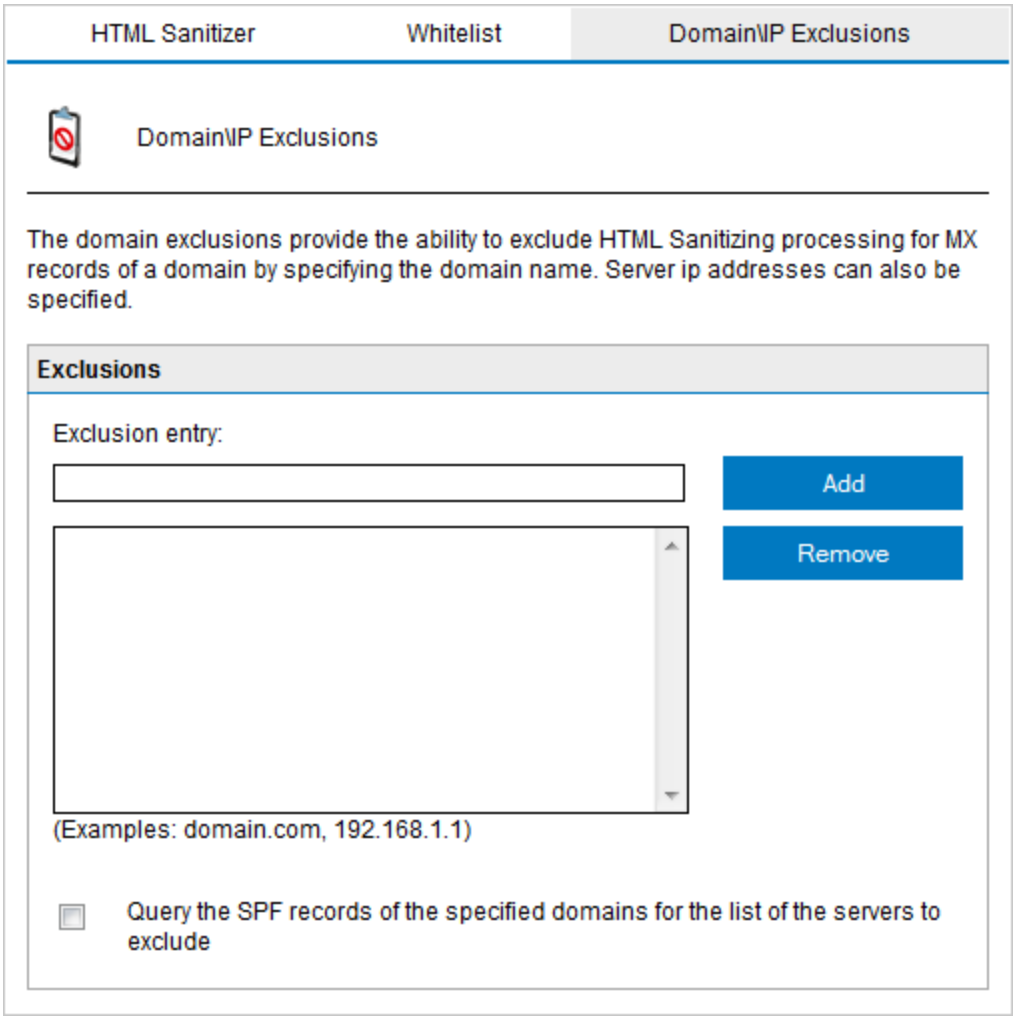
1. Por padrão, o recurso consulta os registros MX do domínio que estão sendo processados.

2. Como alternativa, você pode optar por consultar o registro SPF do domínio. Se o domínio não tiver um registro SPF, a parte SPF será ignorada e apenas os registros MX serão usados.

Se o endereço IP do qual o email foi originado (o que enviou o email para o servidor de perímetro) for um IP listado na guia Domains\IPs exclusions ou resolvido de um domínio na mesma lista e, o email não será processado pelo HTML Sanitizer. Esse é um tipo de lista de permissão de IPs, mas com o benefício adicional de especificar domínios e resolver os registros MX de domínios MX e (opcionalmente) o registro SPF para obter os endereços IP.

Para gerenciar domínios/exclusões de IP na Lista de permissão do HTML Sanitizer:

1. Acesse **Email Security > HTML Sanitizer** e selecione a guia **Domains\IP exclusions**.



Screenshot 62: Exclusões de Domínio\IP

2. Digite o domínio ou o endereço IP que você deseja excluir e clique em **Add**.

> **OBS.**
> Para remover uma entrada de HTML Sanitizer Domain\IP Exclusions, selecione uma entrada e clique em **Remove**.

3. Como alternativa, selecione a **Query the SPF records of the specified domains for the list of the servers to exclude**.

4. Clique em **Apply**.

6 Anti-spam

Os filtros anti-spam fornecidos com o GFI MailEssentials ajudam a detectar e bloquear emails indesejados (spam).

Tópicos deste capítulo:

6.1 Filtros anti-spam

O GFI MailEssentials utiliza vários filtros de verificação para identificar emails com spam:

FILTRO	DESCRIÇÃO	HABILITADO POR PADRÃO
SpamRazer	Um mecanismo anti-spam que determina se um email é spam usando a reputação do email, mensagem da "impressão digital" e análise de conteúdo.	Sim
Anti-phishing	Bloqueia emails que contêm links no corpo da mensagem que direcionam para sites de phishing conhecidos ou se eles contiverem palavras-chave de phishing conhecidas.	Sim
Coleta de diretório	Ataques do tipo Directory harvesting ocorrem quando os remetentes de spam tentam adivinhar endereços de email anexando nomes dos usuários conhecidos a seu domínio. A maioria dos endereços de email é inexistente.	Sim (somente se oGFI MailEssentials estiver instalado em um ambiente de Active Directory)
Lista de bloqueio de emails	A Lista de bloqueio de email é um banco de dados personalizado de endereços de email e domínios do qual você não deseja receber emails.	Sim
Lista de bloqueio de IP	A Lista de bloqueio de IP é um banco de dados personalizado de endereços de email e domínios do qual você não deseja receber emails.	Não
Lista de bloqueio DNS IP	A Lista de bloqueio de DNS de IP verifica o endereço IP do servidor de email de envio em relação a uma lista de servidores de email conhecidos por serem remetentes de spam.	Sim
Lista de bloqueio DNS URI	Bloqueia emails que contêm links para domínios listados em lista de bloqueio de URI de spam públicas.	Sim

FILTRO	DESCRIÇÃO	HABILITADO POR PADRÃO
Estrutura de políticas do remetente	Este filtro usa registros SPF para bloquear emails enviados de endereços IP falsificados, identificando se o endereço IP do remetente é autorizado.	Não
Anti-spoofing	Verifica emails recebidos com um endereço de email do remetente originado de seu próprio domínio em relação a uma lista de endereços IP do GFI MailEssentials. Se o endereço IP do remetente não estiver na lista de endereços IP do servidor do domínio, o email será bloqueado.	Não
Lista de exclusão temporária	O filtro Lista de exclusão temporária bloqueia temporariamente a entrada de emails recebidos de remetentes desconhecidos. Sistemas de email legítimos normalmente tentam enviar o email após alguns minutos. Os remetentes de spam simplesmente ignoram essas mensagens de erro.	Não
Detecção de idioma	Determina o idioma do texto do corpo do email e é configurável para bloquear certos idiomas.	Não
Verificação de cabeçalho	O filtro Verificação de cabeçalho analisa o cabeçalho de email para identificar emails com spam.	Não
Verificação de palavras-chave de spam	Este filtro permite a identificação do spam baseada em palavras-chave no email que está sendo recebido.	Não
Análise bayesiana	Um filtro anti-spam que pode ser treinado para determinar com precisão se um email é spam com base na experiência.	Não
Lista de permissão	A lista de permissão contém listas de critérios que identificam um email legítimo. Emails que correspondam a esses critérios não são examinados pelos filtros anti-spam e são sempre entregues ao destinatário.	Sim
Novos remetentes	O filtro Novos remetentes identifica emails que foram recebidos de remetentes para os quais emails nunca foram enviados.	Não

6.1.1 SpamRazer

Um mecanismo anti-spam que determina se um email é spam usando a reputação do email, mensagem da "impressão digital" e análise de conteúdo. O SpamRazer é o principal mecanismo anti-spam e é habilitado por padrão na instalação. Atualizações frequentes são lançadas para o SpamRazer que diminuir ainda mais o tempo de reação a novas tendências de spam.

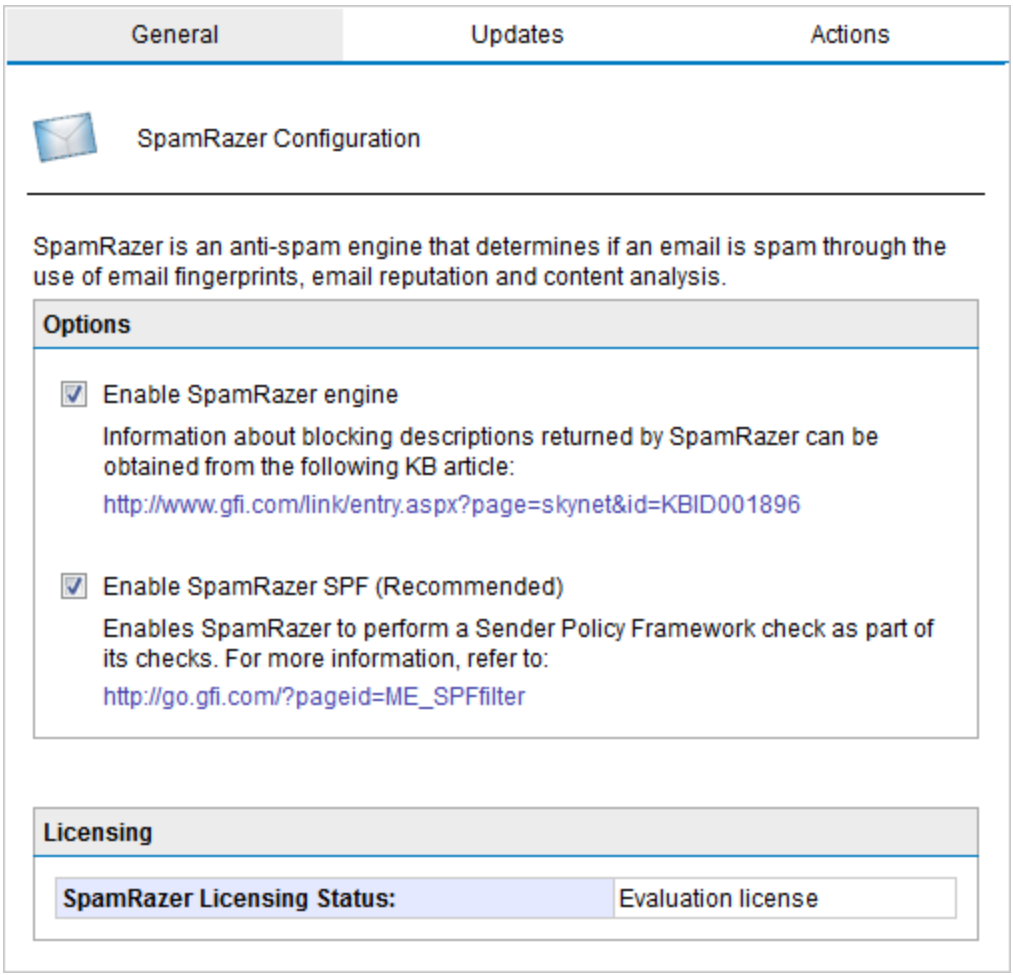
O SpamRazer também inclui a filtragem Estrutura de políticas do remetente, que detecta remetentes forjados. É recomendável que os remetentes publiquem o servidor de email em um registro SPF. Para obter mais informações sobre o SPF e como funciona, acesse o site da Estrutura de políticas do remetente: http://www.openspf.org.

Este filtro também bloqueia spam NDR. Para obter mais informações sobre spam NDR, consulte http://go.gfi.com/?pageid=ME_NDRSpam

Configurar o SpamRazer

> **OBS.**
>
> 1. **NÃO** é recomendado desabilitar o SpamRazer.
> 2. O GFI MailEssentials faz o download de atualizações do SpamRazer de: ***.mailshell.net**

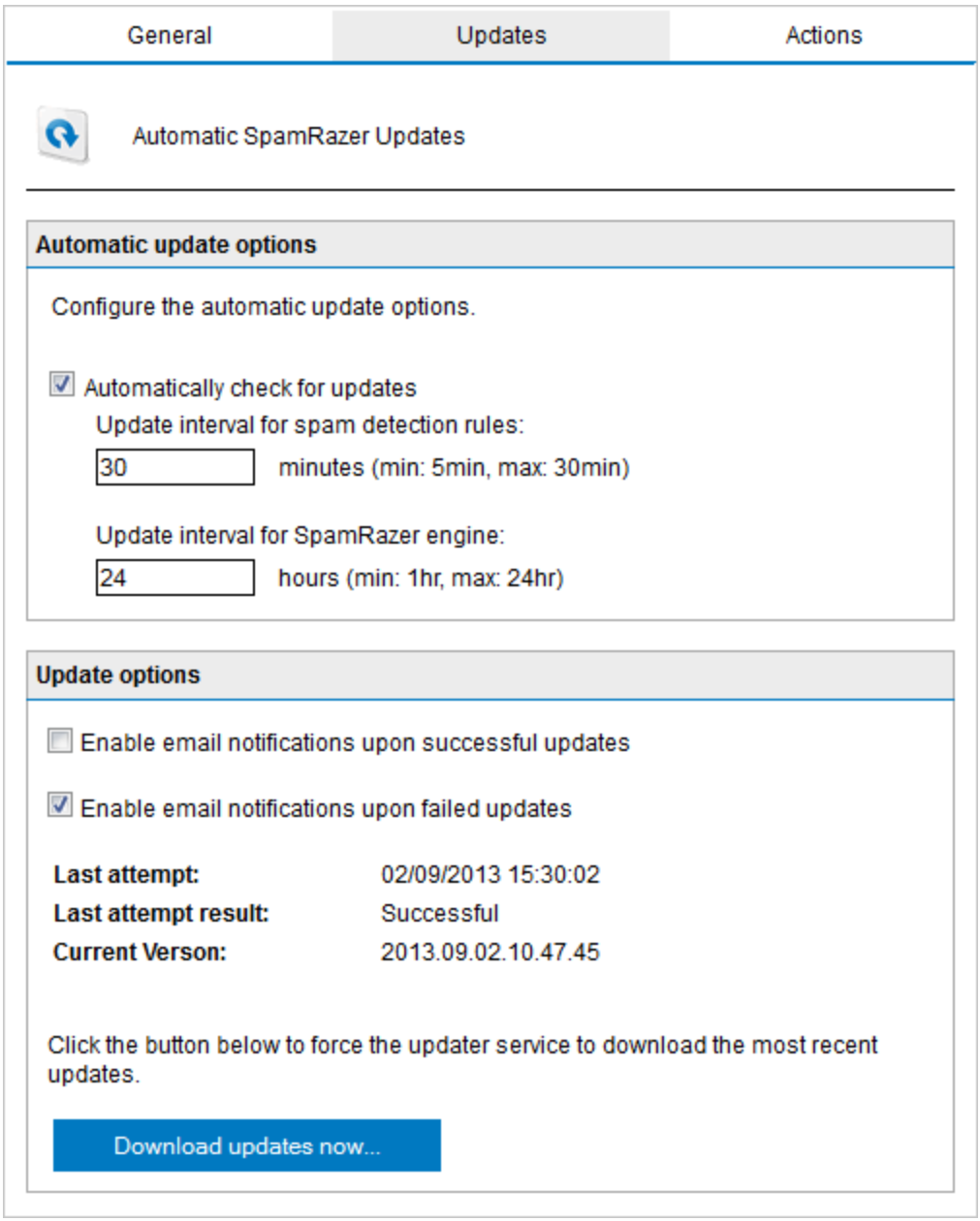
1. Acesse **Anti-Spam > Anti-Spam Filters > SpamRazer**.



Screenshot 63: Propriedades do SpamRazer

2. Na guia **General**, execute uma das seguintes ações:

Opção	Descrição
Enable SpamRazer engine	Habilitar ou desabilitar SpamRazer.
Enable SpamRazer SPF (Recommended)	Habilitar ou desabilitar a Estrutura de políticas do remetente. É recomendado habilitar esta opção e executar este filtro após o filtro Lista de permissão de email.



Screenshot 64: Guia Atualizações SpamRazer

3. Na guia **Updates**, execute uma das seguintes ações:

Opção	Descrição
Automatically check for updates	Configurar GFI MailEssentials para verificar e fazer download automático de quaisquer atualizações SpamRazer. Especificar o intervalo de tempo em minutos para a verificação de atualizações das regras de detecção de spam e do mecanismo SpamRazer. **OBS.** É recomendável habilitar esta opção para que o SpamRazer seja mais eficiente na detecção das tendências mais recentes de spam.
Enable email notifications upon successful updates	Selecione esta opção se quiser ser informado por email quando novas atualizações forem obtidas por download.

Opção	Descrição
Enable email notifications upon failed updates	Selecione esta opção se quiser ser informado por email quando ocorrer falha em um download ou na instalação.
Download updates now...	Clique para fazer o download das atualizações.

> **OBS.**
> Você pode fazer o download das atualizações usando um servidor proxy. Para obter mais informações, consulte Configurações de proxy (página 241).

4. Clique na guia **Actions** para selecionar as ações a serem executadas nas mensagens identificadas como spam. Para obter mais informações, consulte Ações de spam - O que fazer com emails de spam (página 148).

5. Clique em **Apply**.

6.1.2 Anti-phishing

Bloqueia emails que contêm links no corpo da mensagem que direcionam para sites de phishing conhecidos ou se eles contiverem palavras-chave de phishing conhecidas. Phishing é uma técnica de engenharia social baseado em email que tem como objetivo fazer com que usuários de emails divulguem informações pessoais a remetentes de spam. Um email de phishing é provavelmente criado para que seja semelhante a um email oficial de uma empresa respeitável, por exemplo, um banco. Os emails de phishing geralmente contêm instruções que exigem que os usuários reconfirmem informações confidenciais, como dados de acesso a serviços bancários on-line ou dados de cartão de crédito. Emails de phishing geralmente incluem um Uniform Resource Identifier (URI) de phishing que o usuário deverá seguir para inserir informações confidenciais em um site de phishing. O site acessado pelo URI de phishing pode ser uma réplica de um site oficial, mas, na verdade, é controlado por quem enviou os emails de phishing. Quando o usuário digita as informações confidenciais no site de phishing, os dados são coletados e usados, por exemplo, para retirar dinheiro de contas bancárias.

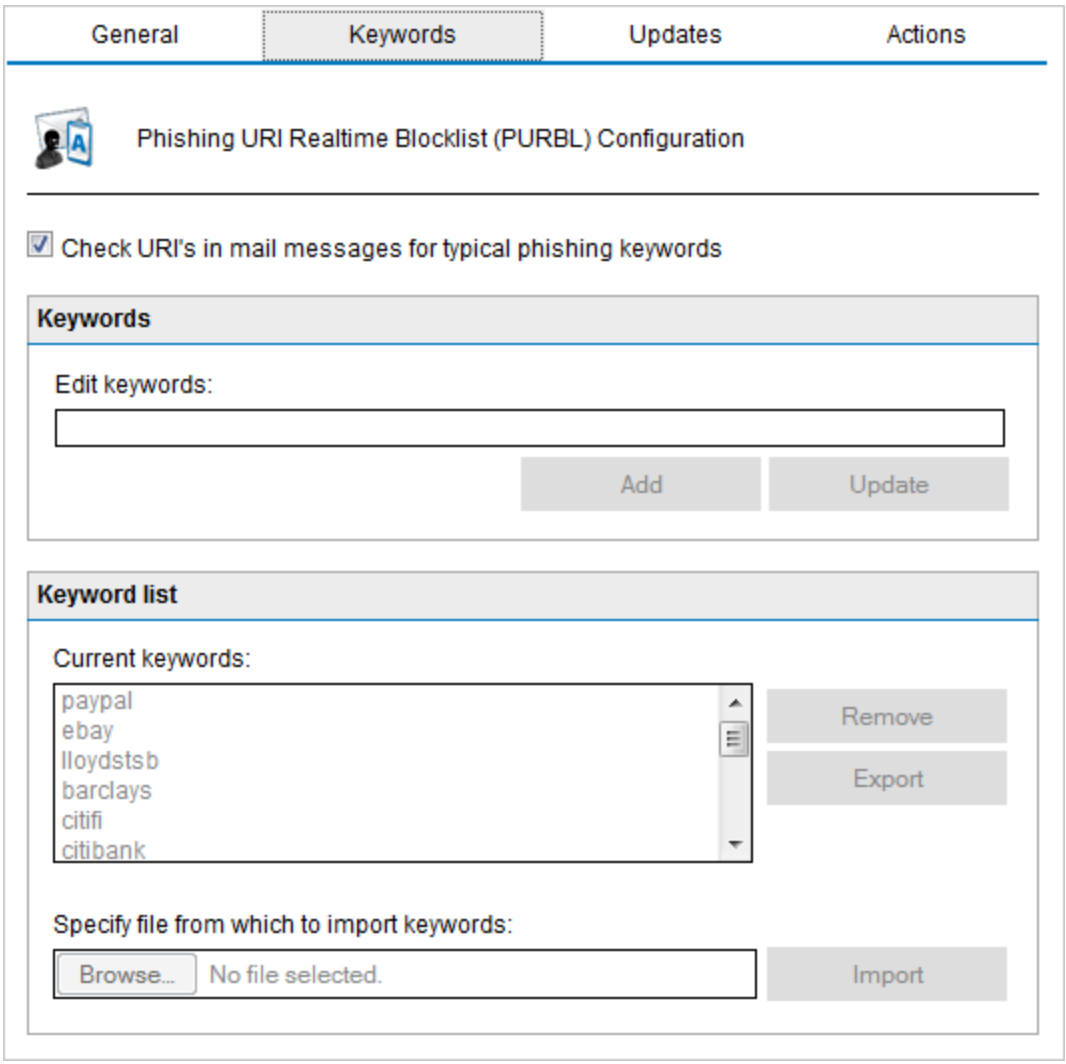
O filtro antiphishing detecta emails de phishing comparando URIs presentes no email com um banco de dados de URIs conhecido por ser utilizado em ataques de phishing. O phishing também procura palavras-chaves típicas de phishing nos URIs.

Por padrão, o filtro antiphishing é ativado na instalação.

Configurar o filtro antiphishing

> **OBS.**
> A desativação do filtro antiphishing **NÃO** é recomendada.

1. Acesse **Anti-Spam > Anti-Spam Filters > Anti-Phishing**.



Screenshot 65: Opções de filtros antiphishing

2. Na guia **General**, marque/desmarque **Check mail messages for URI's to known phishing sites** para habilitar/desabilitar o filtro antiphishing.

3. Na guia **Keywords**, selecione uma das seguintes opções:

Opção	Descrição
Check URI's in mail messages for typical phishing keywords	Habilitar/Desabilitar verificações de palavras-chave típicas de phishing
Add	Permite a adição de palavras-chave ao filtro antiphishing. Digite uma palavra-chave e clique em **Add** para adicionar uma palavra-chave ao filtro antiphishing
Update	Permite a atualização de palavras-chave selecionadas. Selecione uma palavra-chave na lista **Current Keywords**, faça alterações na palavra-chave no campo **Edit Keywords** e clique em **Update**.
Remove	Permite a remoção de palavras-chave selecionadas da lista. Selecione uma palavra-chave na lista **Current Keywords** e clique em **Remove**.
Export	Exporta a lista atual para um arquivo no formato XML.
Browse...	Permite a importação de uma lista de palavras-chave previamente exportada. Clique em **Browse**, selecione um arquivo de palavras-chave previamente exportado e clique em **Import**.

4. Na guia **Updates**, selecione uma das seguintes opções:

Opção	Descrição
Automatically check for updates	Configure o GFI MailEssentials para verificar automaticamente e fazer o download de atualizações do filtro antiphishing. Especifique o intervalo de tempo em minutos para a verificação de atualizações. **OBS.** É recomendável habilitar esta opção para que o filtro antiphishing seja mais eficiente na detecção das tendências mais recentes de phishing.
Enable email notifications upon successful updates	Marque/desmarque a caixa de texto para ser informado por email quando novas atualizações forem obtidas por download.
Enable email notifications upon failed updates	Marque/desmarque para ser informado quando ocorrer falha em um download ou em uma instalação.
Download updates now...	Clique para fazer imediatamente o download de atualizações do filtro antiphishing.

OBS.
Você pode fazer o download das atualizações usando um servidor proxy. Para obter mais informações, consulte Configurações de proxy (página 241).

5. Clique na guia **Actions** para selecionar as ações a serem executadas nas mensagens identificadas como spam. Para obter mais informações, consulte Ações de spam - O que fazer com emails de spam (página 148).

6. Clique em **Apply**.

6.1.3 Coleta de diretório

Ataques do tipo Directory harvesting ocorrem quando os remetentes de spam tentam adivinhar endereços de email anexando nomes dos usuários conhecidos a seu domínio. A maioria dos endereços de email é inexistente. Os remetentes de spam enviam emails para endereços de emails gerados aleatoriamente. Embora alguns endereços de email correspondam a usuários reais, a maioria dessas mensagens são inválidas e, consequentemente, lotam o servidor de email da vítima.

O GFI MailEssentials interrompe esses ataques bloqueando emails endereçados a usuários que não estejam no Active Directory ou no servidor de email das organizações.

O filtro Coleta de diretório pode ser configurado para ser executado quando a mensagem completa for recebida ou no nível do SMTP, isto é, os emails são filtrados enquanto estão sendo recebidos. A filtragem no nível do SMTP encerra a conexão do email e interrompe o download do email completo, economizando largura de banda e recursos de processamento. Nesse caso, a conexão foi encerrada imediatamente e os emails não precisam passar por nenhum outro filtro de spam.

Este filtro é ativado por padrão ao instalar o GFI MailEssentials em um ambiente do Active Directory.

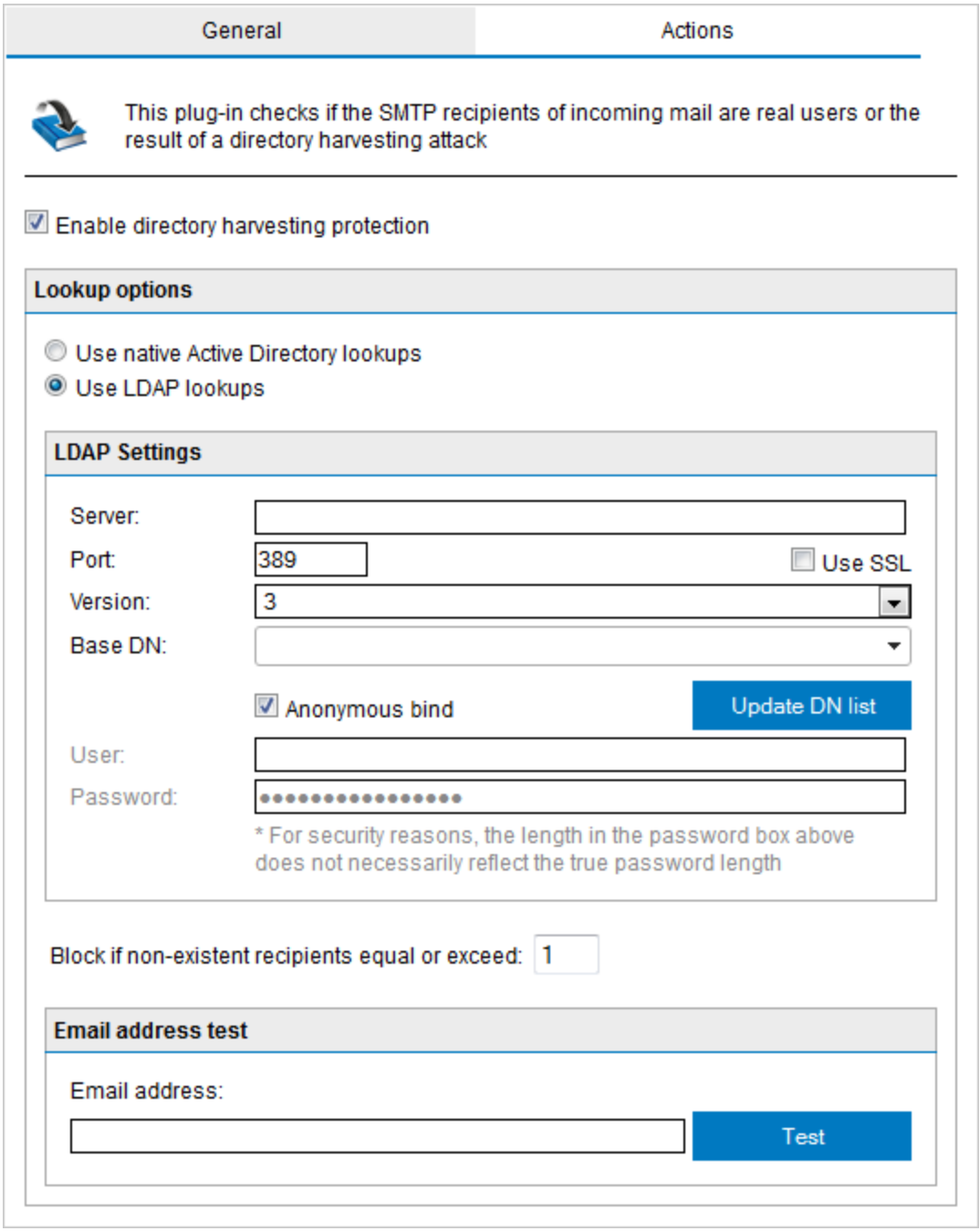
A Coleta de diretório é configurada em dois estágios da seguinte maneira:

Estágio 1 - Configurar as propriedades da Coleta de diretório

Estágio 2 - Selecionar se a Coleta de diretório deve ser executado durante a transmissão SMTP.

Estágio 1 - Configurar as propriedades da Coleta de diretório

1. Acesse **Anti-Spam > Anti-Spam Filters > Directory Harvesting.**



Screenshot 66: Página da Coleta de diretório

2. Habilite/desabilite a Coleta de diretório e selecione o método de pesquisa a ser usado:

Opção	Descrição
Enable directory harvesting protection	Habilite/desabilite a Coleta de diretório.

Opção	Descrição
Use native Active Directory lookups	Selecione a opção se o GFI MailEssentials estiver instalado no Active Directory. **OBS.** Quando o GFI MailEssentials estiver protegido por um firewall, o recurso de Coleta de diretório pode não ser capaz de se conectar diretamente ao Active Directory interno por causa das configurações do firewall. Use as pesquisas LDAP para estabelecer uma conexão com o Active Directory interno de sua rede e certifique-se de habilitar a porta padrão 389/636 em seu firewall.
Use LDAP lookups	Selecione para configurar as definições LDAP se o GFI MailEssentials estiver instalado no modo SMTP. Se seu servidor LDAP exigir autenticação, desmarque a opção **Anonymous bind** e digite os detalhes de autenticação a serem usados por este recurso. **OBS.** Especifique as credenciais de autenticação usando o formato Domínio\Usuário (por exemplo, domínio-mestre\administrador). **OBS.** Em um Active Directory, o servidor LDAP normalmente é o Controlador de domínio.

3. Em **Block if non-existent recipients equal or exceed**, especifique o número de destinatários inexistentes que qualificará o email como spam. Emails serão bloqueados pelo filtro Coleta de diretório se todos os destinatários de um email forem inválidos ou o número de destinatários inválidos em um email for igual ao ou exceder o limite especificado.

OBS.
Para evitar falsos positivos, defina um valor razoável na caixa de edição **Block if non-existent recipients equal or exceed**. Esse valor deve levar em consideração os usuários que enviarem emails legítimos com os endereços de email digitados incorretamente ou os usuários que não trabalham mais na empresa. É recomendável que esse valor seja pelo menos **2**.

4. Forneça um endereço de email e clique em **Test** para verificar as configurações do filtro Coleta de diretório. Repita o teste usando um endereço de email não existente e certifique-se de que a pesquisa do Active Directory falhe.

5. Clique na guia **Actions** para selecionar as ações a serem executadas nas mensagens identificadas como spam. Para obter mais informações, consulte Ações de spam - O que fazer com emails de spam (página 148).

OBS.
Se o filtro Coleta de diretório estiver configurado para ser executado no nível do SMTP, somente a opção **Log rule occurrence to this file** estará disponível na guia **Actions**.

6. Clique em **Apply**.

Estágio 2 - Selecionar se o filtro Coleta de diretório deve ser executado durante a transmissão SMTP.

1. Acesse **Anti-spam > Filter Priority** e selecione a guia **SMTP Transmission Filtering**.

2. Clique no botão **Switch** para ativar ou desativar a filtragem da coleta de diretório:

Opção	Descrição
Filtering on receiving full email	A filtragem é feita quando todo o email é recebido.
Filtering during SMTP transmission	A filtragem é feita durante a transmissão SMTP verificando se os destinatários do email existem antes que o corpo e os anexos do email sejam recebidos. **OBS.** Se essa opção for marcada, a Coleta de diretório será executada sempre antes de outros tipos de filtros de spam.

3. Clique em **Apply**.

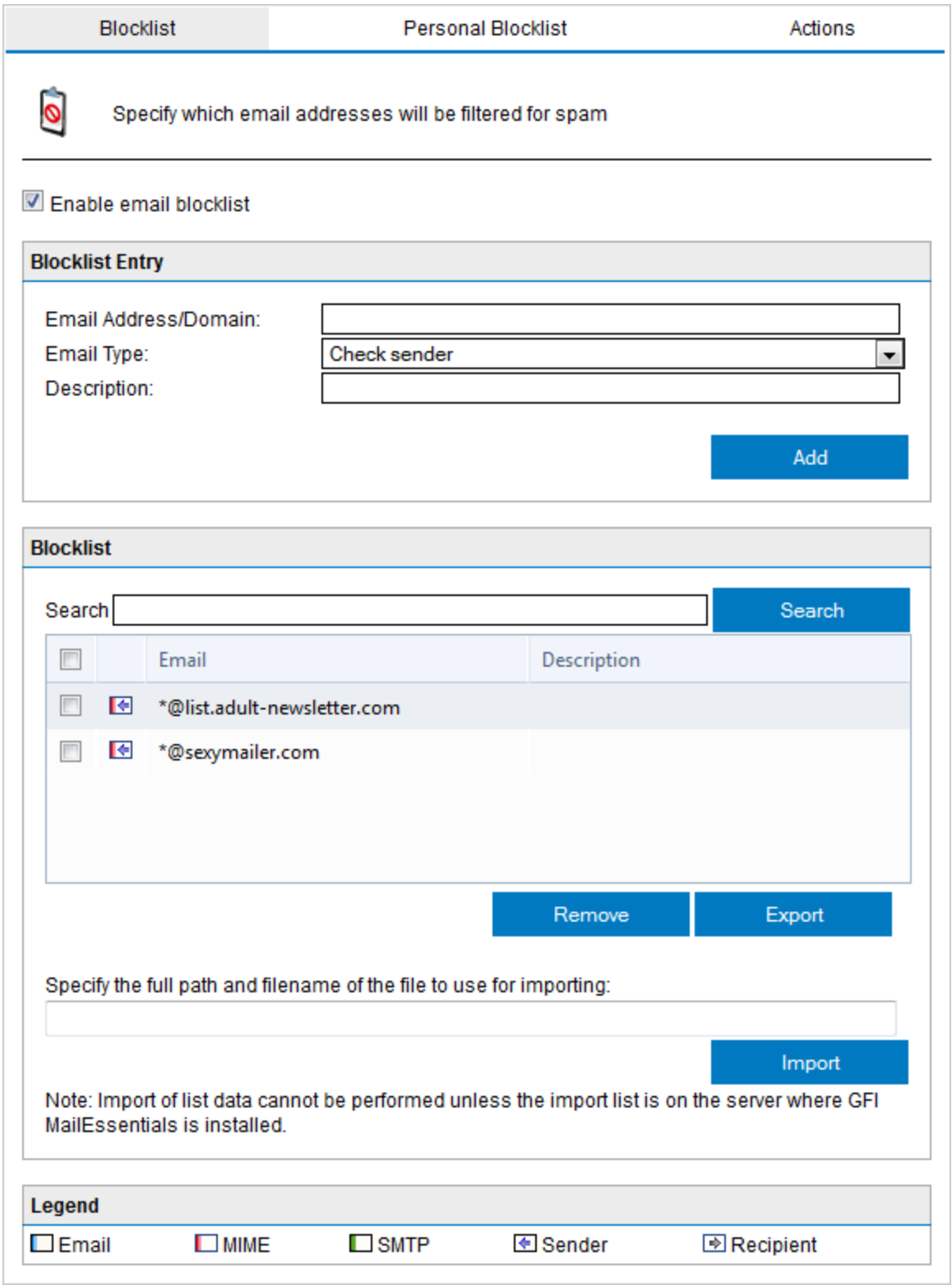
6.1.4 Lista de bloqueio por email

A Lista de bloqueio de email é um banco de dados personalizado de endereços de email e domínios do qual você não deseja receber emails.

Este filtro é habilitado por padrão ao instalar o GFI MailEssentials.

Configurar Lista de bloqueio de email

1. Acesse **Anti-Spam > Anti-Spam Filters > Email Blocklist**.



Screenshot 67: Lista de bloqueio de email

2. Na guia **Blocklist**, configure os endereços de email e os domínios a serem bloqueados.

OPÇÃO	DESCRIÇÃO
Enable Email Blocklist	Marque/desmarque para habilitar/desabilitar Lista de bloqueio de email.

OPÇÃO	DESCRIÇÃO
Add	Adicione endereços de email, domínios de email ou um sufixo do domínio inteiro à lista de bloqueio. 1. Digite um endereço de email, domínio (por exemplo, *@spammer.com) ou um sufixo de domínio inteiro (por exemplo, *@*.tv) para adicioná-lo à lista de bloqueio. 2. Especifique o tipo de email para fazer a correspondência com os emails a serem bloqueados. **OBS.** Para obter mais informações sobre a diferença entre SMTP e MIME, consulte: http://go.gfi.com/?pageid=ME_DifferenceSMTPMIME 3. (Opcional) Você também pode adicionar uma descrição à entrada no campo Descrição. 4. Clique em **Add**.
Remove	Selecione uma entrada na lista de bloqueio e clique em **Remove** para excluir.
Import	Importe uma lista de itens de lista de bloqueio de um arquivo no formato XML. **OBS.** Uma lista de itens poderá ser importada de um arquivo no formato XML na mesma estrutura que o GFI MailEssentials usaria para exportar a lista de itens.
Export	Exporte a lista dos itens da lista de bloqueio para um arquivo em formato XML.
Search	Digite uma entrada para procurar. Os itens correspondentes são filtrados na lista de entradas da lista de bloqueio.

3. Clique na guia **Actions** para selecionar as ações a serem executadas nas mensagens identificadas como spam. Para obter mais informações, consulte Ações de spam - O que fazer com emails de spam (página 148).

4. Clique em **Apply**.

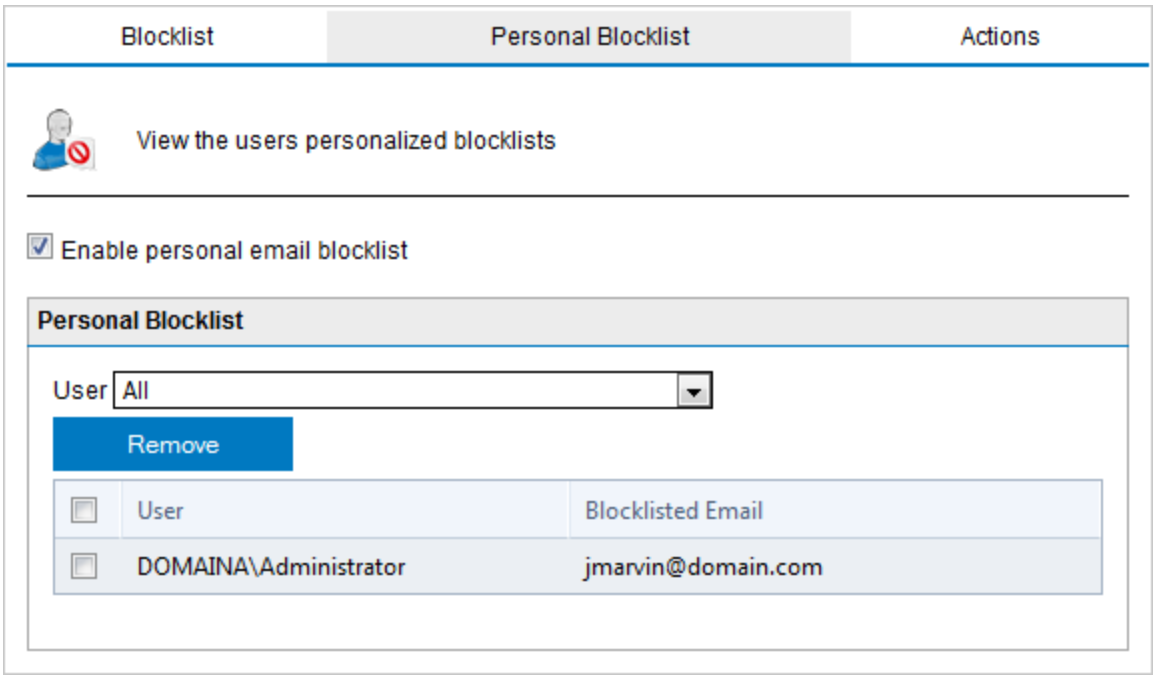
Lista de bloqueio pessoal

A lista de bloqueio pessoal é uma lista de bloqueio adicional que complementa a lista de bloqueio global. Desativada por padrão, a lista de bloqueio pessoal pode ser habilitada para usuários para permitir que eles adicionem determinados endereços de email a uma lista de bloqueio pessoal que eles possam gerenciar. Para obter mais informações, consulte Ações do usuário final (página 21).

Para fins de gerenciamento, os administradores também podem remover endereços de email específicos que os usuários adicionaram a listas de bloqueio pessoal.

Habilitar/desabilitar a lista de bloqueio pessoal

1. Acesse **Anti-Spam > Email Blocklist**.



Screenshot 68: Lista de bloqueio pessoal

2. Selecione a guia **Personal Blocklist** e marque ou desmarque **Enable personal email blocklist** para habilitar ou desabilitar o recurso da lista de bloqueio pessoal.

3. Clique em **Apply**.

Remover emails de listas de bloqueio pessoais de usuários

1. Acesse **Anti-Spam > Email Blocklist** e selecione a guia **Personal Blocklist**.

2. Na lista suspensa **User**, selecione o usuário cujo endereço de email você deseja excluir.

3. Selecione um endereço de email na lista de endereços de email. Clique em **Remove**.

4. Clique em **Apply**.

6.1.5 Lista de bloqueio de IP

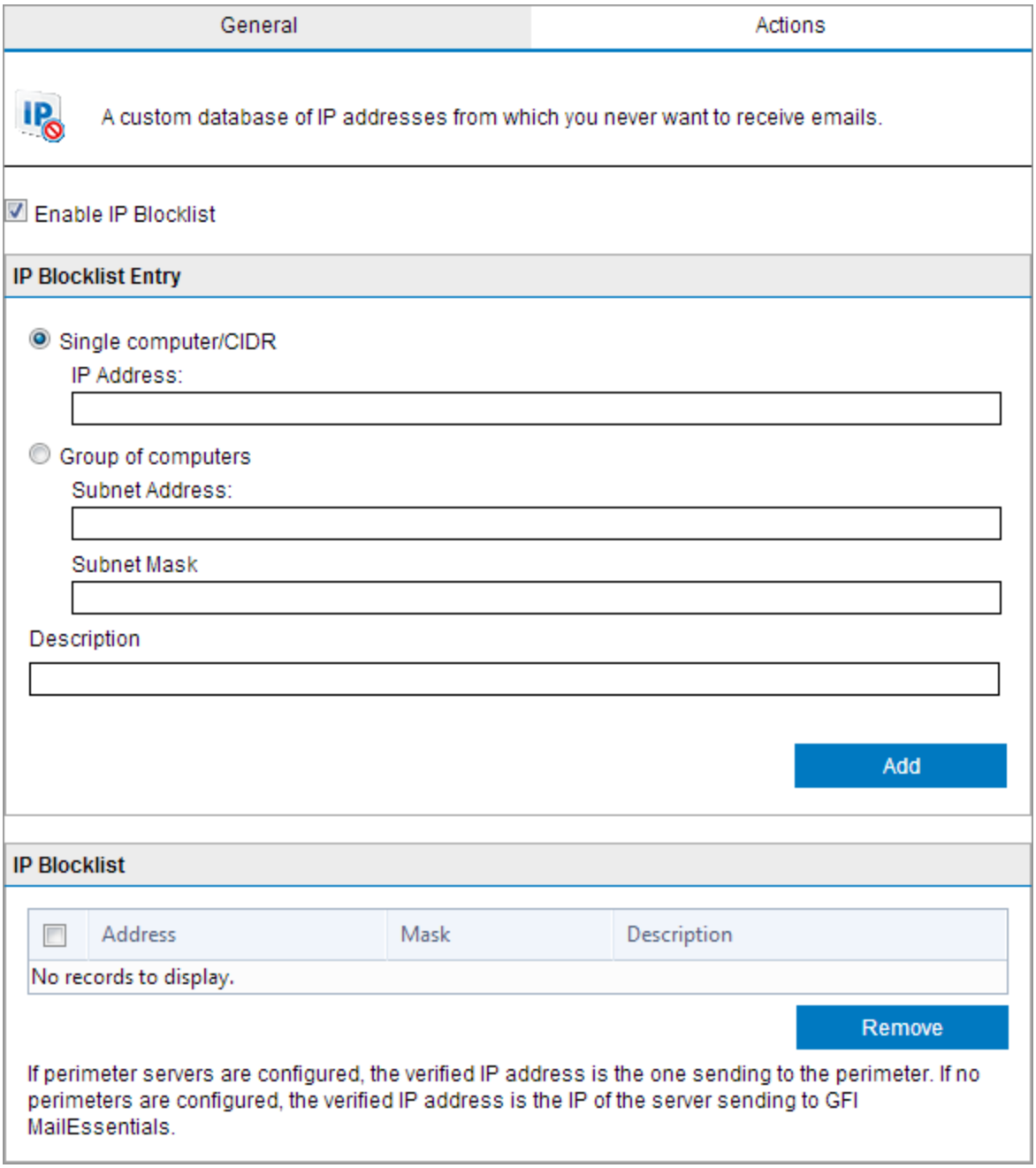
A Lista de bloqueio de IP é um banco de dados personalizado de endereços de email e domínios do qual você não deseja receber emails.

Este filtro pode ser configurado para ser executado quando o email inteiro for recebido ou no nível do SMTP, isto é, emails são filtrados enquanto são recebidos. A filtragem no nível do SMTP encerra a conexão do email e interrompe o download do email completo, economizando largura de banda e recursos de processamento. Nesse caso, a conexão foi encerrada imediatamente e os emails não precisam passar por nenhum outro filtro de spam. Para obter mais informações, consulte Filtragem da transmissão SMTP (página 152).

A Lista de bloqueio de IP NÃO é habilitada por padrão.

Configurar a lista de permissão

1. Acesse **Anti-Spam > Anti-Spam Filters > IP Blocklist**.



Screenshot 69: Lista de bloqueio de IP

2. Na guia **General**, selecione **Enable IP Blocklist** para bloquear todos os emails recebidos de endereços IP específicos.

3. Na caixa **IP Blocklist Entry**, especifique o endereço IP a ser bloqueado:

Opção	Descrição
Single computer / CIDR	Digite um endereço IP único ou um intervalo de endereços IP usando a notação CIDR.
Group of computers	Especifique o **Subnet Address** e a **Subnet Mask** do grupo de IPs da lista de permissão. 2. (Opcional) Adicione uma **Description**. 3 Clique em **Add**.
Descrição	Como alternativa, adicione uma descrição para ajudar a identificar os IPs especificados.

4. Clique em **Add** para adicionar os endereços IP especificados na caixa **IP Blocklist**.

5. Para excluir endereços IP da lista de bloqueio por IP, selecione os endereços a serem removidos e clique em **Remove**.

6. Clique na guia **Actions** para selecionar as ações a serem executadas nas mensagens identificadas como spam. Para obter mais informações, consulte Ações de spam - O que fazer com emails de spam (página 148).

> **OBS.**
> Se a Lista de bloqueio de IP estiver configurada para ser executada no nível do SMTP, somente a opção **Log rule occurrence to this file** estará disponível na guia **Actions**.

7. Clique em **Apply**.

6.1.6 Lista de bloqueio DNS IP

O A Lista de bloqueio de DNS de IP verifica o endereço IP do servidor de email de envio em relação a uma lista de servidores de email conhecidos por serem remetentes de spam. GFI MailEssentials oferece suporte a várias Listas de bloqueio DNS IP. Existem diversas Listas de bloqueio DNS IP de terceiros disponíveis que variam de listas confiáveis com procedimentos descritos de forma clara para ativar ou desativar a Lista de bloqueio DNS IP a listas menos confiáveis.

O GFI MailEssentials mantém um cache com os resultados de consultas à Lista de bloqueio DNS IP para evitar que as Listas de bloqueio DNS IP sejam consultadas várias vezes para os mesmos endereços IP. Os itens permanecem no cache por quatro dias e são apagados no GFI MailEssentials quando o serviço do AS Scan Engine é reiniciado.

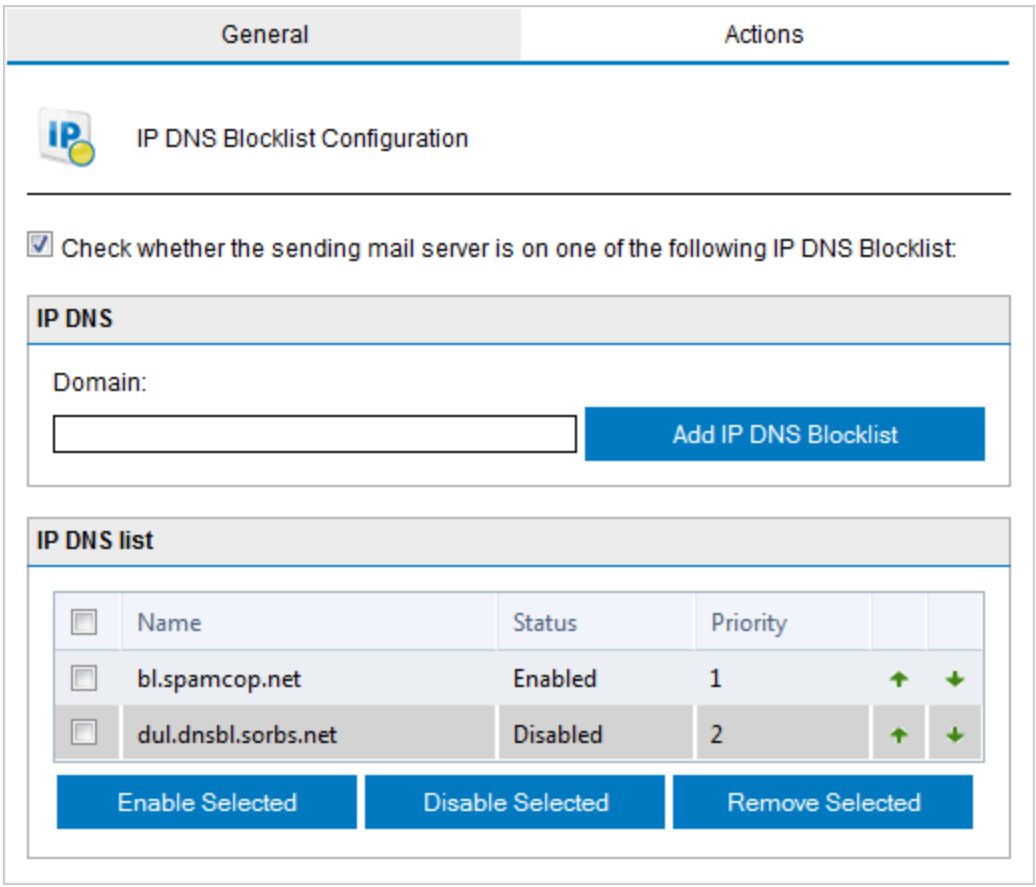
Este filtro pode ser configurado para ser executado quando o email inteiro for recebido ou no nível do SMTP, isto é, emails são filtrados enquanto são recebidos. A filtragem no nível do SMTP encerra a conexão do email e interrompe o download do email completo, economizando largura de banda e recursos de processamento. Nesse caso, a conexão foi encerrada imediatamente e os emails não precisam passar por nenhum outro filtro de spam. Para obter mais informações, consulte Filtragem da transmissão SMTP (página 152).

Este filtro é habilitado por padrão quando o GFI MailEssentials é instalado.

> **Observações importantes**
>
> 1. O servidor DNS deve estar configurado corretamente para que esse recurso funcione. Se esse não for o caso, ocorrerão interrupções no serviço e o tráfego de emails será mais lento. Para obter mais informações, consulte: http://go.gfi.com/?pageid=ME_ProcessingSlow
>
> 2. A consulta de uma Lista de bloqueio DNS IP pode ser lenta (dependendo de sua conexão), e os emails poderão ficar mais lentos.
>
> 3. Certifique-se de que todos os servidores SMTP de perímetro estejam configurados na caixa de diálogo Servidores SMTP de perímetro para que o GFI MailEssentialspossa verificar o endereço IP conectando aos servidores de perímetro. Para obter mais informações, consulte Configurações do servidor SMTP de perímetro (página 238).

Configurar a Lista de bloqueio DNS IP

1. Acesse **Anti-Spam > Anti-Spam Filters > IP DNS Blocklist**.



Screenshot 70: Lista de bloqueio DNS IP

2. Configure as seguintes opções:

Opção	Descrição
Check whether the sending mail server is on one of the following IP DNS Blocklists:	Selecione esta opção para ativar o filtro Lista de bloqueio DNS IP.
Add IP DNS Blocklist	Se necessário, adicione mais Listas de bloqueio DNS IP às outras listas. Digite o domínio da Lista de bloqueio DNS IP e clique em **Add IP DNS Blocklist**.
Enable Selected	Selecione uma Lista de bloqueio DNS IP e clique em **Enable Selected** para habilitá-la.
Disable Selected	Selecione uma Lista de bloqueio DNS IP e clique em **Disable Selected** para desabilitá-la.
Remove Selected	Selecione uma Lista de bloqueio DNS IP e clique em **Remove Selected** para removê-la.

3. Clique na guia **Actions** para selecionar as ações a serem executadas nas mensagens identificadas como spam. Para obter mais informações, consulte Ações de spam - O que fazer com emails de spam (página 148).

4. Clique em **Apply**.

OBS.
Para habilitar a Lista de bloqueio DNS IP DNS no nível de filtragem da transmissão SMTP, selecione a guia **Anti-Spam > Filter Priority > SMTP Transmission Filtering** e clique em **Switch** ao lado da Lista de bloqueio DNS IP para habilitar/desabilitar a filtragem no nível SMTP ou no recebimento do email completo.

6.1.7 Lista de bloqueio DNS URI

Bloqueia emails que contêm links para domínios listados em lista de bloqueio de URI de spam públicas.

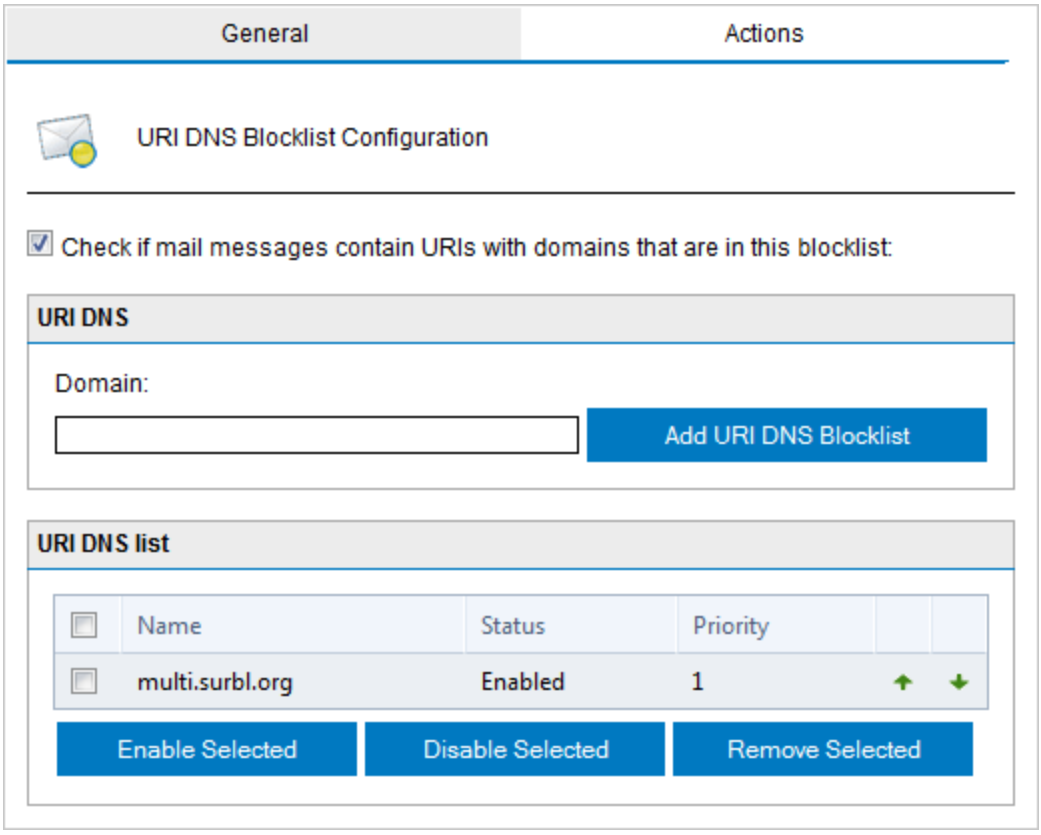
Um Universal Resource Identifier (URI) é um meio padrão de endereçar recursos na Web.

Listas de bloqueio em tempo real (RBL) detectam spam baseados em hiperlinks em emails conhecidos por serem usados por remetentes de spam.

Este filtro é habilitado por padrão ao instalar o GFI MailEssentials.

Configurar a Lista de bloqueio DNS URI

1. Acesse **Anti-Spam > Anti-Spam Filters > URI DNS Blocklist.**



Screenshot 71: Lista de bloqueio DNS URI

2. Na guia **URI DNS Blocklist**:

Opção	Descrição
Check if mail message contains URIs with domains that are in these blocklists:	Selecione esta opção para ativar o filtro Lista de bloqueio DNS URI.

Opção	Descrição
Add URI DNS Blocklist	Se necessário, adicione mais listas de bloqueio DNS URI aos que já estão na lista. Digite o nome completo do domínio Lista de bloqueio DNS URI e clique em **Add URI DNS Blocklist**.
Order of preference	A ordem de preferência para listas de bloqueio DNS URI habilitadas pode ser alterada selecionando uma lista de bloqueio e clicando nos botões Up ou Down.
Enable Selected	Selecione uma Lista de bloqueio DNS URI e clique em **Enable Selected** para habilitá-la. **OBS.** É recomendável desativar qualquer outra lista de bloqueio DNS URI quando habilitar **multi.surbl.org**, pois isso pode aumentar o tempo de processamento de e-mails.
Disable Selected	Selecione uma Lista de bloqueio DNS URI e clique em **Disable Selected** para desativá-la.
Remove Selected	Selecione uma Lista de bloqueio DNS URI e clique em **Remove Selected** para removê-la.

3. Clique na guia **Actions** para selecionar as ações a serem executadas nas mensagens identificadas como spam. Para obter mais informações, consulte Ações de spam - O que fazer com emails de spam (página 148).

4. Clique em **Apply**.

6.1.8 Estrutura de políticas do remetente

Este filtro usa registros SPF para bloquear emails enviados de endereços IP falsificados, identificando se o endereço IP do remetente é autorizado. O filtro Estrutura de políticas do remetente é baseado em um esforço comunitário que exige que os remetentes publiquem os endereços IP de seus servidores de email em um registro SPF.

Exemplo: Se um email for enviado de xyz@EmpresaABC.com, empresaabc.com deverá publicar um registro SPF para que o SPF possa determinar se o email foi realmente enviado pela rede da empresaABC.com ou se foi falsificado. Se um registro SPF não for publicado pela EmpresaABC.com, o resultado do SPF será "desconhecido".

Para obter mais informações sobre o SPF e como ele funciona, visite o site Estrutura de políticas do remetente em:

http://www.openspf.org.

O filtro SPF NÃO é habilitado por padrão e é recomendável habilitar essa opção e executar esse filtro antes do filtro Email Whitelist para bloquear remetentes forjados antes que eles sejam incluídos na lista de permissão.

O GFI MailEssentials não exige a publicação de registros SPF. Para publicar registros SPF, use o assistente de SPF em:

http://www.openspf.org/wizard.html.

Pré-requisitos

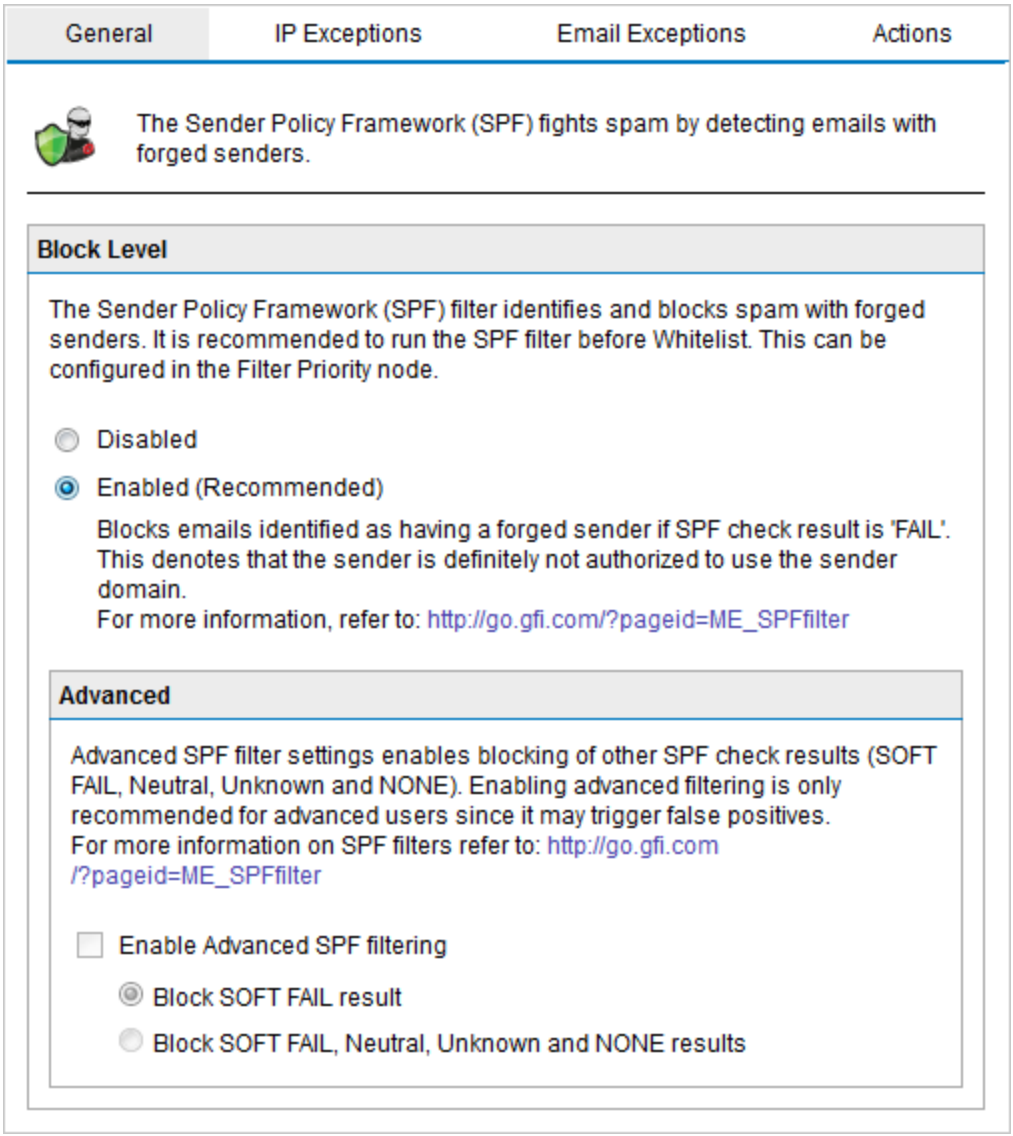
Antes de habilitar o filtro Estrutura de políticas do remetente em uma instalação de servidor fora do gateway:

1. Acesse **General Settings > Perimeter SMTP Servers.**

2. Clique em **Detect** na opção de configuração Perimeter SMTP para efetuar uma pesquisa de MX de DNS e definir automaticamente o endereço IP de seu servidor SMTP de perímetro.

Ativar a Estrutura de políticas do remetente

1. Selecione **Anti-Spam > Anti-Spam Filters > Sender Policy Framework.**



Screenshot 72: Habilitar e configurar a Estrutura da políticas do remetente

2. Clique em **Enabled** para habilitar o filtro Estrutura de políticas do remetente. Se o endereço de IP do remetente do email não for autorizado a enviar emails do domínio do remetente, os emails serão bloqueados.

3. Como alternativa, selecione **Enable Advanced SPF filtering** e selecione uma das opções avançadas de:

OPÇÃO	DESCRIÇÃO
Block SOFT FAIL result	Bloqueia todos os emails cujo: » Endereço IP do remetente definitivamente não tem permissão para enviar emails do domínio do remetente. » Endereço IP do remetente provavelmente não tem permissão para enviar emails do domínio do remetente. Para obter mais informações sobre a filtragem de SPF avançada, consulte: http://go.gfi.com/?pageid=ME_SPFfilter
Block SOFT FAIL, Neutral, Unknown and NONE results	Bloqueia todos os emails cujo: » Endereço IP do remetente definitivamente não tenha permissão para enviar emails do domínio do remetente. » Endereço IP do remetente provavelmente não tenha permissão para enviar emails do domínio do remetente. » Endereço IP do remetente é explicitamente inconclusivo, desconhecido ou sem dados publicados. Para obter mais informações sobre a filtragem de SPF avançada, consulte: http://go.gfi.com/?pageid=ME_SPFfilter

4. Selecione a guia **IP Exceptions** ou **Email Exceptions** para configurar os endereços IP e/ou destinatários para excluir das verificações SPF:

» **IP exception list:** As entradas nesta lista passam automaticamente nas verificações SPF. Selecione a caixa de verificação **IP Exception List**, adicione um novo endereço IP e a descrição e clique em **Add**. Para remover entradas, selecione-as na lista e clique em **Remove Selected**. Para desativar a lista de exceção IP, desmarque a caixa de verificação **IP Exception List**.

> **OBS.**
> Ao adicionar endereços IP à lista de exceção de IP, você poderá adicionar um intervalo de endereços IP usando a notação CIDR.

» **Email exception list:** Esta opção impede que alguns remetentes ou destinatários de emails sejam excluídos da verificação SPF, mesmo se as mensagens de email forem rejeitadas. Selecione a caixa de verificação **Email Exception List**, adicione um novo endereço de email e uma descrição e clique em **Add**. Para remover entradas, selecione-as na lista e clique em **Remove Selected**. Para desativar a lista de exceção de email, desmarque a caixa de verificação **Email Exception List**. Um endereço de email pode ser inserido de qualquer uma das três seguintes maneiras:

- local part - 'abuse' (corresponde a 'abuse@abc.com', 'abuse@xyz.com', etc...)
- domínio - '@abc.com' (corresponde a 'john@abc.com ', 'jill@abc.com', etc...)
- completo - 'joe@abc.com' (corresponde somente a 'joe@abc.com')

5. Clique na guia **Actions** para selecionar as ações a serem executadas nas mensagens identificadas como spam. Para obter mais informações, consulte Ações de spam - O que fazer com emails de spam (página 148).

6. Clique em **Apply** para salvar as configurações.

6.1.9 Anti-spoofing

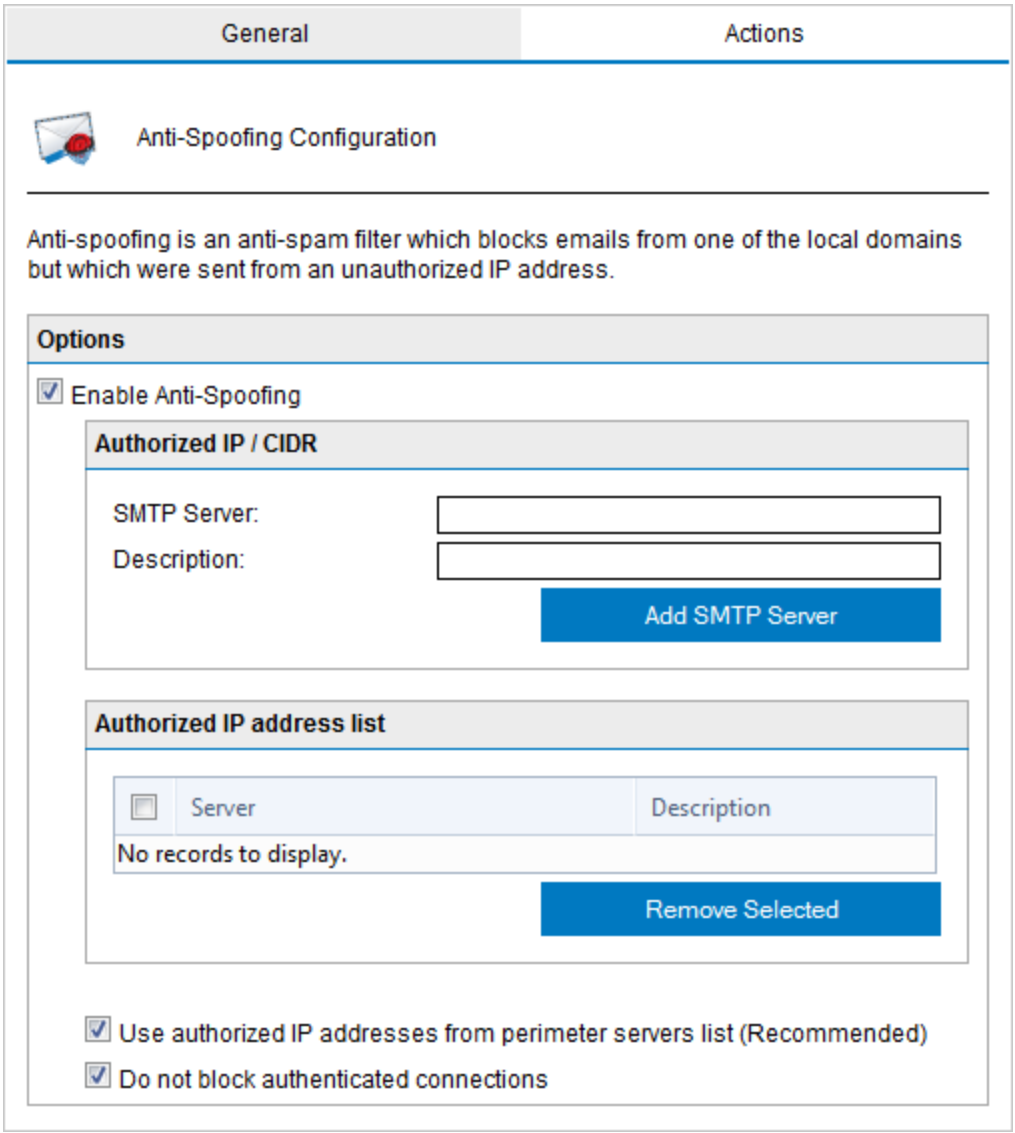
Verifica emails recebidos com um endereço de email do remetente originado de seu próprio domínio em relação a uma lista de endereços IP do GFI MailEssentials. Se o endereço IP do remetente não estiver na lista de endereços IP do servidor do domínio, o email será bloqueado.

Este filtro NÃO é habilitado por padrão.

> **AVISO**
> Se habilitar esse recurso, não inclua usuários internos na lista de permissão, pois isso desativa a verificação anti-spoofing.

Como ativar e configurar o filtro anti-spoofing

1. Acesse **Anti-Spam > Anti-Spam Filters > Anti-Spoofing**.



Screenshot 73: Filtro anti-spoofing do GFI MailEssentials

2. Selecione **Enable Anti-Spoofing** para habilitar o filtro anti-spoofing.

3. No campo **SMTP Server:**, forneça o servidor SMTP no qual o GFI MailEssentials verifica os endereços dos destinatários de emails. Forneça também uma descrição do servidor no campo **Description:**.

> **OBS.**
> O campo SMTP Server oferece suporte aos seguintes tipos de entrada:
>
> » Um endereço IP único
>
> » Um intervalo CIDR (por exemplo, 192.0.2.1/24)

4. Clique em **Add SMTP Server** para salvar os detalhes do servidor SMTP.

> **OBS.**
> Para remover servidores SMTP adicionados anteriormente, selecione um servidor SMTP na lista Endereço IP autorizado e clique em **Remove Selected**.

Por padrão, as opções **Use authorized IP addresses from perimeter server** e **Do not block authenticated connections** são habilitadas. Não é recomendado desativar essas opções.

> **OBS.**
> A caixa de seleção **Do not block authenticated connections** não se aplica ao Microsoft IIS e ao Microsoft Exchange 2003. Funciona apenas com o Exchange 2007 ou superior.

6.1.10 Lista de exclusão temporária

O filtro Lista de exclusão temporária bloqueia temporariamente a entrada de emails recebidos de remetentes desconhecidos. Sistemas de email legítimos normalmente tentam enviar o email após alguns minutos. Os remetentes de spam simplesmente ignoram essas mensagens de erro.Se um email for recebido novamente após um determinado período, a Lista de exclusão temporária irá:

» Armazenar os detalhes do remetente em um banco de dados de forma que quando o remetente enviar outro email, a mensagem não estará na lista de exclusão temporária

» Receber o email e prosseguir com a verificação anti-spam

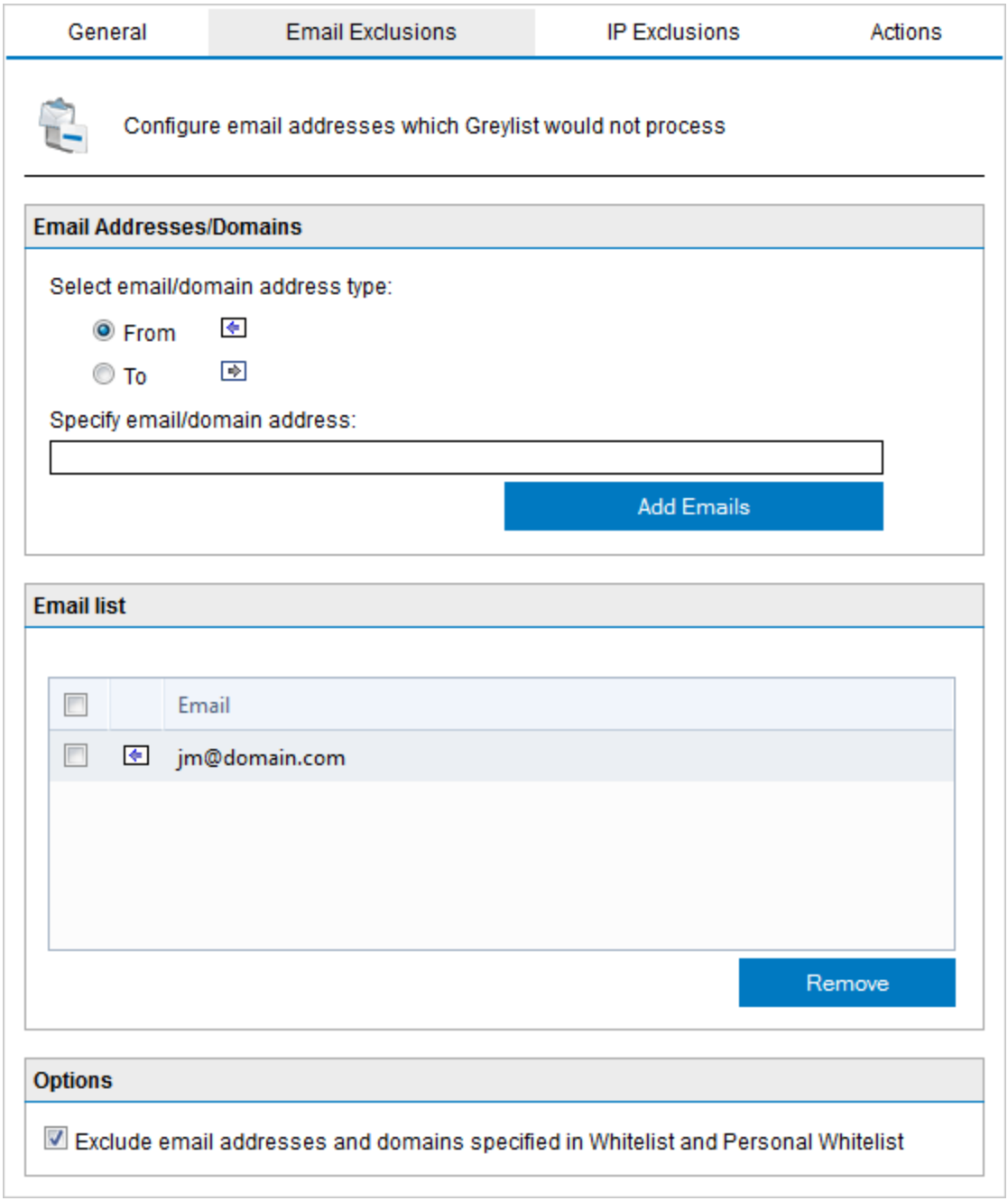
A lista de exclusão temporária **NÃO** é habilitada por padrão.

> **Observações importantes**
>
> 1. Para habilitar a Lista de exclusão temporária, o GFI MailEssentials deve ser instalado no servidor SMTP de perímetro. Para obter mais informações, consulte http://go.gfi.com/?pageid=ME_GreylistSMTP
>
> 2. A Lista de exclusão temporária contém listas de exclusão para que determinados endereços de email, domínios e endereços IP não sejam incluídos em uma lista de exclusão temporária. Exclusões devem ser configuradas quando:
>
> » Emails provenientes de determinados endereços de email, domínios ou endereços IP não possam ser atrasados
>
> » Emails para um determinado usuário local que não possam ser atrasados

Configurar a Lista de exclusão temporária

1. Acesse **Anti-Spam > Anti-Spam Filters > Greylist**.

2. Na guia **General**, marque/desmarque **Enable Greylist** para habilitar/desabilitar a Lista de exclusão temporária.



Screenshot 74: Exclusões de email

3. Selecione a guia **Email exclusions** para especificar todos os endereços de email ou domínios que você não deseja incluir em uma lista de exclusão temporária. Na área **Edit Addresses**, especifique:

» endereço de email completo ou

» emails de um domínio inteiro (por exemplo: *@dominioconfiavel.com) ou

» um sufixo de domínio inteiro (por exemplo: *@*.mil ou *@*.edu)

Também especifique se a exclusão se aplica aos remetentes. Selecione **From (>)** ou **To (>)** para os destinatários locais.

» **Exemplo 1:** Não coloque emails na lista de exclusão temporária se o destinatário for administrator@mydomain.com, para que os emails enviados para administrator@mydomain.com nunca sejam atrasados.

» **Exemplo 2:** Não coloque emails na lista de exclusão temporária se o domínio do remetente for trusteddomain.com (`*@trusteddomain.com`), para que emails recebidos do domínio trusteddomain.com nunca sejam atrasados.

Clique em **Add emails** para adicionar a exclusão.

> **OBS.**
> Para impedir que endereços de email da lista de permissão e da lista de permissão automática sejam incluídos na lista de permissão temporária ou atrasados, selecione **Exclude email addresses and domains specified in Whitelist**.

4. Selecione a guia **IP exclusions** para especificar os endereços IP que serão excluídos da lista de exclusão temporária. Clique em **Add IPs** e especifique um IP a ser excluído.

5. Para impedir que endereços IP na lista de permissão sejam incluídos na lista de exclusão temporária e atrasados, selecione **Exclude IP addresses specified in Whitelist**.

6. Para registrar ocorrências de lista de exclusão temporária em um arquivo de log, clique na guia **ActionsFicheiro** e selecione **Log rule occurrence to this file**.

> **OBS.**
> Arquivos de registro podem ficar muito grandes. GFI MailEssentials oferece suporte à rotação de registros, quando novos arquivos de registro são criados periodicamente ou quando o arquivo de registro atinge um tamanho específico. Para habilitar a rotação de arquivo de registro, acesse **Anti-Spam > Anti-Spam Settings**. Selecione a guia **Anti-spam logging**, marque **Enable log file rotation** e especifique a condição de rotação.

7. Clique em **Apply**.

6.1.11 Detecção de idioma

Determina o idioma do texto do corpo do email e é configurável para bloquear certos idiomas. GFI MailEssentials retira uma parte da mensagem de corpo do email e compara com um mecanismo de idioma integrado.

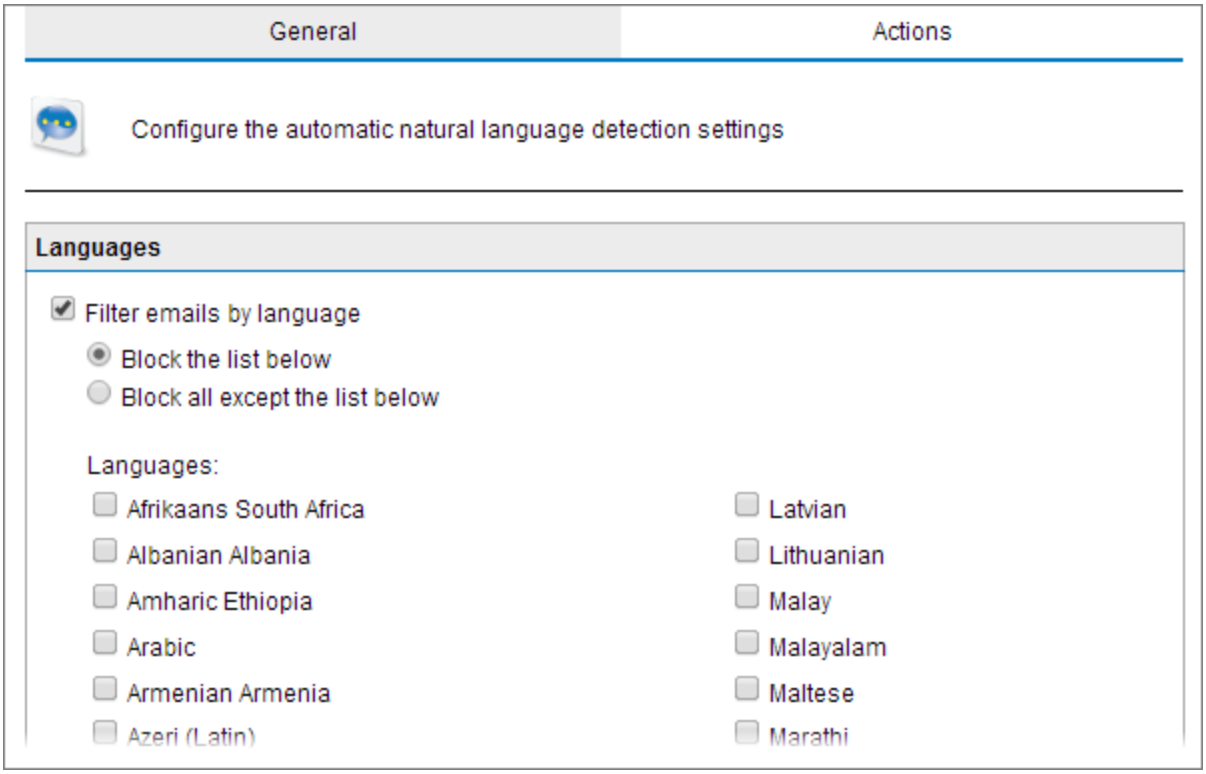
Configurar o filtro de detecção de idioma para bloquear certos idiomas e permitir outros.

> **OBS.**
> O filtro de Detecção de idioma é diferente do filtro Verificação de cabeçalho – Idioma uma vez que ele analisa o idioma do texto do corpo do email. O filtro de verificação de cabeçalho analisa a codificação (conjunto de caracteres) do cabeçalho de email. Os resultados do mecanismo de filtragem de detecção de idioma são geralmente mais confiáveis.

O filtro de Detecção de idioma **NÃO** é habilitado por padrão ao instalar.

Configurar a detecção de idioma

1. Acesse **Anti-Spam > Anti-Spam Filters > Language Detection**.



Screenshot 75: Opções de detecção de idioma

2. Na guia **General**, marque/desmarque **Filter emails by language** para habilitar/desabilitar a Detecção de idioma.

3. Selecione **Block the list below** para selecionar os idiomas para bloquear ou **Block all except the list below** para bloquear todos os idiomas, exceto os selecionados.

4. Selecione os idiomas para bloquear/permitir na área **Languages**.

5. Clique na guia **Actions** para selecionar as ações a serem executadas nas mensagens identificadas como spam. Para obter mais informações, consulte Ações de spam - O que fazer com emails de spam (página 148).

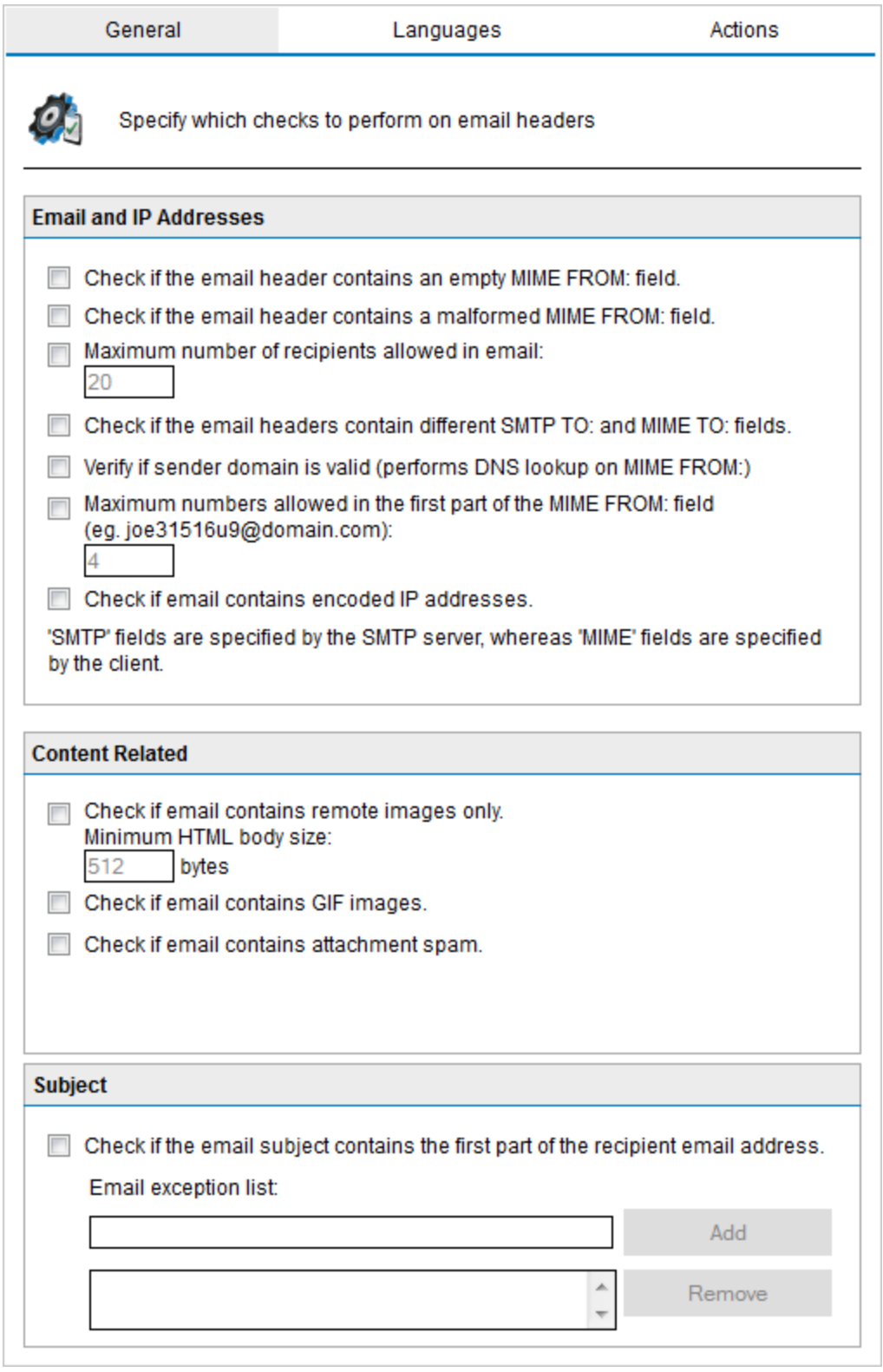
6. Clique em **Apply**.

6.1.12 Verificação de cabeçalho

O filtro Verificação de cabeçalho analisa o cabeçalho de email para identificar emails com spam.

Configurar a verificação de cabeçalho

1. Acesse **Anti-Spam > Anti-Spam Filters > Header Checking**.



Screenshot 76: Opções de verificação de cabeçalho

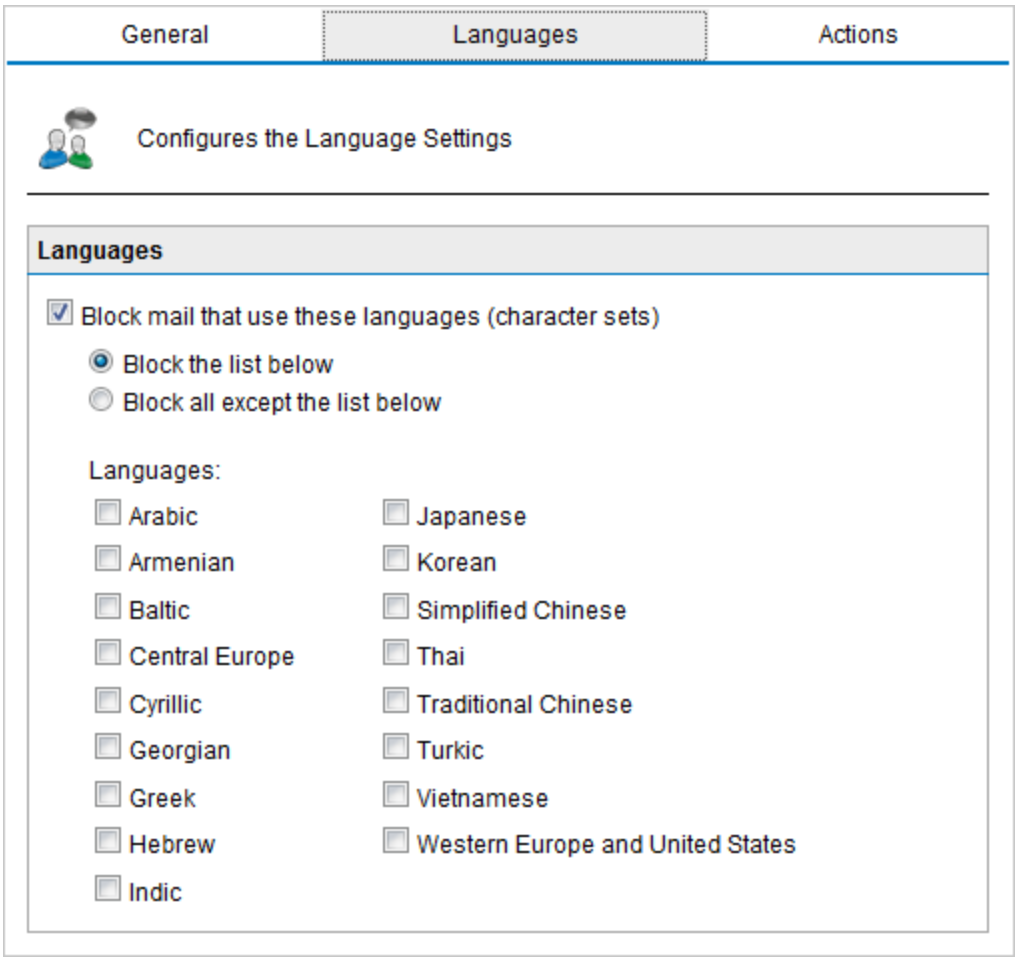
2. Habilite, desabilite ou configure os parâmetros a seguir.

Opção	Descrição
Check if the email header contains an empty MIME FROM: field.	Verifica se o remetente se identificou no campo "De:". Se esse campo estiver vazio, a mensagem será marcada como spam.

Opção	Descrição
Check if the email header contains a malformed MIME FROM: field.	Verifica se o campo MIME é uma notação correta como definida nas RFCs.
Maximum number of recipients allowed in email	Identifica emails com grandes quantidades de destinatários e sinaliza-os como SPAM.
Check if the email headers contain different SMTP TO: and MIME TO: fields.	Verifica se os campos SMTP to: e MIME to: são os mesmos. Os servidor de email de remetentes de spam sempre precisa incluir um endereço SMTP para:. No entanto, o endereço email MIME para: muitas vezes não é incluído ou é diferente. **OBSERVAÇÃO:** Esse recurso identifica muitos spams, mas alguns servidores de lista também não incluem o MIME para:. Portanto, é recomendável incluir o boletim informativo da lista de endereços permitidos para usar esse recurso.
Verify if sender domain is valid (performs DNS lookup on MIME FROM:)	Executa uma pesquisa de DNS no domínio no MIME do campo e verifica a validade do domínio. **OBSERVAÇÃO:** Certifique-se de que o servidor DNS esteja configurado corretamente para evitar tempo de espera e fluxo de email lento.
Maximum numbers allowed in the first part of the MIME FROM: field:	Identifica a presença de números no campo MIME de. Os remetentes de spam normalmente usam ferramentas que criam automaticamente endereços de resposta únicos usando números no endereço.
Check if email contains encoded IP addresses.	Verifica o cabeçalho e o corpo da mensagem quanto à presença de URLs com IP codificado hexagonal/octogonal (http://0072389472/hello.com) ou que apresentem uma combinação nome de usuário/senha (por exemplo, www.citibank.com@scammer.com). Os exemplos a seguir são sinalizados como spam. » http://12312 » www.microsoft.com:hello%01@123123
Check if email contains remote images only. Tamanho mínimo do corpo da mensagem em HTML	Sinalizar emails que somente têm imagens remotas e uma quantidade mínima de texto como spam. Ajuda na identificação do spam "email apenas com imagens".
Check if email contains GIF images.	Verifica se o email contém uma ou mais imagens GIF incorporadas. Imagens GIF incorporadas são geralmente usadas para burlar os filtros de spam. **IMPORTANTE:** Como alguns emails legítimos contêm imagens GIF incorporadas, essa opção pode gerar falsos positivos.
Check if email contains attachment spam.	Verifica anexos de email quanto à presença de propriedades comuns em anexos enviados em email com spam. Isso ajuda a identificar as últimas técnicas usadas por remetentes de spam que usam anexos para enviar spam.
Check if the email subject contains the first part of the recipient email address.	Identifica o email de spam personalizado, no qual os remetentes de spam frequentemente incluem a primeira parte do endereço de email de destinatário no assunto.

3. Na guia **Language**, selecione **Block mail that use these languages (character sets)** para ativar a detecção do idioma.

> **OBS.**
> O filtro de verificação de cabeçalho é diferente do filtro Detecção de idioma uma vez que ele analisa a codificação (conjunto de caracteres) do cabeçalho de email. A detecção de idioma analisa o idioma do texto do corpo do email. Os resultados do mecanismo de filtragem de detecção de idioma são geralmente mais confiáveis.



Screenshot 77: Detecção de idioma

4. Selecione **Block the list below** para selecionar os idiomas para bloquear ou **Block all except the list below** para bloquear todos os idiomas, exceto os selecionados.

5. Selecione os idiomas para bloquear/permitir na área **Languages**.

6. Clique na guia **Actions** para selecionar as ações a serem executadas nas mensagens identificadas como spam. Para obter mais informações, consulte Ações de spam - O que fazer com emails de spam (página 148).

7. Clique em **Apply**.

6.1.13 Verificação de palavras-chave de spam

Este filtro permite a identificação do spam baseada em palavras-chave no email que está sendo recebido.

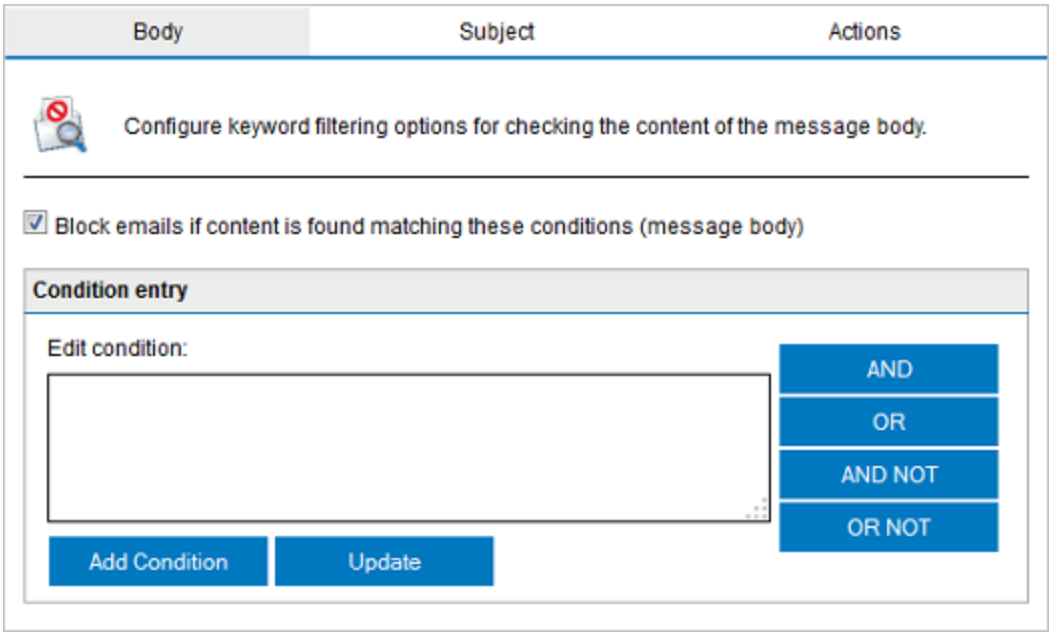
Este filtro **NÃO** é habilitado por padrão ao instalar o GFI MailEssentials.

> **OBS.**
> Esse filtro apenas verifica o conteúdo de email quanto a texto que identifique o email como spam. Para obter uma filtragem de conteúdo de email abrangente (por exemplo, bloquear conteúdo racista ou linguagem vulgar), use a opção Keyword filtering no nó Content Filtering.

Adicionar a verificação da palavra-chave de spam

1. Acesse **Anti-Spam > Anti-Spam Filters > Spam Keyword Checking**.

2. Na guia **Body**, selecione **Block emails if content is found matching these conditions (message body)** para habilitar a Verificação de palavras-chave de spam no corpo do email.



Screenshot 78: Propriedades da Verificação de palavras-chave de spam

3. Na área **Condition Entry**, digite uma palavra-chave ou uma combinação de palavras-chave que devam ser bloqueadas por este filtro. Use os operadores "E", "OU", "E NÃO" e "OU NÃO" para configurar condições específicas.

Por exemplo:

- `Basquete esporte` - GFI MailEssentials bloqueia emails com a frase`Basquete esporte`. Somente essa frase ativará a regra, não a palavra `basquete` OU `esporte` separada por algumas outras palavras.
- `Basquete E beisebol` - GFI MailEssentials bloqueará emails que contenham essas duas palavras. Emails com apenas `basquete` ou apenas `beisebol` não serão bloqueados.

4. Selecione **Match whole words only** para pesquisar especificamente palavras completas evitando o bloqueio de palavras que façam parte de outras palavras. Por exemplo, ativar esta opção não bloquearia a palavra "MSExchange", apesar de a palavra "sex" fazer parte de "MSExchange".

5. Selecione a guia **Subject** e selecione **Block emails if content is found matching these conditions (message subject)** para habilitar a Verificação de palavras-chave de spam no assunto do email.

6. Na área **Condition Entry**, digite uma palavra-chave ou uma combinação de palavras-chave que devam ser bloqueadas por este filtro. Use os operadores "E", "OU", "E NÃO" e "OU NÃO" para configurar condições específicas.

7. Selecione **Apply the keywords list to also scan senders' display names** para verificar o nome de exibição do remetente do email, que pode conter palavras-chave de spam. Por exemplo, spam com o assunto Viagra, que frequentemente simula remetentes e usa a palavra Viagra no

8. Clique na guia **Actions** para selecionar as ações a serem executadas nas mensagens identificadas como spam. Para obter mais informações, consulte Ações de spam - O que fazer com emails de spam (página 148).

9. Clique em **Apply**.

Remover condições

Para remover uma condição de Verificação de palavras-chave de spam:

1. Na área **Conditions list** nas guias **Body** ou **Subject**, selecione uma ou mais condições para remover.

> **OBS.**
> Para encontrar a condição a ser removida, use os controles na lista de condições para percorrer as páginas que listam as condições.

2. Clique em **Remove** e **Apply**.

Importar e exportar condições

Para exportar mais condições:

1. Na área **Conditions list**, nas guias **Body** ou **Subject**, selecione uma ou mais condições para exportar.

> **OBS.**
> Para localizar as condições a serem exportadas, use os controles na lista de condições para percorrer as páginas que listam as condições.

2. Na tela de **File Download**, clique em **Save** e selecione uma pasta onde salvar o arquivo exportado.

Para importar condições:

1. Na área da lista **Conditions**, nas guias **Body** ou **Subject**, digite a pasta e o nome do arquivo a ser importado.

2. Clique em **Import**.

6.1.14 Análise bayesiana

Um filtro anti-spam que pode ser treinado para determinar com precisão se um email é spam com base na experiência.

Este manual também contém informações sobre o funcionamento do filtro bayesiano e como ele pode ser programado. Para obter mais informações, consulte Apêndice - Filtragem bayesiana (página 291).

O filtro de Análise Bayesiana **NÃO** é habilitado por padrão.

> **IMPORTANTE**
> Habilite a coleta de informações de emails de saída e aguarde pelo menos uma semana antes de habilitar o filtro. Isso é necessário porque o filtro bayesiano adquire a taxa de detecção mais alta quando se adapta aos padrões do seu email.

Configurar o filtro bayesiano

A configuração do filtro bayesiano é feita em dois estágios:

Estágio 1: Programar o filtro bayesiano

Estágio 2: Ativar o filtro bayesiano

Estágio 1: Programar o filtro bayesiano

O filtro bayesiano pode ser programado de duas maneiras:

Método 1: Automaticamente, por meio de emails de saída.

O GFI MailEssentials processa emails legítimos (ham) efetuando a verificação de emails de saída. O filtro bayesiano pode ser ativado depois de ter coletado pelo menos 500 emails de saída (se você enviar principalmente emails em inglês) ou 1000 emails de saída (se você enviar emails em outro idioma).

Para fazer isso:

1. Acesse **Anti-Spam > Anti-Spam Filters > Bayesian Analysis**.

2. Selecione **Automatically learn from outbound emails**.

3. Clique em **Apply**.

Método 2: Manualmente, através de emails existentes.

Copie de 500 a 1000 mensagens de seus itens enviados para a subpasta **This is legitimate email** nas pastas públicas **GFI AntiSpam Folders** programa o filtro bayesiano da mesma forma usada na programação do envio de emails.

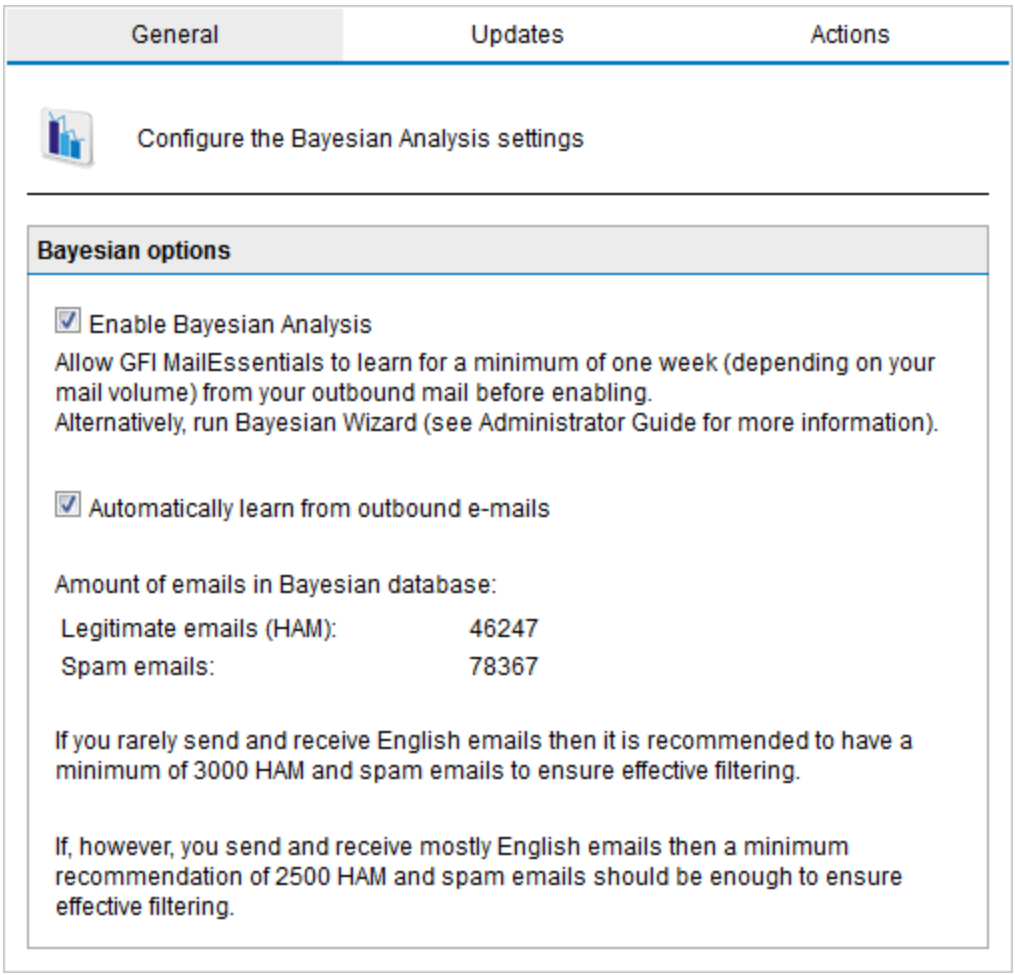
> **OBS.**
> Para usar essa opção, a verificação de pastas públicas deve estar habilitada. Para obter mais informações, consulte Verificação de pasta pública (página 169).

Estágio 2: Como ativar o filtro bayesiano

Depois que o filtro bayesiano for programado, ele deverá ser habilitado.

1. No console de configuração do GFI MailEssentials, acesse **Anti-Spam > Anti-Spam Filters > Bayesian Analysis**.

2. Na guia **General**, selecione **Enable Bayesian Analysis**.



Screenshot 79: Propriedades da análise bayesiana

3. Na guia **Updates**, configure a frequência de atualizações no banco de dados de spam habilitando a opção **Automatically check for updates** e configurando um intervalo de hora em hora.

> **OBS.**
> Clique em **Download updates now...** para fazer imediatamente o download de qualquer atualização.

> **OBS.**
> Você pode fazer o download das atualizações usando um servidor proxy. Para obter mais informações, consulte Configurações de proxy (página 241).

4. Clique na guia **Actions** para selecionar as ações a serem executadas nas mensagens identificadas como spam. Para obter mais informações, consulte Ações de spam - O que fazer com emails de spam (página 148).

5. Clique em **Apply**.

OBS.
O GFI MailEssentials também fornece um assistente da análise bayesiana que permite programar o filtro de análise bayesiana em uma máquina diferente da máquina na qual o GFI MailEssentials está instalado. Para obter mais informações, consulte Treinar o filtro de análise bayesiana (página 292).

6.1.15 Lista de permissão

OBS.
O filtro da lista de permissão afeta somente os filtros anti-spam, e não a segurança de emails e a filtragem de conteúdo

A lista de permissão contém listas de critérios que identificam um email legítimo. Emails que correspondam a esses critérios não são examinados pelos filtros anti-spam e são sempre entregues ao destinatário.Emails podem ser adicionados à lista de permissão usando os seguintes critérios:

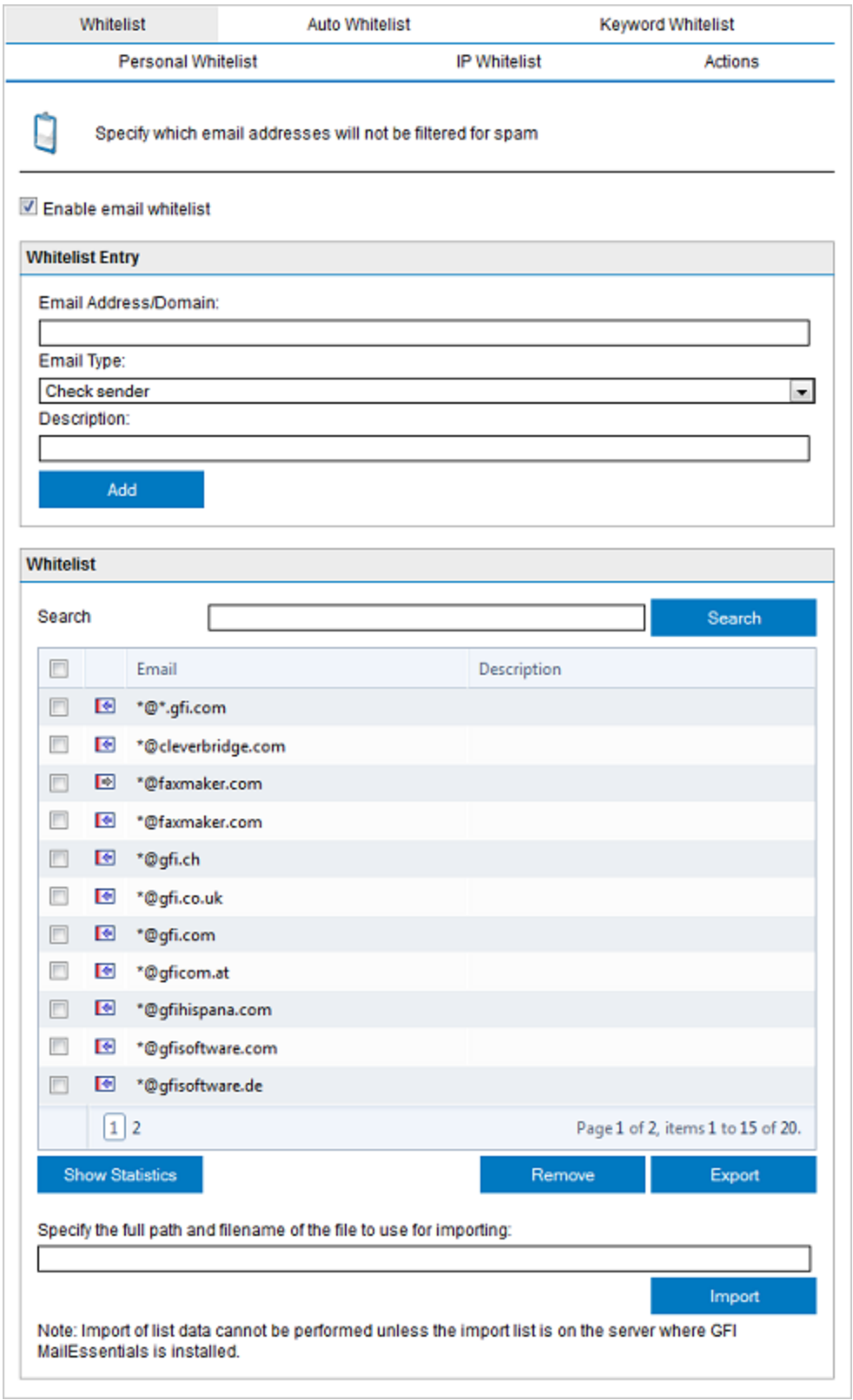
- Endereço de email do remetente, domínio do email ou endereço IP
- Remetentes para os quais um email foi enviado anteriormente (Lista de permissão automática)
- Destinatário (exclui a filtragem de emails em endereços de email locais)
- Palavras-chave no corpo ou assunto do email

Os recursos Lista de permissão e Lista de permissão automática são habilitados por padrão.

Notas importantes
Usar o recurso da Lista de permissão automática é recomendável, uma vez que ele elimina uma alta porcentagem de falsos positivos.
Em Palavra-chave Lista de permissão, é recomendado adicionar termos que os remetentes de spam não usem e termos relacionados à natureza de seu negócio, por exemplo, nomes de seus produtos. Inserir muitas palavras-chave aumenta a possibilidade de emails não serem filtrados pelo GFI MailEssentials e serem entregues nas caixas de correio dos usuários.
Incluir em uma lista de permissão um usuário interno vai contra a finalidade do filtro Anti-Spoofing. Para obter mais informações, consulte Anti-spoofing (página 129).

Configurar a lista de permissão

1. Acesse **Anti-Spam > Whitelist**.



Screenshot 80: Guia Lista de permissão

2. Na guia **Whitelist**, configure os endereços de email e domínios a serem incluídos na lista de permissão. Marque/desmarque **Enable email whitelist** para habilitar/desabilitar a lista de permissão. Execute as seguintes ações:

Ação	Descrição
Adicione uma entrada à lista de permissão	1. Em **Email Address/Domain**, forneça o endereço/domínio do email para a lista de permissão. **Por exemplo:** . *@companysupport.com ou. *@*.edu. 2. Em **Email Type**, especifique o campo do cabeçalho do email para corresponder aos emails a serem adicionados à lista de permissão. **OBS.** Para obter mais informações sobre a diferença entre SMTP e MIME, consulte: http://go.gfi.com/?pageid=ME_DifferenceSMTPMIME 3. (Opcional) Em **Description**, adicione uma descrição do item. 4. Clique em **Add**.
Remova entradas de lista de permissão	1. Selecione uma ou mais entradas da lista de permissão na lista **Whitelist**. 2. Clique em **Remove**.
Pesquise uma entrada na lista de permissão	1. Em **Search**, digite os detalhes do item da lista de permissão a ser pesquisado. 2. Clique em **Search** para exibir a lista de correspondência de termos.
Mostrar estatísticas	Usar o botão **Show Statistics** para exibir o número total de emails bloqueados por entrada da lista de permissão.
Importar entradas da lista de permissão	1. Especifique o caminho completo e o nome do arquivo a ser usado para importar os dados exportados anteriormente. 2. Clique em **Import** para importar entradas.
Exportar entradas da lista de permissão	Clique em **Export** para exportar a lista atual de entradas da lista de permissão para um arquivo XML.

3. Selecione a guia **Auto Whitelist** para configurar as seguintes opções:

Opção	Descrição
Populate Auto Whitelist automatically:	Se selecionada, os endereços de email de destino dos emails de saída serão adicionados automaticamente à lista de permissão automática.
Enable Email Auto Whitelist	Selecione esta opção para ativar a lista de permissão automática. Remetentes de emails recebidos são comparados com a lista de permissão automática. Se o remetente estiver presente na lista, o email será encaminhado diretamente para a caixa de entrada do destinatário.
Maximum entries allowed in the Auto Whitelist:	Especifique o número de entradas permitidas na lista de permissão automática. Quando o limite especificado for excedido, as entradas mais antigas e menos usadas serão automaticamente substituídas por novas entradas. **OBS.** Inserir um valor maior que o valor padrão de 30.000 pode afetar de modo negativo o desempenho do GFI MailEssentials.

4. Na guia **Keyword Whitelist**, especifique as palavras-chave que marcam emails como válidos:

Opção	Descrição
Enable email body keyword whitelist	Selecione esta opção para verificar as palavras-chaves no corpo da mensagem de email que qualificam um email como válido. Adicione palavras-chave à lista **Body Keywords**. Você também poderá importar ou exportar listas de palavras-chave de/para um arquivo XML.

Opção	Descrição
Enable email subject keyword whitelist	Selecione esta opção para verificar palavras-chave no assunto do email que qualifiquem um email como válido. Adicione palavras-chave à lista **Subject Keywords**. Você também poderá importar ou exportar listas de palavras-chave de/para um arquivo XML.
Match whole words only (words/phrases in subject/body)	Ao selecionar esta opção, somente é feita a correspondência de palavras inteiras da lista de permissão por palavra-chave que qualifiquem um email como válido.

5. Na guia **IP Whitelist**, configure:

Opção	Descrição
Enable IP Whitelist	Selecione para permitir que os emails recebidos de endereços IP específicos sejam adicionados à lista de permissão.
Add IP Whitelist entries	1. Especifique: » **Single computer / CIDR**: Digite um endereço IP único ou um intervalo de endereços IP usando a notação CIDR. » **Group of computers**: Especifique o **Subnet Address** e a **Subnet Mask** do grupo de IPs da lista de permissão. 2. (Opcional) Adicione uma **Description**. 3 Clique em **Add**.
Remove IP Whitelist entries	Selecione os IPs a serem removidos e clique em **Remove**.

6. Clique na guia **Actions** para habilitar/desabilitar o registro de ocorrências de lista de permissão de um arquivo. Forneça um caminho/uma pasta onde armazenar o arquivo de registro gerado.

7. Clique em **Apply**.

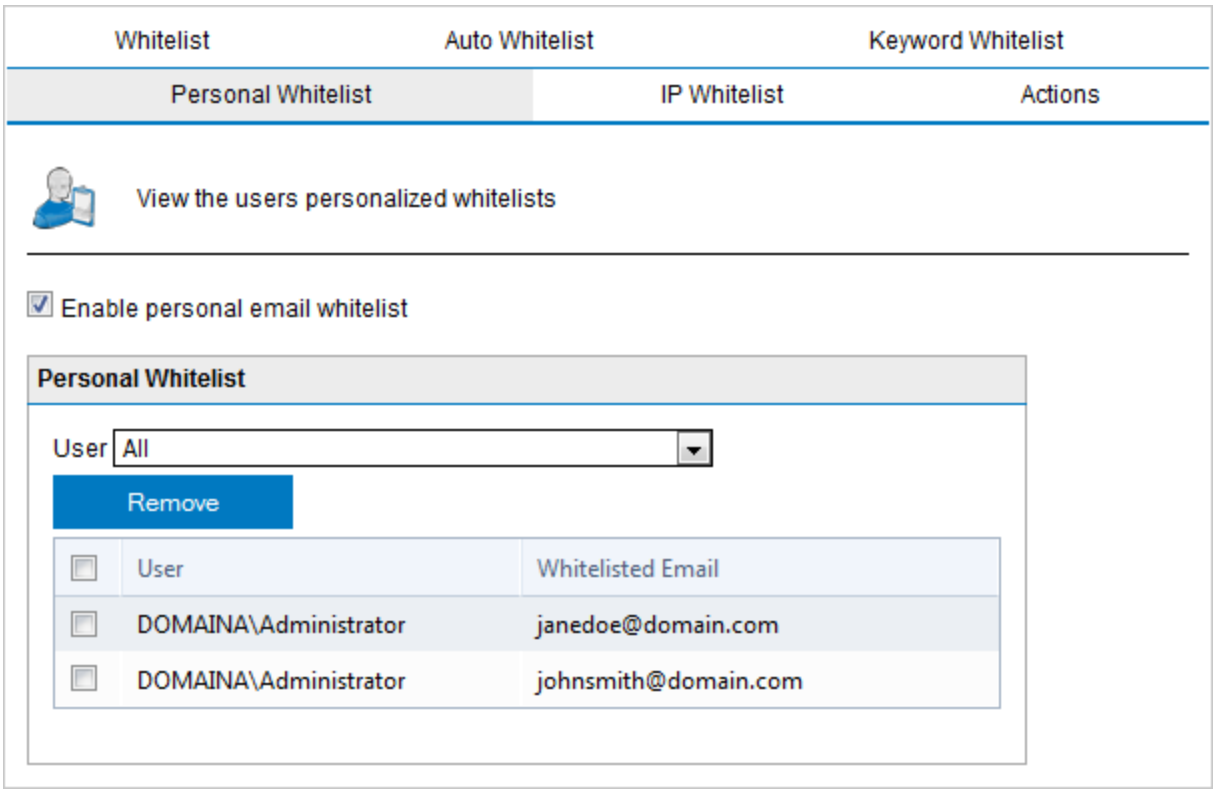
Lista de permissão pessoal

A lista de permissão pessoal é uma lista de permissão adicional que complementa a lista de permissão global. Desabilitada por padrão, a lista de permissão pessoal pode ser habilitada para usuários para permitir que eles adicionem endereços de email específicos a uma lista de permissão pessoal que possam gerenciar. Para obter mais informações, consulte Ações do usuário final (página 21).

Para fins de gerenciamento, os administradores também podem remover endereços de email específicos que os usuários adicionaram à lista de permissão pessoal.

Habilitar/desabilitar listas de permissão pessoais

1. Acesse **Anti-Spam > Whitelist**.



Screenshot 81: Lista de permissão pessoal

2. Selecione a guia **Personal Whitelist** e marque ou desmarque **Enable personal email whitelist** para ativar ou desativar o recurso de lista de permissão.

3. Clique em **Apply**.

Remover emails da lista de permissão pessoal dos usuários

1. Acesse **Anti-Spam > Whitelist** e selecione a guia **Personal Whitelist**.

2. Na lista suspensa **User**, selecione o usuário cujo endereço de email você deseja excluir.

3. Selecione um endereço de email na lista de endereços de email. Clique em **Remove**.

4. Clique em **Apply**.

6.1.16 Novos remetentes

O filtro Novos remetentes identifica emails que foram recebidos de remetentes para os quais emails nunca foram enviados. Para identificar esses remetentes, é preciso consultar os dados coletados na Lista de permissão.

Somente emails sem spam e cujo remetente não esteja presente em uma Lista de permissão são acionados pelo filtro New Senders.

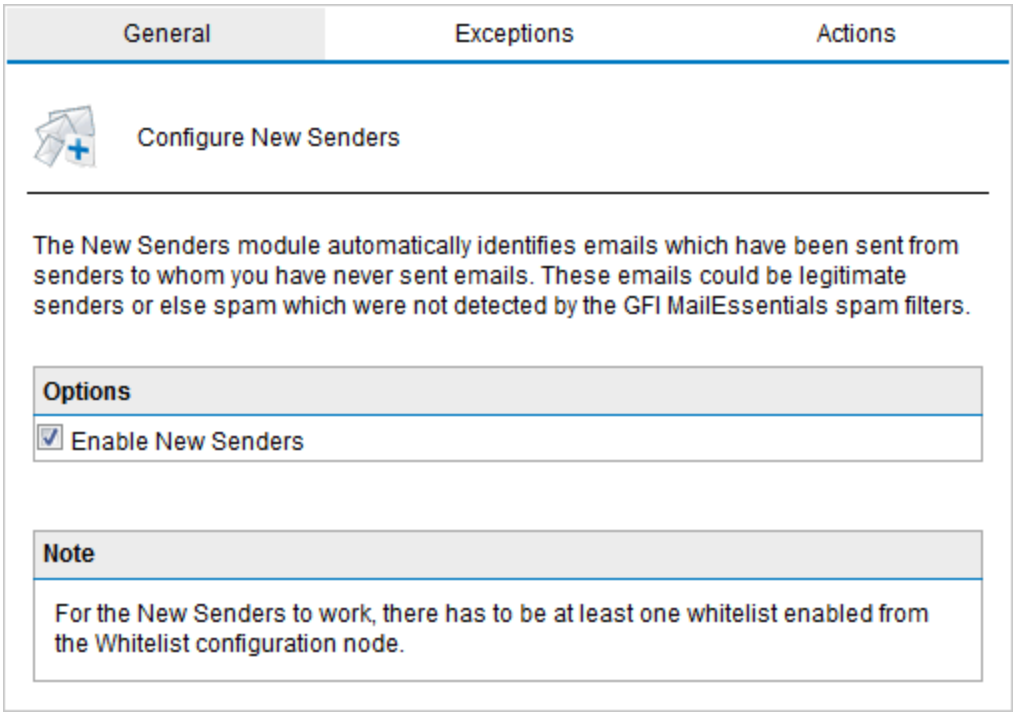
Esse filtro **NÃO** fica habilitado por padrão.

Importante

Habilite pelo menos uma das listas de permissão disponíveis para usar a função New Senders. Sem as funções da Lista de permissão (se nenhum spam for detectado pelos outros filtros), as mensagens recebidas serão entregues na caixa de entrada do destinatário. **SOMENTE** emails in which no spam was detected and whose senders are not present in the Whitelist are delivered in the New Senders folder.

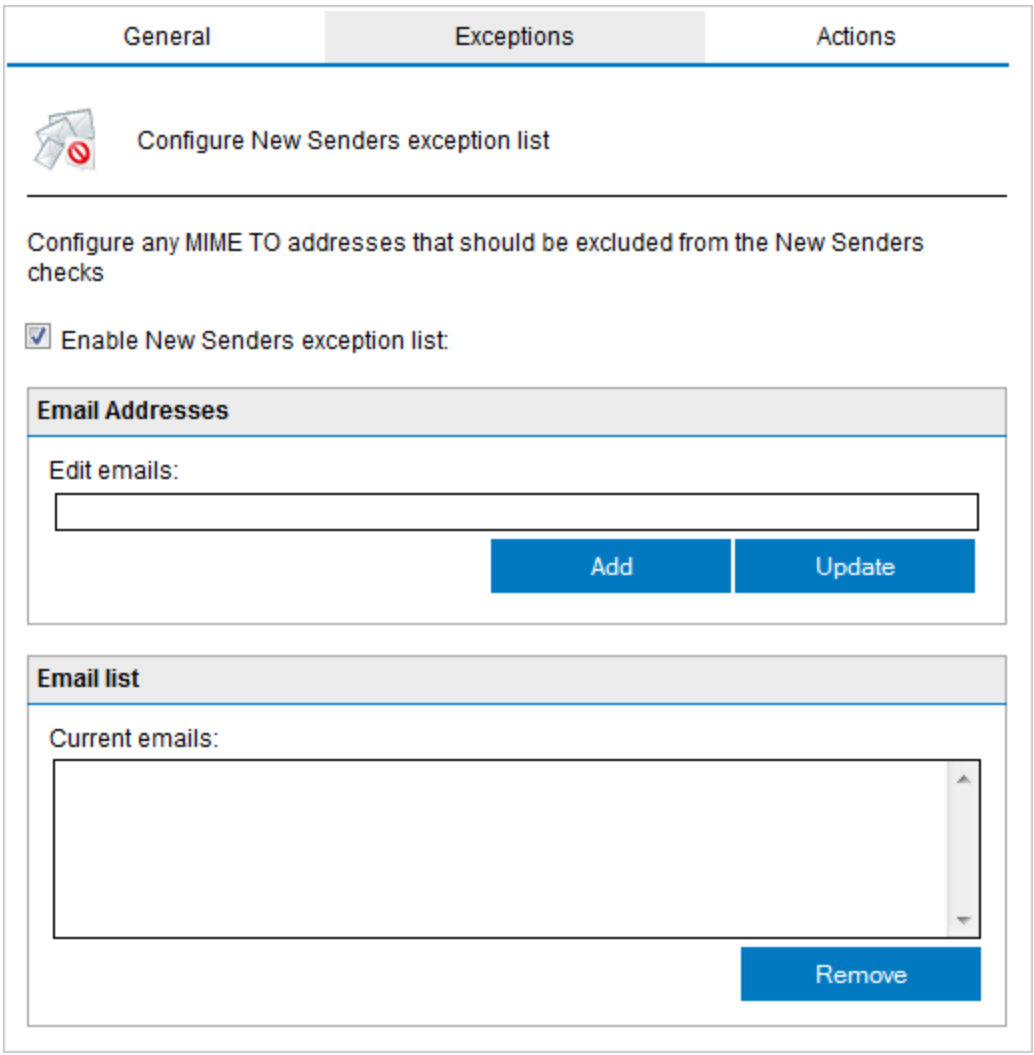
Configurar o filtro Novos remetentes

1. Acesse **Anti-Spam > New Senders.**



Screenshot 82: Guia General de Novos remetentes

2. Na guia **General**, selecione **Enable New Senders** para habilitar a verificação de novos remetentes em todas as mensagens de entrada.



Screenshot 83: Guia Exceções de Novos remetentes

3. Na guia **Exceptions**, configure remetentes/destinatários cujas mensagens são excluídas da verificação Novos remetentes.

Opção	Descrição
Enable New Senders exception list	Selecione esta opção para ativar a lista de exceções.
Adicionar exceção	Digite um endereço de email a ser excluído e clique em **Add**. Repita para cada endereço a ser adicionado.
Como editar uma exceção	1. Selecione uma exceção na **Email list**. 2. Edite o endereço de email. 3. Clique em **Update**.
Excluir uma exceção	Selecione uma exceção da **Email list** e clique em **Remove**.

4. Clique na guia **Actions** para selecionar as ações a serem executadas nas mensagens identificadas como spam. Para obter mais informações, consulte Ações de spam - O que fazer com emails de spam (página 148).

5. Clique em **Apply**.

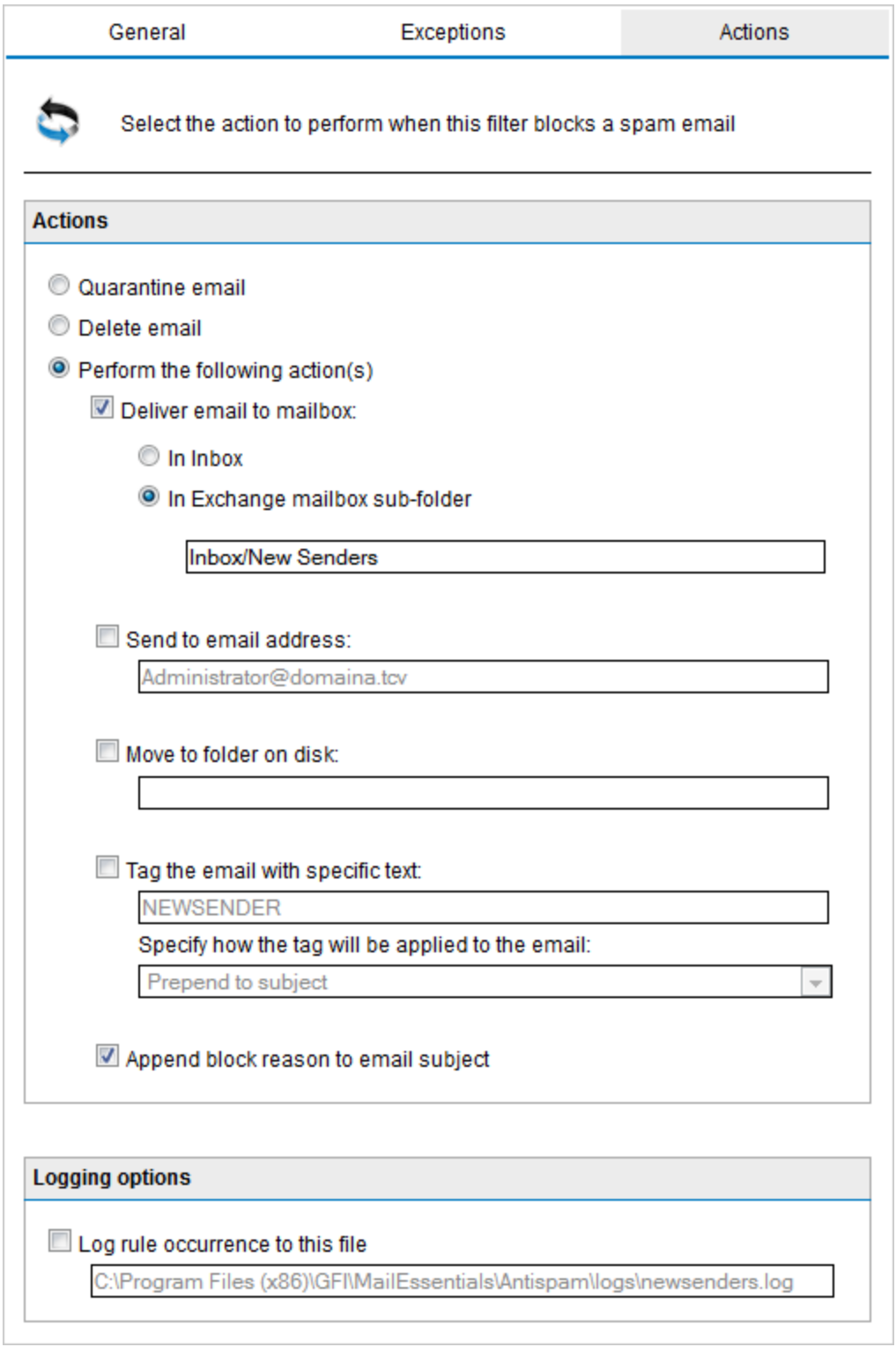
6.2 Ações de spam - O que fazer com emails de spam

A guia **Actions** nas propriedades de filtros Anti-spam define o que deve ser feito com as mensagens marcadas como spam. Ações diferentes podem ser definidas para cada um dos filtros de spam.

» **Por exemplo:** Exclua emails detectados pelo filtro SpamRazer, mas não exclua os emails marcados como spam pelo filtro Lista de bloqueio de email.

6.2.1 Configurar as ações de spam

Na guia **Actions**, selecione uma opção que defina qual ação executar em mensagens marcadas como spam.



Screenshot 84: Ações anti-spam

Ação	Descrição
Quarantine Email	Mensagens detectadas como spam são armazenadas no armazenamento da quarentena. Outras ações de spam serão desativadas se o email for colocado em quarentena. Para obter mais informações, consulte Quarentena (página 203).
Delete Email	Exclua um email bloqueado pelo filtro de spam específico. Outras ações de spam serão desativadas se o email for excluído.

Ação	Descrição
Deliver email to mailbox	Escolha a pasta para onde deseja enviar a mensagem. As opções disponíveis são: » **In Inbox**: direciona spams para a caixa de entrada do usuário » **In Exchange junk email folder**: direciona spams para a pasta Lixo Eletrônico dos usuários. Esta opção só funciona quando o GFI MailEssentials está instalado no Microsoft Exchange. Ela não está disponível para o filtro Novos remetentes. » **In Exchange mailbox sub-folder**: direciona todos os spams para uma pasta específica na caixa de correio do usuário. Digite a pasta para onde transferir as mensagens com spam. • **Exemplo 1:** Digite `Suspected Spam` para criar uma pasta personalizada no mesmo nível da pasta Inbox. • **Exemplo 2:** Digite `Inbox\Suspected Spam` para criar uma pasta personalizada na pasta Inbox. **OBS.:** Esta opção requer que: • O GFI MailEssentials esteja instalado no Microsoft® Exchange Server. Se o GFI MailEssentials não estiver instalado no Microsoft® Exchange Server, configure o servidor de email para rotear emails ou usar o Gerenciador de Regras. Para obter mais informações, consulte Transferir email de spam para as pastas da caixa de correio do usuário (página 262). • O servidor de email seja o Microsoft® Exchange Server 2003 ou Microsoft® Exchange Server 2007/2010 com a função de servidor Caixa de Correio. No Microsoft® Exchange 2010, é necessário um usuário dedicado precisa habilitar essa opção. Para obter mais informações, consulte Transferir spam para a pasta do Exchange 2010 (página 264).
Send to email address	Envie emails identificados como spam para um endereço de email específico. **Exemplo**: Encaminhe todo o spam para um endereço de email verificado por alguém que verifica as mensagens que podem ter sido marcadas equivocadamente como spam. O assunto do email terá o formato: `[recipient] [subject]`
Move to folder on disk	Salva email detectados como spam no caminho especificado **Exemplo:** `C:\Spam\` Nomes de arquivos dos emails salvos têm o seguinte formato: `[Sender_recipient_subject_number_.eml]` **Exemplo:** `C:\Spam\jim@comp.com_bob@comp.com_MailOffers_1_.eml`)
Tag the email with specific text	Selecione esta opção para adicionar uma marca ao assunto do email. Digite o texto a ser usado para a marcação e especifique onde colocar a marcação: » **Prepend to subject**: insira a etiqueta específica no início (ou seja, como um prefixo) do texto do assunto do email. **Exemplo:** `[SPAM] Email da web gratuito` » **Append to subject -**: insira a etiqueta específica no final (ou seja, como um sufixo) do texto do assunto do email. **Exemplo:** `Email da web gratuito[SPAM]` » **Add tag in an X-header...**: adicione a marca especificada como um novo cabeçalho-X ao email. Nesse caso, o cabeçalho-X terá o seguinte formato: • X-GFIME-SPAM: [TEXTO DA MARCA] • X-GFIME-SPAM-REASON: [REASON] **Exemplo:** – X-GFIME-SPAM: [É SPAM] – X-GFIME-SPAM-REASON: [Falha na verificação da Lista de bloqueio de DNS de IP: enviado pelo domínio da lista de bloqueio] **OBS.** O gerenciador de regras pode ser usado para transferir emails quando esse recurso for usado.

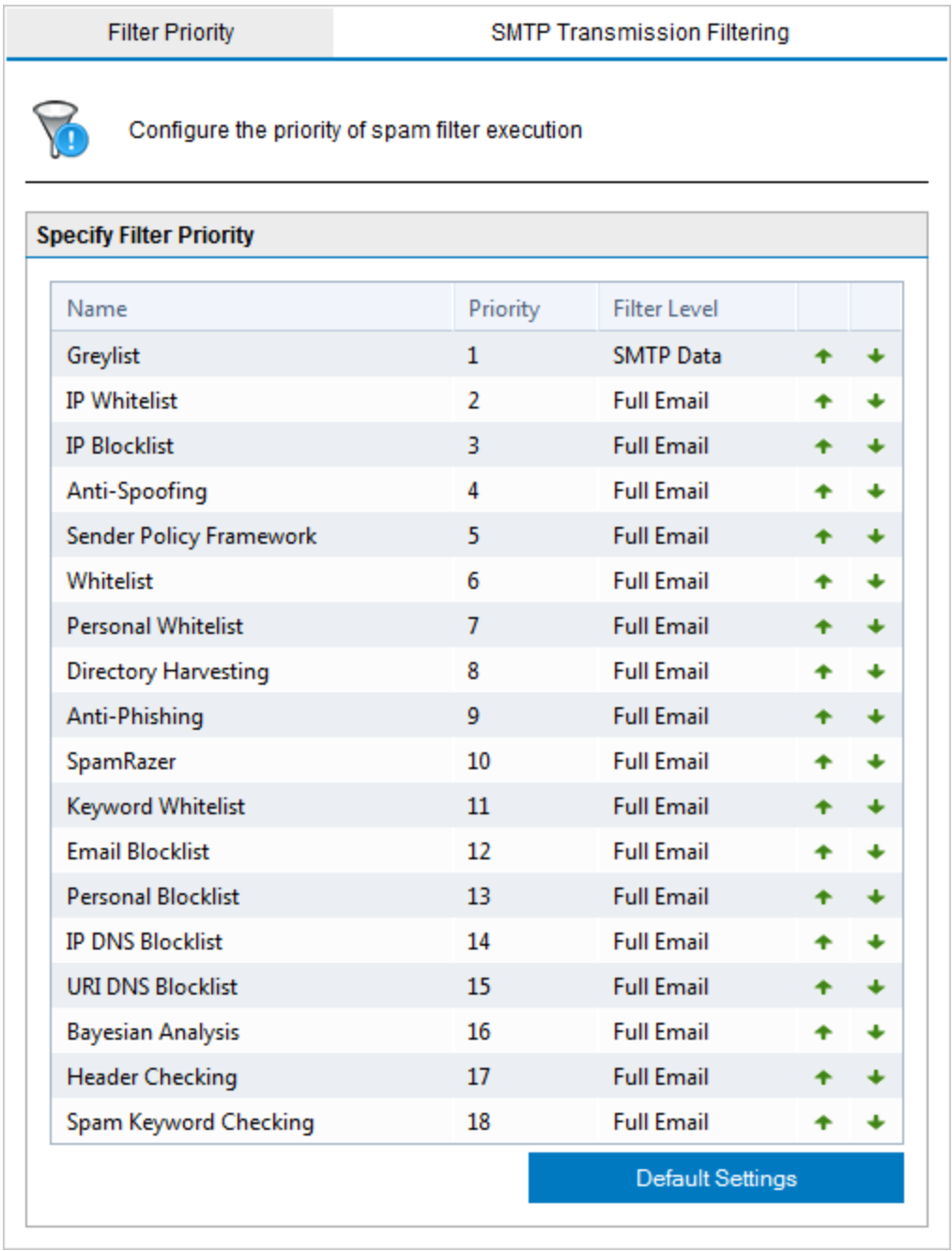
Ação	Descrição
Append block reason to email subject	Se esta opção for habilitada, o nome do filtro que bloqueou a mensagem de email e o motivo do bloqueio serão colocados no assunto do email.
Log rule occurrence to this file	Registre a ocorrência de email de spam em um arquivo de registro de sua escolha. Por padrão, os arquivos de registro são armazenados em: *<GFI MailEssentials installation path>*\GFI\MailEssentials\AntiSpam\Logs\<nome do filtro>.log **OBS.** Arquivos de registro podem ficar muito grandes. GFI MailEssentials habilita a rotação de registros, na qual novos arquivos de registro são criados periodicamente ou quando o arquivo de registro atinge um tamanho específico. Para habilitar a rotação de arquivo de registro, acesse **Anti-Spam > Anti-Spam Settings**. Selecione a guia **Anti-spam logging** e marque a rotação **Enable log file**. Especifique a condição da rotação por tempo ou tamanho do arquivo.

6.3 Classificar filtros anti-spam por prioridade

No GFI MailEssentials, a ordem na qual as verificações anti-spam são aplicadas às mensagens de entrada pode ser personalizada.

> **OBS.**
> A ordem dos filtros disponíveis pode ser personalizada, exceto para o filtro **New Senders**, que é sempre configurado automaticamente com a prioridade mais baixa. Isso acontece devido a sua dependência nos resultados das verificações da Lista de permissão e dos outros filtros de spam.
> A prioridade padrão é recomendada na maioria dos casos.

1. Acesse **Anti-Spam > Filter Priority**.



Screenshot 85: Atribuir prioridades de filtro

2. Selecione um filtro e clique no botão ↑ (up) para atribuir uma prioridade maior ou clique no botão ↓ (down) para atribuir uma prioridade mais baixa.

> **OBS.**
> Clique em **Default Settings** para restaurar os filtros para o padrão.

3. Clique em **Apply**.

6.4 Filtragem da transmissão SMTP

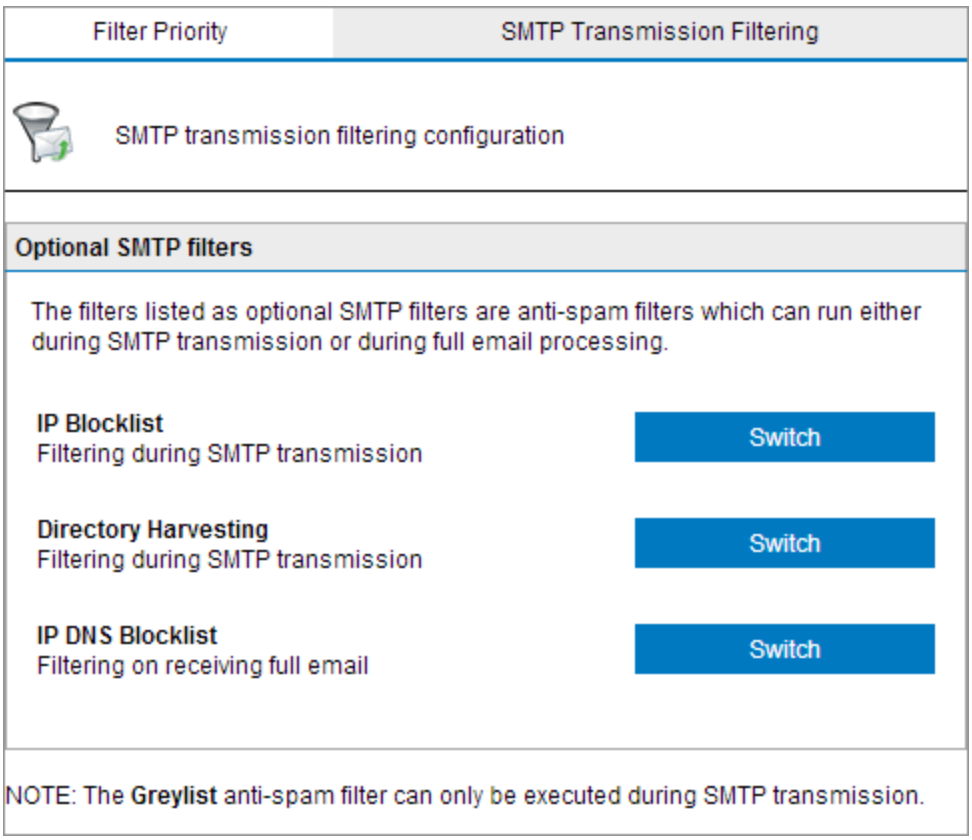
Em GFI MailEssentials, alguns filtros anti-spam podem ser configurados para serem executados quando o email completo for recebido ou no nível de transmissão SMTP. Na filtragem da transmissão SMTP, os

emails são examinados enquanto são recebidos.

A filtragem no nível do SMTP encerra a conexão do email e interrompe o download do email completo, economizando largura de banda e recursos de processamento. Nesse caso, a conexão foi encerrada imediatamente e os emails não precisam passar por nenhum outro filtro de spam.

> **IMPORTANTE**
> Para fazer a melhor filtragem da transmissão de SMTP, use-a quando o GFI MailEssentials for instalado em um gateway de Internet ou quando ele for o primeiro servidor a receber emails da Internet.

1. Acesse **Anti-Spam > Filter Priority** e selecione a guia **SMTP Transmission Filtering**.



Screenshot 86: Propriedades da filtragem de transmissão SMTP

2. Clique no botão **Switch** para ativar ou desativar a filtragem da coleta de diretório:

Opção	Descrição
Filtering on receiving full email	A filtragem é feita quando todo o email é recebido.
Filtering during SMTP transmission	A filtragem é feita durante a transmissão SMTP. Se esta opção estiver marcada, o filtro será executado sempre antes dos outros tipos de filtros de spam.

> **OBS.**
> O filtro Lista de exclusão temporária é executado somente no nível da transmissão SMTP.

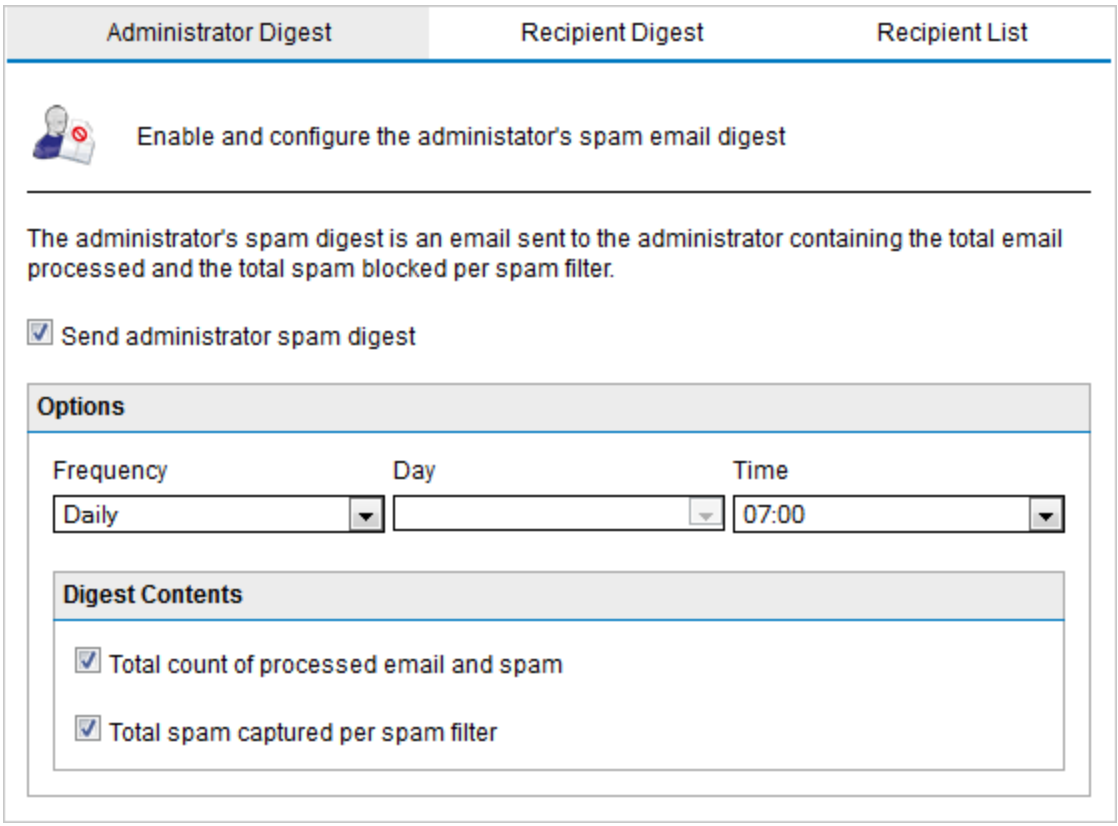
3. Clique em **Apply**.

6.5 Resumo de spam

O resumo de spam é um pequeno relatório enviado para um administrador ou usuário por email. Esse relatório mostra o número total de emails processados pelo GFI MailEssentials e o número de mensagens de emails de spam bloqueados em um determinado período de tempo (desde o último resumo de spam).

6.5.1 Configurar resumos de spam: resumo do administrador de spam

1. Acesse **Anti-Spam > Spam Digest**.



Screenshot 87: Resumo das propriedades de spam/ resumo do administrador de spam

2. Na guia **Administrator Digest**, clique em **Send administrator spam digest** para ativar o resumo de spam.

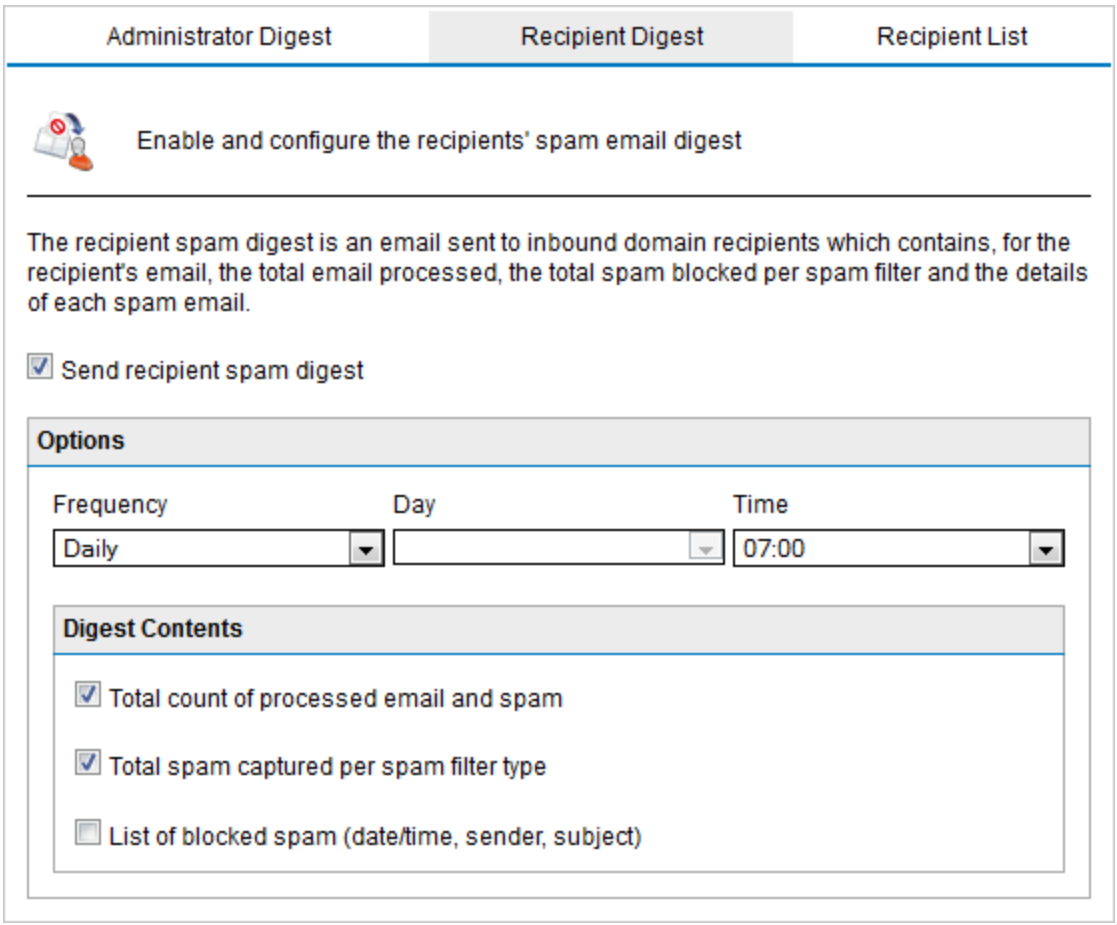
3. Configure a frequência de envio desejada (diariamente, semanalmente, mensalmente) e especifique uma data e uma hora para o envio de emails.

4. Especifique o conteúdo do resumo que será enviado no email, um **Total count of processed email and spam** ou **Total spam captured per spam filter** ou ambos.

5. Finalize as configurações selecionando **Apply**.

6.5.2 Configurar resumos de spam: resumo do destinatário de spam

1. Acesse **Anti-Spam > Spam Digest**.



Screenshot 88: Resumo do destinatário de spam

2. Na guia **Recipient Digest**, selecione **Send recipient spam digest** para ativar o resumo de spam.

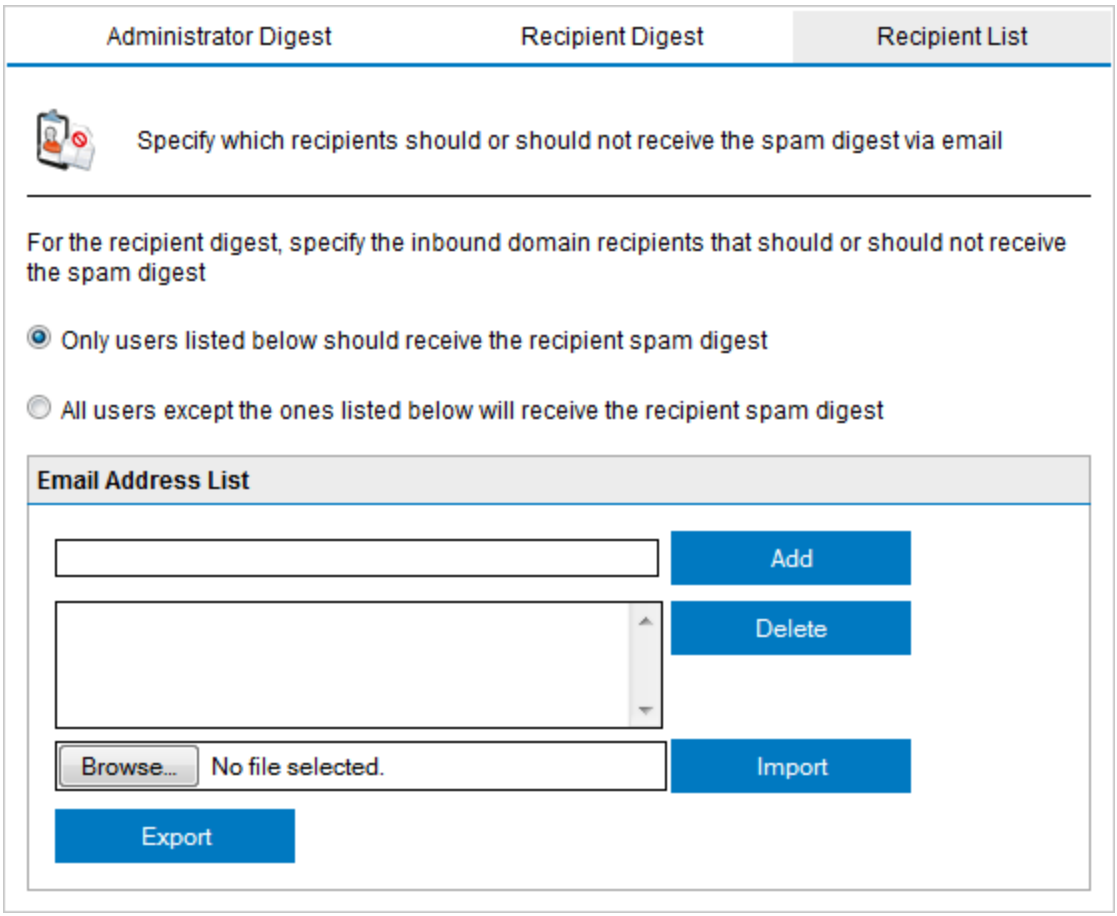
3. Configure a frequência de envio desejada (diariamente, semanalmente, mensalmente) e especifique uma data e uma hora para o envio de emails.

4. Especifique o conteúdo do resumo que será enviado no email:

» Total de emails e spam processados

» Total de spam captado pelo tipo de filtro de spam

» A lista de spam bloqueada ou qualquer combinação de opções conforme necessário.



Screenshot 89: Lista de destinatários do resumo de spam

4. Clique na guia **Recipients list**, adicione os usuários que recebem o resumo de spam e selecione o método usado para determinar quem deve receber o resumo de spam.

As opções disponíveis são:

» Apenas os usuários listados abaixo devem receber o resumo de destinatário de spam.

» Todos os usuários, exceto aqueles listados abaixo, receberão o resumo de destinatário de spam.

> **OBS.**
> A lista de usuários exigida também pode ser importada de um arquivo no formato XML na mesma estrutura que o GFI MailEssentials exportaria os arquivos.

6. Selecione **Apply** para finalizar as configurações.

6.6 Configurações anti-spam

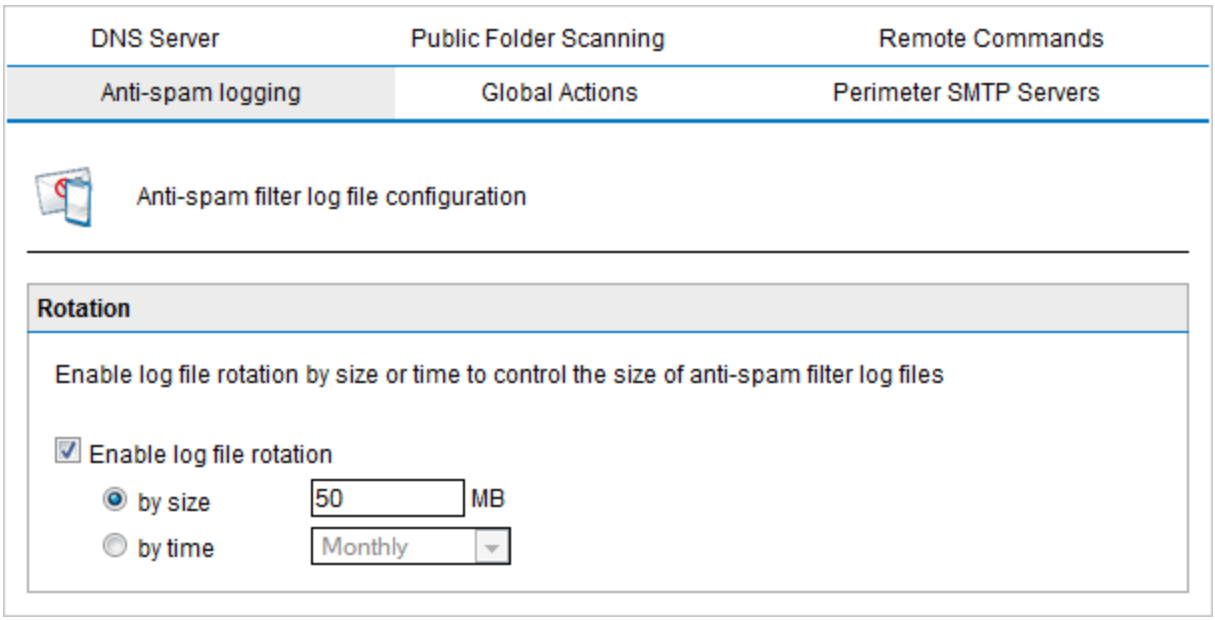
As seguintes configurações podem ser definidas para filtros de spam e emails bloqueados somente por filtros de spam.

6.6.1 Rotação do arquivo de registro

Ao longo do tempo, os arquivos de registro podem ficar muito grandes. GFI MailEssentials habilita a rotação de registros, na qual novos arquivos de registro são criados periodicamente ou quando o arquivo de registro atinge um tamanho específico.

Para ativar a rotação do arquivo de registro:

1. Acesse **Anti-Spam > Anti-Spam Settings**.



Screenshot 90: Rotação do arquivo de registro

2. Na guia **Anti-spam logging**, marque **Enable log file rotation** e especifique a condição da rotação (**by size** ou **by time**).

3. Forneça o tamanho ou valores de horário e clique em **Apply**.

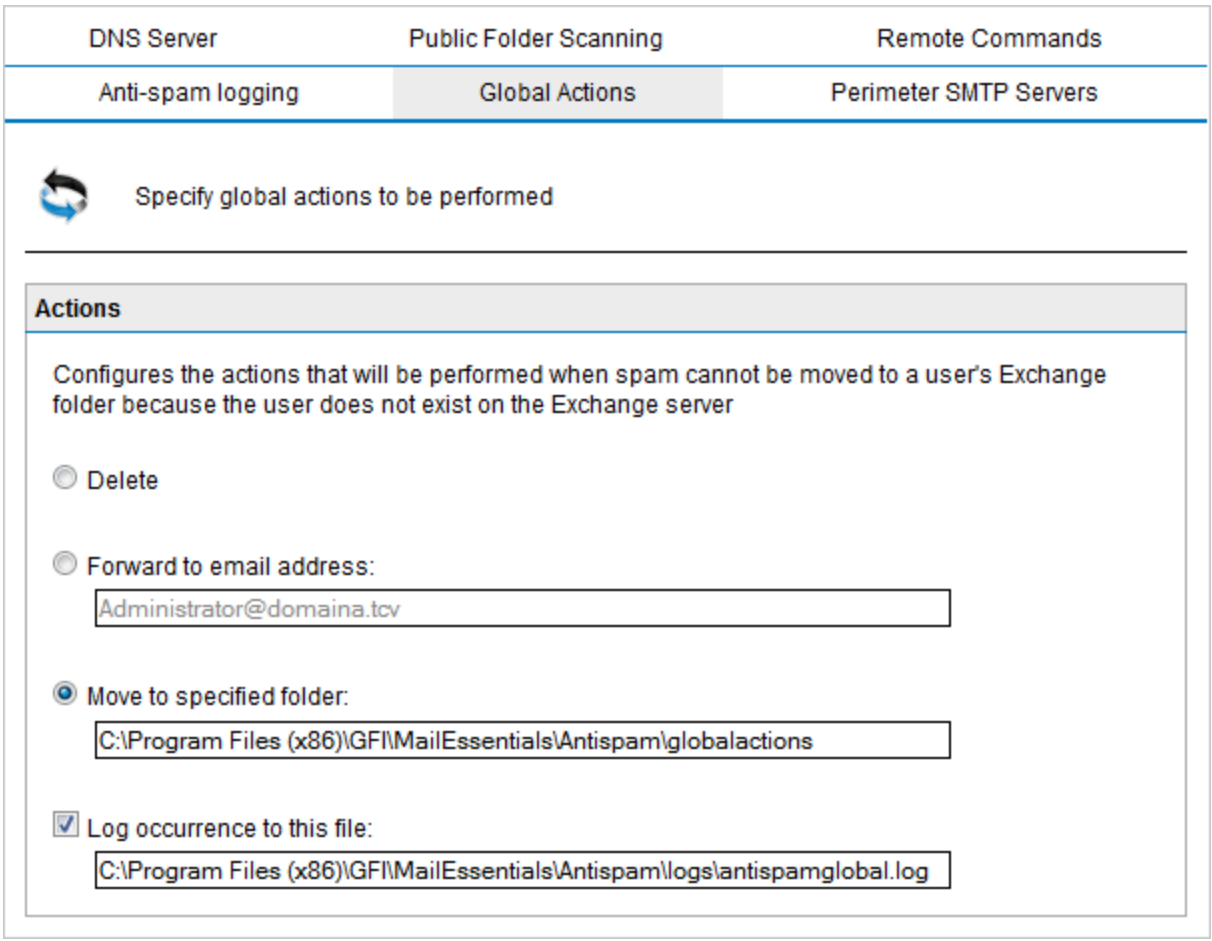
6.6.2 Ações anti-spam globais

Um conjunto de spam é enviado para endereços de email que não existem mais. Geralmente, esses emails são simplesmente excluídos. No entanto, para a resolução de problemas ou fins de avaliação, você pode colocar as mensagens em uma pasta ou encaminhá-las para um determinado endereço de email.

> **OBS.**
> Esta seção se aplica apenas a instalações no Microsoft® Exchange Server nas quais a ação **Move to subfolder of user's mailbox** está habilitada. Para obter mais informações, consulte Ações de spam - O que fazer com emails de spam (página 148).
> Em outros servidores de email, a guia ações anti-spam globais não será exibida.

Configurar as ações anti-spam globais

1. Acesse **Anti-Spam > Anti-Spam Settings**.



Screenshot 91: Ações globais

2. Selecione a guia **Global Actions** e escolha se deseja:

» Excluir o email

» Encaminhá-lo para um endereço de email

» Movê-lo para uma pasta especificada.

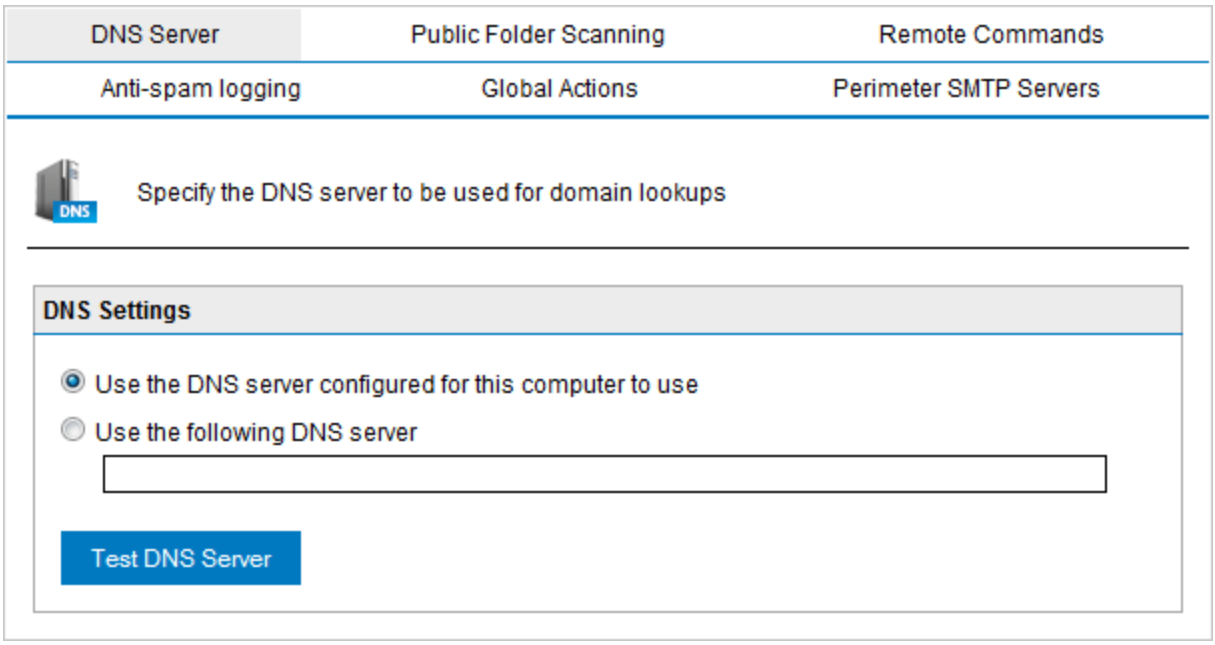
3. Selecione **Log occurrence to this file** para registrar as ocorrências em um arquivo de registro.

4. Clique em **Apply**.

6.6.3 Configurações do servidor DNS

Configurações do servidor DNS são muito importantes no GFI MailEssentials pois vários filtros anti-spam, tais como IP DNS Blocklist, URI DNS Blocklist and SpamRazer, realizam pesquisas de domínio quando filtram spam.

1. A partir deGFI MailEssentials Configuration, acesse **Anti-Spam > Anti-Spam Settings**.



Screenshot 92: Configurações do servidor DNS

1. Na guia **DNS Server** configure:

Opção	Descrição
Use the DNS server configured for this computer to use	Selecione esta opção para usar o mesmo servidor DNS usado pelo sistema operacional no qual o GFI MailEssentials está instalado.
Use the following DNS server	Selecione esta opção para definir um servidor DNS que seja diferente daquele usado pela máquina local.

2. Clique em **Test DNS Server** para testar a conexão com o servidor DNS indicado. Se isso não funcionar, especifique outro servidor DNS.

3. Clique em **Apply**.

6.6.4 Comandos remotos

Comandos remotos facilitam a adição de domínios ou endereços de email aos filtros Lista de bloqueio/Lista de permissões de email e atualizam o filtro Bayesian com spam ou não spam (emails válidos).

Comandos remotos funcionam enviando um email para o GFI MailEssentials. Endereçar um e-mail para **rcommands @mailessentials.com** (configurável) faz com que o GFI MailEssentialsreconheça que o email contém comandos remotos e os processa conforme descrito abaixo.

Com comandos remotos, as seguintes tarefas podem ser executadas:

1. Adicionar spam ou não spam ao banco de dados da Análise bayesiana.

2. Adicionar palavras-chave ao recurso da verificação de palavras-chave do assunto e ao recurso de verificação de palavras-chave do corpo.

3. Adicionar endereços de email ao filtro Lista de bloqueio/Lista de permissão de emails.

Configurar comandos remotos

1. Clique em **Anti-Spam > Anti-Spam Settings**, acesse a guia **Remote Commands** e selecione **Enable remote commands**.

2. Edite o endereço de email para o qual os comandos remotos devem ser enviados.

> **OBS.**
> O endereço de email **NÃO** deve ser um domínio local. O endereço padrão é **rcommands@mailessentials.com**. Não é preciso ter uma caixa de correio para o endereço configurado, mas a parte do domínio do endereço deve ser um domínio de endereço de email real que retorne um resultado positivo para uma pesquisa de registro MX via DNS. Essa também pode ser uma conta de email pública que você pode gerenciar (por exemplo, Gmail ou Yahoo Mail)

3. Opcionalmente, configure segurança básica para comandos remotos:

» Uma senha compartilhada para incluir na mensagem de email. Para obter mais informações, consulte Usar comandos remotos (página 160).

» Quais usuários têm permissão de enviar emails com comandos remotos.

4. Clique em **Apply**.

Usar comandos remotos

Comandos remotos podem ser enviados por email para oGFI MailEssentials a partir de um cliente de email no domínio. Condições para enviar comandos remotos:

» A mensagem de email deve estar em formato de texto simples

» O assunto do email é ignorado

» A seguinte sintaxe deve ser usada para todos os comandos:

```
<nome do comando>: <parâmetro1>, <parâmetro2>, <parâmetro3>, … ;
```

Por exemplo:`ADDBLIST: spammer@spam.com;`

» Pode haver mais de um comando no corpo de uma mensagem de email, com cada comando separado por um ponto-e-vírgula (;).

» Se uma senha for configurada para comandos remotos, digite a senha na primeira linha usando a seguinte sintaxe:

```
PASSWORD: <senha compartilhada>;
```

» Os nomes dos comandos diferenciam maiúsculas de minúsculas e devem ser escritos apenas em MAIÚSCULAS.

» Condições como `IF, AND, OR` não são compatíveis.

» Comandos remotos somente podem ser usados para adicionar entradas, e não para excluir ou modificar entradas existentes.

Comandos de palavra-chave

Use comandos de palavras-chave para adicionar palavras-chave ou uma combinação de palavras-chave na listas de corpo e de assunto no filtro de verificação de palavras-chave.

Comandos disponíveis:

» ADDSUBJECT - Adiciona as palavras-chave especificadas para o banco de dados de verificação de palavras-chave do assunto.

- Exemplo: ADDSUBJECT: sexo, pornô, spam;

» ADDBODY - Adiciona as palavras-chave especificadas para o banco de dados de verificação de palavras-chave do corpo.

- Exemplo: ADDBODY : gratuito, "100% free", "absolutamente grátis";

> **OBS.**
> Ao configurar frases em vez de palavras, coloque-as entre aspas (" ").

Comandos da lista de bloqueio

Use os comandos da lista de bloqueio para adicionar um único endereço de email ou um domínio inteiro à lista de bloqueio por email.

Comandos disponíveis:

» `ADDBLIST: <e-mail>;`

- Exemplo: `ADDBLIST: usuario@somewhere.com;`

> **OBSERVAÇÕES**
> 1. Adicione um domínio inteiro para a lista de bloqueio especificando um curinga antes do domínio
>
> **Exemplo**: `ADDBLIST: *@domain.com;`
>
> 2. Curingas não podem ser usados em nomes de domínio.
>
> **Exemplo:**`ADDBLIST: *@*.dominio.com;` é inválido e será rejeitado.
>
> 3. Por razões de segurança, só pode haver um comando `ADDBLIST` em um email, e apenas um endereço pode ser especificado como o parâmetro do comando. O parâmetro é um usuário de email ou um domínio:
>
> **Exemplo:**`ADDBLIST: spammer@spam.com;` ou `ADDBLIST:*@spammers.org;`

Comandos do filtro Bayesiano

Adicione email de spam ou email válido (ham) ao banco de dados do filtro Bayesiano. Comandos disponíveis:

Comando	Descrição
ADDASSPAM	Instrui o filtro Bayesiano a classificar emails como spam.
ADDAGOODMAIL	Instrui o filtro Bayesiano a classificar emails como não spam.

> **OBS.**
> Esses comandos não tem parâmetros. O conteúdo do e-mail é o parâmetro.

Registro do comando remoto

Para manter um registro das alterações feitas no banco de dados de configuração por meio de comandos remotos, cada email com comandos remotos (mesmo se o email com comandos remotos for inválido) será salvo em:

<GFI MailEssentials installation path>\GFI\MailEssentials\AntiSpam\ADBRProcessed\

O nome do arquivo de cada email é formatado de acordo com o seguinte formato:

» <endereço_de_e-mail_do_remetente>_SUCCESS_<carimbo_de_data/hora>.eml - em caso de processamento bem-sucedido.

» <endereço_de_e-mail_do_remetente>_FAILED_<carimbo_de_data/hora>.eml - em caso de falha.

OBS.
O carimbo de data e hora é formatado como aaaammddhhmmss.

6.7 SpamTag para Microsoft Outlook

O plug-in SpamTag do GFI MailEssentialsé um complemento do Microsoft Outlook que instala uma barra de ferramentas nas máquinas dos usuários finais, oferecendo algum controle para os usuários no que se refere ao gerenciamento de emails com spam. O plug-in também sincroniza as configurações de Lixo Eletrônico do Microsoft Outlook com o GFI MailEssentials.

Embora a funcionalidade Lixo Eletrônico do Microsoft Outlook permita aos usuários gerenciar emails com spam no cliente, com o plug-in SpamTag, os usuários podem gerenciar emails com spam no nível do servidor.

O administrador do GFI MailEssentials pode escolher quais dos seguintes recursos e funções serão habilitados:

» Treinar o filtro de análise bayesiana

» Adicionar remetentes e/ou domínios à Lista de bloqueio pessoal ou Lista de permissão pessoal

» Sincronize automaticamente os remetentes permitidos e bloqueados no Microsoft Outlook com a Lista de permissão pessoal e a Lista de bloqueio pessoal do GFI MailEssentials, respectivamente.

» Adicione automaticamente os contatos dos usuários à Lista de permissão pessoal.

OBS.
Usuários com acesso total ao GFI MailEssentials também podem adicionar remetentes/domínios à Lista de bloqueio e à Lista de permissão pessoais do GFI MailEssentials.

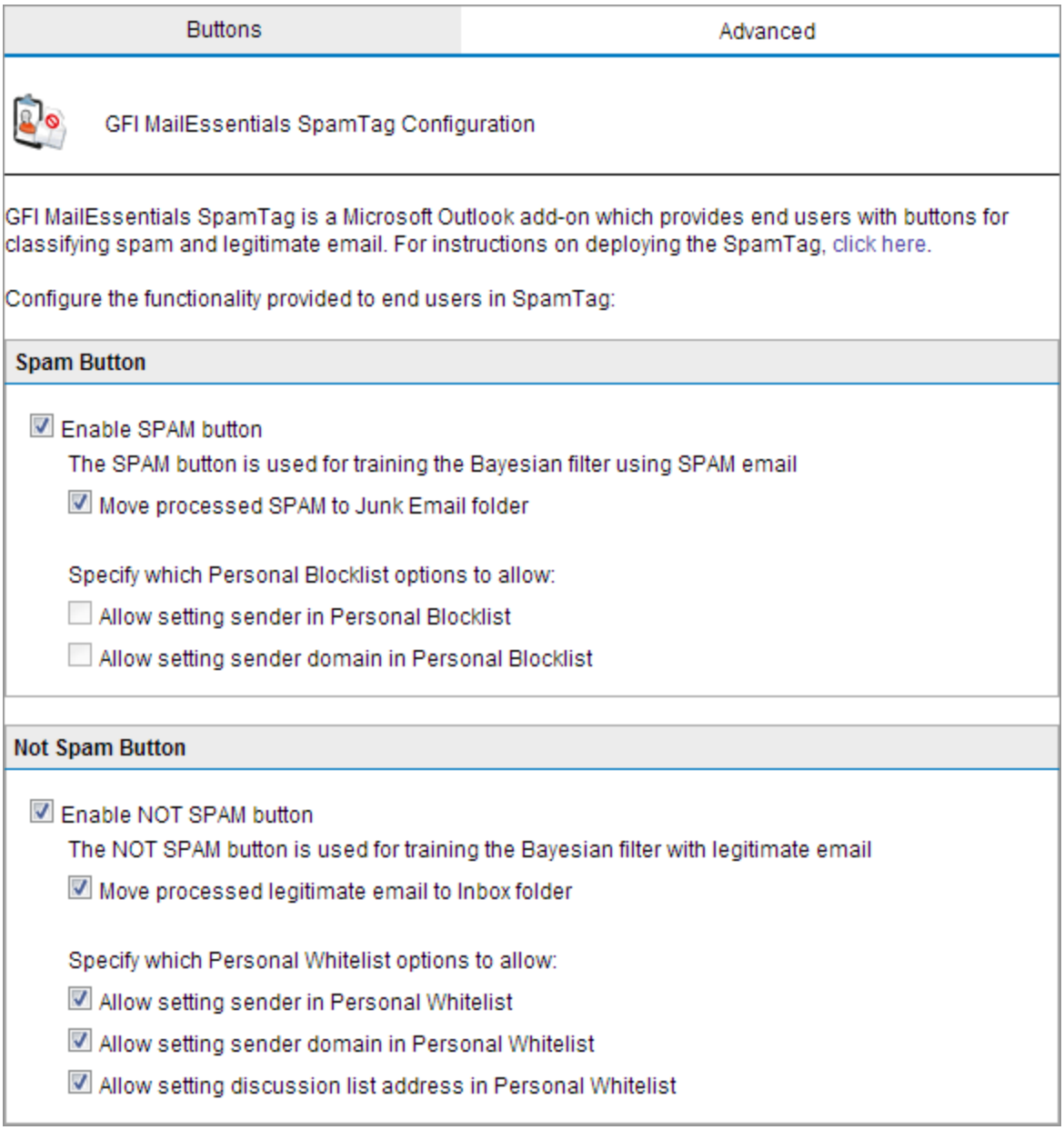
OBS.
Quando usar o SpamTag, instale WCF HTTP Activation no servidor do GFI MailEssentials. Para fazer isso, acesse **Server Manager > Features > Add Feature > .NET Framework > WCF Activation > HTTP Activation**.

6.7.1 Escolher os recursos do SpamTag

O administrador do GFI MailEssentials pode configurar quais recursos do SpamTag os usuários podem usar. Por exemplo, o administrador pode habilitar os usuários para adicionar remetentes à lista de permissão pessoal, mas desabilitar a adição de domínios à lista de permissão pessoal. O SpamTag também pode ser configurado para substituir os recursos do Lixo Eletrônico do Microsoft Outlook.

Para configurar os recursos do Spamtag:

1. Acesse **Anti-Spam > SpamTag.**



2. Na área **Spam Button**, configure os recursos relacionados a falsos negativos, isto é, quando emails com spam não são detectados como spam:

Opção	Descrição
Enable SPAM button	O botão **Spam** é mostrado no SpamTag e, quando é clicado, os emails selecionados treinam o filtro Análise bayesiana.
Move processed SPAM to Junk Email folder	Ao clicar em **Spam**, o email selecionado é automaticamente movido para a pasta Lixo Eletrônico do Microsoft Outlook.
Allow setting sender in Personal Blocklist	Uma subopção é mostrada no botão **Spam** que permite que os usuários adicionem o endereço de email do remetente à Lista de bloqueio pessoal. Para usar esta opção, a Personal Blocklist deve estar habilitada.
Allow setting sender domain in Personal Blocklist	Uma subopção é mostrada no botão **Spam** que permite que os usuários adicionem o domínio do remetente à Lista de bloqueio pessoal. Para usar esta opção, a Personal Blocklist deve estar habilitada.

3. Na área **Not Spam Button**, configure os recursos relacionados a falsos positivos, isto é, quando emails legítimos são incorretamente identificados como spam:

Opção	Descrição
Enable NOT SPAM button	O botão **Not Spam** não é mostrado no SpamTag e, quando clicado, o email selecionado treina o filtro Análise bayesiana.
Move processed legitimate email to Inbox folder	Ao clicar em **Not Spam**, o email selecionado é automaticamente movido para a pasta Caixa de entrada.
Allow setting sender in Personal Whitelist	Uma subopção é mostrada no botão **Not Spam** que permite que os usuários adicionem o endereço de email do remetente à Lista de permissão pessoal. Para habilitar esta opção, a Personal Whitelist deve estar habilitada.
Allow setting sender domain in Personal Whitelist	Uma subopção é mostrada no botão **Not Spam** que permite que os usuários adicionem o domínio do remetente à Lista de permissão pessoal. Para habilitar esta opção, a Personal Whitelist deve estar habilitada.
Allow setting discussion list address in Personal Whitelist	Uma subopção é mostrada no botão **Not Spam** que permite que os usuários incluam boletins informativos/listas de discussões à lista de permissão. Para habilitar esta opção, a Personal Whitelist deve estar habilitada.

4. Na guia **Avançado**, configure as seguintes opções avançadas:

Opção	Descrição
Import Outlook Junk Settings to Personal Blocklist and Personal Whitelist	Importar os endereços listados nos Remetentes Confiáveis e Remetentes Bloqueados do Microsoft Outlook para a Lista de permissão pessoalt e Lista de bloqueio pessoal do GFI MailEssentials. A lista de Remetentes Confiáveis e Remetentes Bloqueados do Microsoft Outlook está disponível nas opções de **Lixo > Lixo eletrônico**. **OBS.:** As importações são feitas automaticamente em segundo plano pelo SpamTag a cada duas horas, e o usuário não configura nem vê opções na tela. **OBS.:** Quando o usuário utiliza o Microsoft Outlook instalado em um dispositivo carregado por bateria, como um laptop ou tablet, a sincronização automática não é feita para economizar a bateria.
Import Outlook contacts to Personal Whitelist	Importa a lista de contatos do Microsoft Outlook para a Lista de permissão pessoal. **OBS.:** As importações são feitas automaticamente em segundo plano pelo SpamTag a cada duas horas, e o usuário não configura nem vê opções na tela. **OBS.:** Quando o usuário utiliza o Microsoft Outlook instalado em um dispositivo carregado por bateria, como um laptop ou tablet, a sincronização automática não é feita para economizar a bateria.
Override Microsoft Outlook Junk	Quando você seleciona essa opção, as opções habilitadas no SpamTag substituem as configurações equivalentes no Lixo Eletrônico do Microsoft Outlook para garantir que apenas um sistema de gerenciamento anti-spam seja utilizado pelo cliente. Quando o usuário utiliza uma opção do Lixo Eletrônico do Microsoft Outlook, uma função do SpamTag é executada em seu lugar. Por exemplo, se o usuário clicar em **Nunca Bloquear Remetente** no Lixo Eletrônico do Outlook, a função **Não é spam** do SpamTag será executada em seu lugar. **OBS.:** Se uma determinada opção não estiver habilitada no SpamTag, e o usuário utilizar a função equivalente no Outlook, nenhuma ação será executada quando a função do Lixo Eletrônico do Outlook for usada. Por exemplo, se o botão Não é spam não estiver habilitado, nada acontecerá quando o usuário clicar em **Nunca Bloquear Remetente**.
Hide the Console button	Oculta o botão Console da barra de ferramentas do SpamTag. Não há acesso direto ao console do GFI MailEssentials, mas o usuário pode fazer login digitando a URL em um navegador. As configurações fornecidas ao usuário no console do GFI MailEssentials dependem das permissões do Active Directory ou de outras configurações de controle de acesso personalizadas. Para obter mais informações, consulte Controle de acesso (página 247).

5. Clique em **Apply**.

IMPORTANTE

O SpamTag verifica quais recursos estão habilitados ou desabilitados no GFI MailEssentials quando o Microsoft Outlook é iniciado. Depois de alterar qualquer uma das configurações acima, o Microsoft Outlook precisará ser reiniciado para aplicar as alterações.

6.7.2 Requisitos do SpamTag

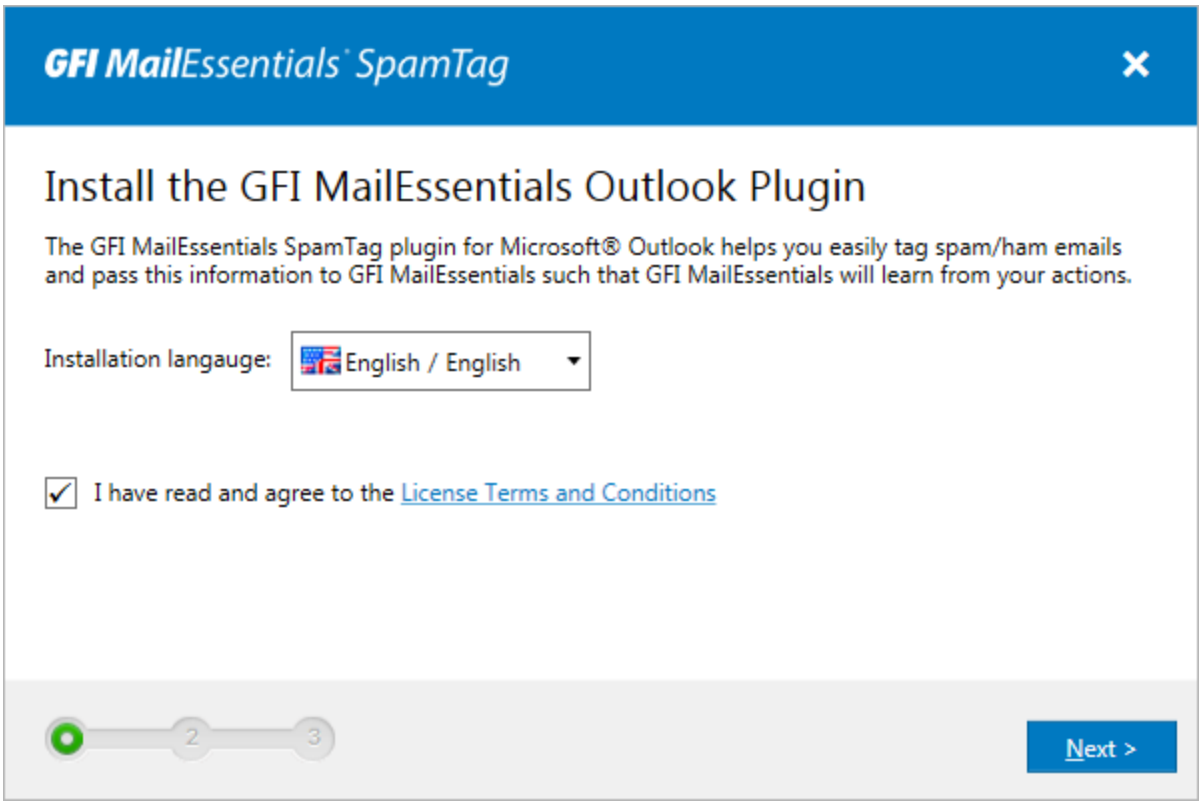
As máquinas nas quais o SpamTag será instalado devem ser compatíveis ou superar as seguintes especificações:

Hardware	» Processador - 1 GHz ou mais » Memória - Mínimo de 512 MB, recomenda-se 2 GB » Armazenamento físico - Armazenamento físico de 50 MB dedicado para o SpamTag
Sistemas operacionais compatíveis	» Windows® 8 e 8.1 » Windows® 7 » Windows® Vista » Windows® XP » Windows® Server 2012 » Windows® Server 2008 » Windows® Server 2003
Versões compatíveis do Microsoft Outlook®	» Microsoft Outlook® 2013 » Microsoft Outlook® 2010 » Microsoft Outlook® 2007 » Microsoft Outlook® 2003
Conexão com GFI MailEssentials	O SpamTag estabelece uma conexão com o GFI MailEssentials na porta 80 por HTTP. Para confirmar a conexão, no navegador do cliente, certifique-se de que você abriu o URL do GFI MailEssentials.
Outros softwares	Microsoft .Net Framework 4 - é obtido por download e instalado automaticamente se não for encontrado.

6.7.3 Instalar o SpamTag manualmente

Execute o instalador do SpamTag nas máquinas do cliente para instalar o SpamTag manualmente.

1. Obtenha o instalador em **<GFI MailEssentials pasta de instalação>/Outlook**.
2. Copie **GFIMailEssentialsSpamTag.exe** na máquina onde instalará o SpamTag.
3. Feche o Microsoft Outlook.
4. Clique com o botão direito do mouse no arquivo e selecione **Run as administrator**.
5. Na primeira tela, selecione o idioma de instalação.



Screenshot 93: Idioma de instalação e termos de licença do SpamTag

6. Leia os **License Terms and Conditions** e, se concordar, selecione **I have read and agree to the License Terms and Conditions**. Clique em **Next**.

7. Digite o URL usado para estabelecer uma conexão com o GFI MailEssentials. Por exemplo: `http://192.168.1.2/MailEssentials` ou `http://myg-fiserver.mydomin.com/MailEssentials`. Aguarde o instalador para verificar a conexão com o GFI MailEssentials por meio de um URL especificado e clique em **Next**.

8. Especifique o local onde instalar o SpamTag e clique em **Install**.

9. Quando terminar, clique em **Finish**.

10. Inicie o Microsoft Outlook e digite as credenciais do usuário.

O SpamTag está disponível na faixa de opções do Microsoft Outlook Home (versão 2007 em diante) ou na barra de ferramentas (versão 2003).

Para obter mais informações, clique em **Help** no SpamTag.

6.7.4 Instalar o SpamTag via GPO

Esta seção irá ajudá-lo a instalar o GFI MailEssentials SpamTag em várias máquinas automaticamente via GPO. Escolha o ambiente do controlador de domínio:

» Windows Server 2008 e 2012

» Windows Server 2003

Instalar o SpamTag via GPO no Windows Server 2008 e 2012

Etapa 1: Preparar arquivos MSI e ADM

1. No servidor do GFI MailEssentials, acesse a pasta de instalação do GFI MailEssentials e abra a subpasta **Outlook**.

2. Copie os arquivos MSI e ADM em uma pasta compartilhada que possa ser acessada por todos os usuários que instalem o SpamTag. Certifique-se de que os usuários tenham pelo menos os direitos de leitura da pasta.

Etapa 2: Implantar o SpamTag

1. No controlador de domínio, abra o **Server Manager**.

2. Expanda **Server Manager > Features > Group Policy Management > Forest > Domains > *domain name***. Clique com o botão direito do mouse no nome de domínio ou uma unidade organizacional e selecione **Create a GPO in this domain, and Link it here...**

3. Digite um nome para o novo Objeto de Política de Grupo (GPO). Por exemplo: `GFI MailEssentials SpamTag`. Clique em **OK**.

4. Clique com o botão direito do mouse no GPO recém-criado e clique em **Edit**.

5. Na janela **Group Policy Management Editor**, expanda **Computer Configuration > Policies > Software settings > Software Installation**. Clique com o botão direito do mouse em **Software Installation > New > Package** para configurar o GPO para ser instalado no login.

6. Digite o caminho de rede da pasta compartilhada que contém o pacote MSI do SpamTag. Clique em **OK**.

> **OBS.**
> Quando selecionar o local do arquivo MSI, certifique-se de que isso seja feito em "Meus locais de rede" para que o nome do compartilhamento no GFI MailEssentials inclua o caminho completo do compartilhamento de rede, e não apenas o caminho local.

7. No pop-up **Deploy Software**, selecione **Assigned** e clique em **OK**.

8. O novo pacote já está adicionado em **Software Installation**.

9. Clique com o botão direito do mouse em **Computer Configuration > Policies > Administrative Templates** e selecione **All Tasks > Add/Remove Templates**.

10. Clique em **Add** e procure a pasta compartilhada que contém **spamtag.adm**.

11. Clique em **Close**.

12. Acesse **Computer Configuration > Policies > Administrative Templates > Classic Administrative Templates (ADM) > GFI MailEssentialsSpamTag**.

13. No painel direito, clique duas vezes na política **DefaultWebServiceUrl** e selecione **Enabled**. No **Portal Website Address GFI MailEssentials**, digite o URL público do GFI MailEssentials. As máquinas nas quais o SpamTag será implantado devem ser capazes de estabelecer uma conexão com este URL através de um navegador da Web. Caso contrário, o SpamTag não poderá estabelecer uma conexão com o GFI MailEssentials.

14. Como alternativa, clique em **Previous Setting** para alterar o idioma padrão do SpamTag. Clique em **Enabled** e modifique o valor **Default Language**.

15. Clique em **OK**.

Etapa 3: Como verificar a instalação

A configuração será concluída. O SpamTag será instalado da próxima vez que cada máquina cliente for iniciada.

Para verificar a instalação, verifique se a barra de ferramentas do SpamTag está visível no Microsoft® Outlook e pode estabelecer uma conexão com o GFI MailEssentials.

Instalar o SpamTag via GPO no Windows Server 2003

Etapa 1: Preparar arquivos MSI e ADM

1. No servidor do GFI MailEssentials, acesse a pasta de instalação do GFI MailEssentials e abra a subpasta **Outlook**.

2. Copie os arquivos MSI e ADM em uma pasta compartilhada que possa ser acessada por todos os usuários que instalem o SpamTag. Certifique-se de que os usuários tenham pelo menos os direitos de leitura da pasta.

Etapa 2: Implantar o SpamTag

1. No prompt de comando, carregue `mmc.exe` para iniciar o Console de Gerenciamento Microsoft.

2. Acesse **File > Add/Remove Snap-in…** e clique em **Add...**

3. Selecione o snap-in **Group Policy Object Editor** e clique em **Add**.

4. Clique em **Browse…** para selecionar a política de domínio a ser editada.

5. Selecione a política de domínio e clique em **OK**.

6. Clique em **Finish** para fechar o diálogo "Selecionar objeto de diretiva de grupo". Clique em **Close** para fechar o diálogo "Adicionar Snap-in independente" e clique em **OK** para fechar o diálogo "Adicionar/Remover Snap-in" e retornar ao Console de Gerenciamento Microsoft.

7. Acesse **Console Root > <política do domínio> > User Configuration**, clique com o botão direito do mouse em **Administrative Templates** e selecione **Add/Remove Templates…**.

8. Clique em **Add…** e procure o arquivo ADM localizado na pasta compartilhada na etapa 1. Clique em **Open**.

9. Clique em **Close** para retornar ao Console de Gerenciamento Microsoft.

10. Expanda **Console Root > <política do domínio> > User Configuration > Administrative Templates > GFI Applications**.

11. No painel direito, clique duas vezes na política **DefaultWebServiceUrl** e selecione **Enabled**. Digite o URL público do GFI MailEssentials. As máquinas nas quais o SpamTag será implantado devem ser capazes de estabelecer uma conexão com este URL através de um navegador da Web. Caso contrário, o SpamTag não poderá estabelecer uma conexão com o GFI MailEssentials.

12. Como alternativa, clique em **Previous Setting** para alterar o idioma padrão do SpamTag. Clique em **Enabled** e modifique o valor **Default Language**.

13. Clique em **OK**.

14. Selecione **Console Root** > **<*política do domínio*>** > **Computer Configuration** > **Software Settings**.

15. Clique com o botão direito do mouse em **Software installation** e selecione **New** > **Package...**

16. No diálogo **Open**, localize o compartilhamento no qual o arquivo MSI foi salvo na etapa 1.

> **OBS.**
> Quando selecionar o local do arquivo MSI, certifique-se de que isso seja feito em "Meus locais de rede" para que o nome do compartilhamento no GFI MailEssentials inclua o caminho completo do compartilhamento de rede, e não apenas o caminho local.

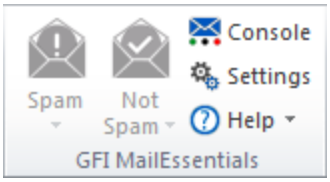
17. Escolha a opção de implantação - selecione **Assigned** e **OK**.

Etapa 3: Como verificar a instalação

A configuração será concluída. O SpamTag será instalado da próxima vez que cada máquina cliente for iniciada.

Para verificar a instalação, verifique se a barra de ferramentas do SpamTag está visível no Microsoft® Outlook e pode estabelecer uma conexão com o GFI MailEssentials.

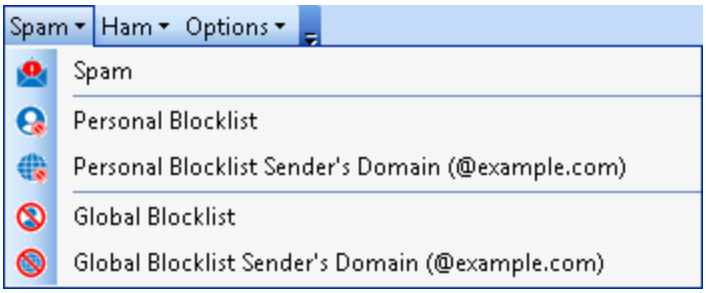
6.7.5 Usar o SpamTag



Screenshot 94: SpamTag no Microsoft Outlook 2010

Para obter informações sobre como usar o SpamTag, consulte a ajuda integrada clicando em **Help** no SpamTag.

A ajuda mostra automaticamente as informações relacionadas aos recursos habilitados pelo administrador na página das configurações do SpamTag.



Screenshot 95: SpamTag no Microsoft Outlook 2003

6.8 Verificação de pasta pública

As técnicas de spam estão sempre evoluindo e, consequentemente, você pode encontrar spams passas pelos filtros de spam e chegam à caixa de entrada do destinatário. Com a verificação da pasta pública, os usuários podem classificar manualmente emails como spam e "ensinar" os padrões de spam

do GFI MailEssentials a classificar emails parecidos como spam. Os emails também podem ser adicionados à lista de permissão.

IMPORTANTE
É altamente recomendado usar o SpamTag do GFI MailEssentials em vez da Verificação de pasta pública quando os clientes da rede usam o Microsoft Outlook como cliente de email. Para obter mais informações, consulte SpamTag para Microsoft Outlook (página 162).

Como funciona:

1. Quando um email classificado incorretamente (falso positivo ou falso negativo) for identificado, os usuários arrastam e soltam o email na pasta pública GFI AntiSpam apropriada. Para obter mais informações, consulte Usar a verificação de pasta pública (página 174).

2. A verificação de pastas públicas recupera emails de pastas públicas GFI AntiSpam e adiciona esses emails ao banco de dados de HAM/SPAM.

As pastas públicas GFI Antispam devem ser criadas e configuradas no servidor de email. Para obter mais informações, consulte Habilitar a verificação de pasta pública (página 170).

6.8.1 Habilitar a verificação de pasta pública

Para habilitar a verificação das pastas públicas, siga as instruções nas seções abaixo:

- Configuração da verificação de pastas públicas do Microsoft ® Exchange
- Configurar uma conta de usuário dedicada para o Microsoft ® Exchange Server 2003
- Configurar uma conta de usuário dedicada para o Microsoft ® Exchange Server 2007/2010
- Ocultar postagens do usuário nas pastas anti-spam do GFI

OBS.
Você também pode usar o GFI MailEssentials com o Lotus Domino. Para obter mais informações, consulte Lotus Domino (página 33).

Configuração da verificação de pastas públicas para o Microsoft® Exchange Servers

1. No console de configuração do GFI MailEssentials, acesse **Anti-spam > Anti-Spam Settings**. Selecione a guia **Public Folder Scanning**.

2. Selecione **Enable Public Folder Scanning** e, na lista **Poll public folder via**, selecione:

- **Exchange Server 2003** - Selecione MAPI, IMAP ou WebDav.
- **Exchange Server 2007** - Escolha WebDAV ou Serviços Web.
- **Exchange Server 2010** - Escolha Serviços Web.

As opções são descritas na tabela abaixo.

Opção	Descrição
MAPI	Para usar o MAPI, o GFI MailEssentials deve estar instalado na máquina em que o Microsoft® Exchange Server está instalado. Não é necessária outra configuração.

Opção	Descrição
IMAP	Exige o serviço IMAP do Microsoft ® Exchange. O IMAP permite a verificação remota de pastas públicas e funciona bem em ambientes com firewalls. Além disso, IMAP pode ser usado com outros servidores de email que sejam compatíveis com IMAP. Os parâmetros obrigatórios são: » Nome do servidor de email » O número da porta (a porta IMAP padrão é a 143) » Nome do usuário/senha » Selecione a opção **Use SSL** para usar uma conexão segura
WebDAV	Especifique o nome do servidor de email, a porta (a porta WebDav padrão é 80), nome do usuário/senha e domínio. Para usar uma conexão segura, selecione a caixa de texto **Use SSL**. Por padrão, as pastas públicas são acessíveis no diretório virtual "público". Se esse diretório tiver sido alterado, especifique o nome do diretório virtual correto para acessar as pastas públicas editando o texto na caixa **URL**.
Serviços da Web	Especifique as seguintes informações: » **Server** - nome do servidor de email » **Domain** - use o domínio local **OBS.:** Se existir um domínio local e um domínio público, use sempre o local. » **Port** - Porta dos serviços da Web padrão (80 ou 443 se usar SSL). » **Username/password** - use credenciais com privilégios administrativos ou crie um usuário dedicado a partir do Shell de Gerenciamento do Microsoft ® Exchange® digitando o seguinte comando para adicionar as permissões: `Add-ADPermission -identity "Mailbox Store" -User NewUser -AccessRights GenericALL` Substitua o `Mailbox Store` pelo nome do armazenamento da caixa de correio que contém as caixas de correio do usuário e `NewUser` pelo nome de usuário do usuário criado. » **Use SSL** - Selecione esta opção se os Serviços Web do Exchange exigirem uma conexão segura. Por padrão, os Serviços Web exigem SSL. » **URL** - Por padrão, as pastas públicas podem ser acessadas no diretório virtual "EWS/exchange.asmx". Se esse diretório tiver sido alterado, especifique o nome do diretório virtual correto para acessar as pastas públicas editando o texto na caixa URL. **OBSERVAÇÃO:** É recomendado testar as configurações manualmente, carregando o URL em um navegador da Web. Isso carregará um arquivo formatado XML chamado **services.wsdl**.

3. Clique em **Scan Now** para criar as pastas públicas automaticamente.

4. Clique em **Test** se você estiver configurando IMAP, WebDAV ou Serviços da Web. Uma notificação na tela confirmará o sucesso/falha. Se o teste falhar, verifique/atualize as credenciais e refaça o teste.

5. Clique em **Apply**.

Configurar uma conta de usuário dedicada para o Microsoft® Exchange Server 2003

Por razões de segurança, é recomendável que quando o GFI MailEssentials for instalado em DMZ, uma conta de usuário dedicada seja criada para recuperar/verificar emails de pastas públicas.

1. Criar um novo usuário do Active Directory (AD).

2. No Gerenciador do Sistema do Microsoft ® Exchange, expanda o nó **Folders > Public Folders**.

3. Clique com o botão direito do mouse na pasta pública **GFI AntiSpam Folders** e selecione **Properties**.

4. Clique na guia **Permissions** e selecione **Client permissions**.

5. Clique em **Add…**, selecione o novo usuário e clique em **OK**.

6. Selecione o novo usuário na lista de permissões do cliente e, na lista fornecida, defina a função como **Proprietário**. Certifique-se de que todas as caixas de texto estejam selecionadas e os botões de opção estejam definidos para **All**.

7. Clique em **OK** para finalizar as configurações.

8. No Microsoft® Exchange System Manager, clique com o botão direito do mouse em **GFI AntiSpam Folders** e selecione **All tasks > Propagate settings**.

> **OBS.**
> No Microsoft® Exchange Server 2003 SP2, clique com o botão direito do mouse na opção **GFI AntiSpam Folders** e selecione a opção **All tasks > Manage Settings**.

9. Selecione **Folder rights ou Modify client permissions** e clique em **OK** ou em **Next**.

10. Especifique as credenciais da nova conta de usuário criada na etapa 1 e teste a configuração para assegurar que as permissões estejam corretas.

Configurar uma conta de usuário dedicada para o Microsoft ® Exchange Server 2007/2010

Quando configurar uma conta de usuário dedicado para recuperar emails das pastas públicas GFI AntiSpam, o usuário precisa ter os direitos de acesso "proprietário" às GFI AntiSpam Public Folders

1. Criar um novo usuário (proprietário) do Active Directory (AD).

2. Faça logon para o Microsoft® Exchange Server usando os privilégios administrativos.

3. Abra o Shell de Gerenciamento do **Microsoft® Exchange** e digite o seguinte comando:

```
Get-PublicFolder -Identity "\GFI AntiSpam Folders" -Recurse | ForEach-
Object {Add-PublicFolderClientPermission -Identity $_.Identity -User
"USERNAME" -AccessRights owner -Server "SERVERNAME"}
```

Altere `USERNAME` e `SERVERNAME` de acordo com os detalhes relevantes do usuário do Active Directory em questão. Exemplo:

```
Get-PublicFolder -Identity "\GFI AntiSpam Folders" -Recurse | ForEach-
Object {Add-PublicFolderClientPermission -Identity $_.Identity -User
"mesuser" -AccessRights owner -Server "exch07"}
```

Como ocultar postagens de usuários em GFI AntiSpam Folders

Por motivos de privacidade e segurança, é altamente recomendável que você oculte as postagens de usuários feitas nas pastas GFI AntiSpam. Dessa forma, os usuários só serão capazes de postar nas pastas sem visualizar postagens existentes (nem mesmo as que eles postaram). Para configurar os privilégios de usuário e ocultar postagens de usuários não autorizados:

Microsoft ® Exchange 2003

1. No Gerenciador do Sistema do Microsoft® Exchange, expanda o nó **Folders > Public Folders**.

2. Clique com o botão direito do mouse na pasta pública **GFI AntiSpam Folders** e selecione **Properties**.

3. Selecione a guia **Permissions** e clique em **Client permissions**.

4. Clique em **Add...**, selecione o usuário/grupo do qual ocultar postagens e clique em **OK**.

5. Selecione o usuário/grupo configurado anteriormente na lista de permissões do cliente e defina sua função como **Contributor**.

6. Certifique-se de que apenas a opção **Create items** esteja selecionada e os botões de opção estão definidos para **None**.

7. Clique em **OK** para finalizar as configurações.

8. No Microsoft® Exchange System Manager, clique com o botão direito do mouse em **GFI AntiSpam Folders** e selecione **All tasks > Propagate settings**.

9. Selecione a caixa de texto **Folder rights** e clique em **OK**.

Microsoft ® Exchange 2007

1. No Shell de Gerenciamento do **Microsoft® Exchange**, digite o seguinte comando:

```
ReplaceUserPermissionOnPFRecursive.ps1 -Server "server" -
TopPublicFolder "\'GFI AntiSpam Folders'" -User "Default" -Permissions
Contributor
```

Substitua "`servidor`" pelo nome completo do computador.

2. Quando solicitado, digite `y` para confirmar as permissões para cada pasta.

Este comando define as permissões padrão das Pastas públicas de contribuinte GFI MailEssentials, para que os usuários possam transferir emails para as pastas públicas, mas não possam visualizar ou modificar entradas. Por padrão, os administradores são proprietários de pastas públicas e podem visualizar ou modificar entradas. Para obter mais informações sobre permissões de pastas públicas, consulte:

http://go.gfi.com/?pageid=ME_PFPermissionsExch2007

Microsoft® Exchange 2010

1. No Shell de Gerenciamento do Microsoft®Exchange, mude a pasta para a pasta de scripts do Microsoft ® Exchange que pode ser encontrada na pasta de instalação do Microsoft® Exchange. Se o Microsoft® Exchange estiver instalado na localização padrão, a pasta de scripts estará armazenada em:

```
C:\Program Files\Microsoft\Exchange Server\V14\Scripts\
```

2. Digite o seguinte comando:

```
ReplaceUserPermissionOnPFRecursive.ps1 -Server "server" -
TopPublicFolder "\GFI AntiSpam Folders" -User "Default" -Permissions
Contributor
```

Substitua "`servidor`" pelo nome completo do computador.

Este comando define as permissões padrão das Pastas públicas de contribuinte GFI MailEssentials, para que os usuários possam transferir emails para as pastas públicas, mas não possam visualizar ou modificar entradas. Por padrão, os administradores são proprietários de pastas públicas e podem visualizar ou modificar entradas. Para obter mais informações sobre permissões de pastas públicas, consulte:

http://go.gfi.com/?pageid=ME_PFPermissionsExch2010

6.8.2 Usar a verificação de pasta pública

Analisar emails com spam

1. Quando emails com spam forem enviados para a caixa de correio do usuário (caixa de entrada, pasta Lixo Eletrônico ou uma pasta personalizada), instrua os usuários de email individuais a analisar periodicamente os emails com spam.

2. Haverá casos em que emails legítimos serão incorretamente identificados como spam (falsos positivos). Para obter mais informações, consulte Gerenciar emails legítimos (página 174).

3. Podem existir casos nos quais emails com spam não são detectadas (falsos negativos). Para obter mais informações, consulte Gerenciar spam (página 175).

Gerenciar emails legítimos

Como ocorre com qualquer solução anti-spam, o GFI MailEssentials pode levar algum tempo até atingir as condições de filtragem anti-spam ideais. Em casos nos quais essas condições não tenham sido atingidas, emails legítimos podem ser identificados como spam.

Nesses casos, os usuários devem adicionar emails identificados incorretamente como spam às pastas **Add to whitelist** e **This is legitimate email** para "ensinar" ao GFI MailEssentials que o email em questão não é spam.

> **OBSERVAÇÕES**
> 1. No Microsoft® Outlook, arrastar e soltar o email move-o para a pasta selecionada. Para manter uma cópia do email, mantenha a tecla CTRL pressionada para copiar o email em vez de movê-lo.
> 2. Informações detalhadas de como criar as pastas GFI AntiSpam estão incluídas neste manual. Para obter mais informações, consulte Habilitar a verificação de pasta pública (página 170).

Adicionar remetentes à lista de permissão

1. Na lista de pastas públicas do cliente de email (por exemplo, Microsoft® Outlook), localize a pasta pública **GFI AntiSpam Folders > Add to whitelist**.

2. Arraste e solte as mensagens ou boletins informativos na pasta pública **Add to whitelist**.

Adicionar listas de discussão à lista de permissão

Em emails enviados para listas de discussões, o endereço de email da lista de discussão é o destinatário da mensagem. Para receber emails de listas de discussão específicas, o endereço de email da lista precisa estar na lista de permissão.

1. Usando o cliente de email (por exemplo, Microsoft® Outlook), localize a pasta pública **GFI AntiSpam Folders > I want this Discussion list**.

2. Arraste e solte as listas de discussão na pasta pública **I want this Discussion list**.

Usar emails legítimos para "treinar" o filtro Bayesiano

1. Nas pastas públicas do cliente de email (por exemplo, Microsoft® Outlook), localize a pasta pública **GFI AntiSpam Folders > This is legitimate email**.

2. Arraste e solte os emails na pasta **This is legitimate email**.

Gerenciar spam

Embora o GFI MailEssentials comece a identificar emails com spam imediatamente, em algumas situações, o spam pode chegar às caixas de correio dos usuários sem ser detectado. Normalmente, isso ocorre porque as definições de configuração ainda não foram realizadas ou devido a novas formas de spam às quais o GFI MailEssentials ainda não se adaptou. Em ambos os casos, essas situações são resolvidas quando o GFI MailEssentials é configurado para capturar esse tipo de spam.

Nesses casos, os usuários devem adicionar esses emails às pastas **Add to blocklist** e **This is spam email** para "ensinar" ao GFI MailEssentials que o email em questão é spam.

> **OBSERVAÇÕES**
> 1. No Microsoft® Outlook, arrastar e soltar o email move-o para a pasta selecionada. Para manter uma cópia do email, mantenha a tecla CTRL pressionada para copiar o email em vez de movê-lo.
> 2. Informações detalhadas de como criar as pastas GFI AntiSpam estão incluídas neste manual. Para obter mais informações, consulte Habilitar a verificação de pasta pública (página 170).

Adicionar remetentes à Lista de bloqueio de email

1. Nas pastas públicas do cliente de email (por exemplo, Microsoft® Outlook), localize a pasta pública **GFI AntiSpam Folders > Add to blocklist**.

2. Arraste e solte emails na pasta pública **Add to blocklist**.

Usar emails de spam para "treinar" o filtro Bayesiano

1. Nas pastas públicas do cliente de email (por exemplo, Microsoft® Outlook), localize a pasta pública **GFI AntiSpam Folders > This is spam email**.

2. Arraste e solte o email com spam na pasta **This is spam email**.

7 Filtragem de conteúdo

Os mecanismos de filtragem de conteúdo permitem que os administradores controlem o conteúdo dos emails. Esses mecanismos examinam o conteúdo de emails e anexos e bloqueiam emails com conteúdos que corresponda às regras de filtragem de conteúdo.

Tópicos deste capítulo:

7.1 Filtragem de palavras-chave

O recurso de filtragem de palavras-chave permite definir regras que filtram emails com determinadas palavras-chave ou uma combinação de palavras-chave no corpo ou assunto do email. Uma regra é composta por:

- Palavras-chave para bloquear no corpo do email, assunto ou anexo
- Ações a serem executadas quando uma palavra-chave for encontrada
- Os usuários aos quais a regra se aplica.

Para configurar as regras de conteúdo, acesse **Content Filtering > Keyword Filtering**. Esta página permite visualizar, criar, habilitar, desabilitar ou excluir regras.

7.1.1 Criar uma regra de filtragem de palavra-chave

Para criar uma regra de filtragem de palavra-chave, siga as etapas listadas a seguir.

- Etapa 1: Definir a configuração de regras básicas
- Etapa 2: Configurar os termos a serem bloqueados
- Etapa 3: Configurar as ações a serem tomadas nos emails detectados
- Etapa 4: Especificar os usuários aos quais aplicar esta regra

Etapa 1: Configurar as configurações das regras básicas

1. Acesse **Content Filtering > Keyword Filtering** e selecione **Add Rule...**
2. Especifique um nome para a regra na caixa de texto **Rule name**.
3. Selecione se deseja fazer a verificação dos emails de entrada, saída e/ou internos.

Opção	Descrição
Check Inbound emails	Selecione esta opção para verificar emails de entrada

Opção	Descrição
Check Outbound emails	Selecione esta opção para verificar emails de saída
Check Internal emails	Selecione esta opção para fazer a verificação de emails internos. **OBS.** Esta opção só estará disponível quando GFI MailEssentials estiver instalado no servidor Microsoft® Exchange

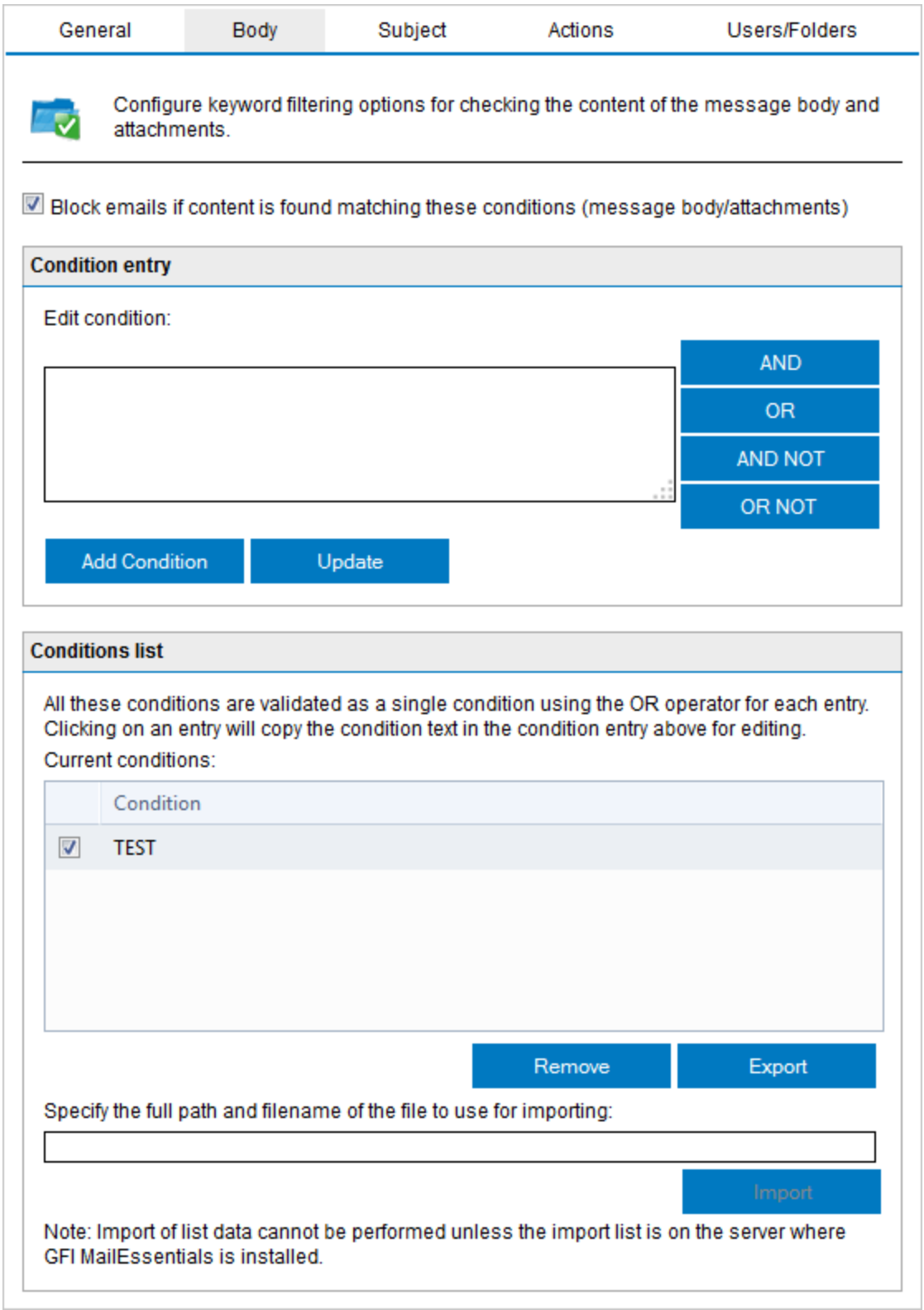
4. Para bloquear emails criptografados usando a tecnologia PGP, selecione **Block PGP encrypted emails.**

> **OBS.**
> A criptografia PGP é um sistema criptográfico de chave pública usado para criptografar emails.

Etapa 2: Configurar os termos a serem bloqueados

1. Selecione a guia **Body** para especificar as palavras-chaves no corpo da mensagem de email a serem bloqueadas.

2. Selecione a caixa de texto **Block emails if content is found matching these conditions (message body/attachments)** para permitir a verificação de palavras-chave no corpo.



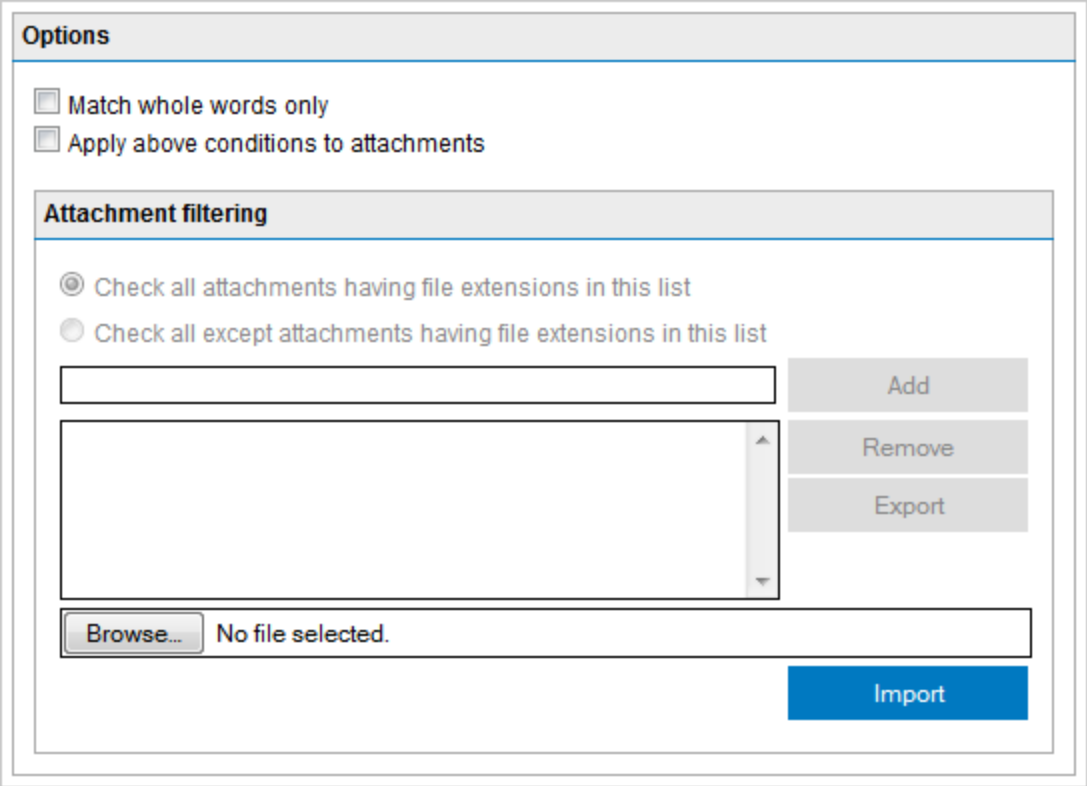
Screenshot 96: Filtragem de conteúdo: Guia Corpo - definir condições

3. Na área **Condition entry**, digite as palavras-chave a serem bloqueadas na caixa **Edit condition**. Você também pode usar as condições **AND**, **OR**, **AND NOT** e **OR NOT** para usar uma combinação de palavras-chave.

4. Para adicionar uma palavra-chave ou uma combinação de palavras-chave digitadas, clique em **Add Condition**.

Para modificar uma entrada na lista **Conditions**, selecione a entrada e faça as alterações necessárias na caixa **Condition entry**. Para remover uma entrada da lista **Conditions**, selecione-a e clique em **Remove**.

Clique em **Update** para aplicar as alterações.



Screenshot 97: Filtragem de conteúdo: Guia Corpo: configurar outras opções

5. (Opcional) Na área **Options**, configure as seguintes opções:

Opção	Descrição
Match whole words only	Bloqueia mensagens de emails quando as palavras-chave especificadas corresponderem a palavras inteiras.
Apply above conditions to attachments	Selecione esta opção para aplicar essa regra também aos textos em anexos. Na área **Attachment filtering**, especifique a extensão de arquivo dos anexos (por exemplo, `.doc`) para aplicar ou excluir nesta regra.

6. Selecione a guia **Subject** para especificar as palavras-chave a serem bloqueadas no assunto do email.

7. Na área **Condition entry**, digite as palavras-chave a serem bloqueadas na caixa **Edit condition**. Você também pode usar as condições **AND**, **OR**, **AND NOT** e **OR NOT** para usar uma combinação de palavras-chave.

8. Para adicionar uma palavra-chave ou uma combinação de palavras-chave digitadas, clique em **Add Condition**.

Para modificar uma entrada na lista **Conditions**, selecione a entrada e faça as alterações necessárias na caixa **Condition entry**. Para remover uma entrada da lista **Conditions**, selecione-a e clique em **Remove**.

Clique em **Update** para aplicar as alterações.

9. Na área **Options**, configure como é feita a correspondência de palavras-chave. Selecione **Match whole words only** para bloquear emails nos quais as palavras-chave especificadas correspondem às palavras inteiras no assunto

Etapa 3: Definir as ações a serem executadas em emails detectados

1. Clique na guia **Actions** para configurar o que deve ser feito quando esta regra for acionada.

2. Para bloquear um email que corresponda às condições da regra, selecione **Block email and perform this action** e uma das seguintes opções:

Opção	Descrição
Quarantine email	Armazena emails bloqueados no armazenamento da quarentena. Em seguida, você pode analisar (aprovar/excluir) todos os emails em quarentena. Para obter mais informações, consulte Quarentena (página 203).
Delete email	Exclui emails bloqueados.
Move to folder on disk	Move o email para uma pasta no disco. Digite o caminho completo da pasta onde guardar os emails bloqueados.

IMPORTANTE

As ações sempre afetam todo o email que contém o conteúdo bloqueado, mesmo se houver outro conteúdo (como anexos) que não acione essa regra.

OBS.

Quando o GFI MailEssentials estiver instalado na mesma máquina do Microsoft® Exchange 2003, o GFI MailEssentials pode não ser capaz de bloquear emails de saída. Em vez disso, ele substitui o conteúdo bloqueado por um relatório de ameaça.

3. Selecione **Send a sanitized copy of the original email to recipient(s)** para escolher se deseja enviar uma cópia do email bloqueado para os destinatários, mas com o conteúdo malicioso removido.

4. O GFI MailEssentials pode enviar notificações por email quando um email acionar esse filtro. Para ativar esse recurso, selecione uma das seguintes opções:

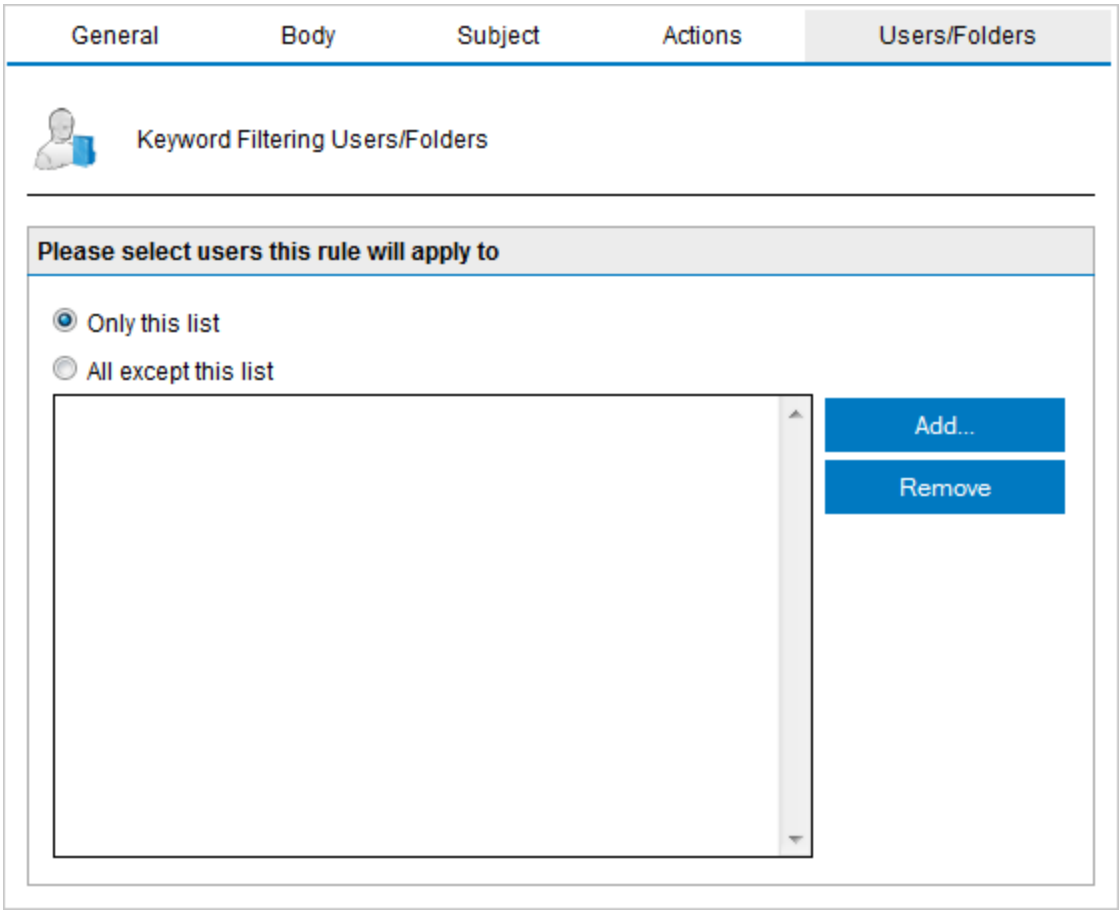
Opção	Descrição
Notify administrator	Notifique o administrador sempre que esse mecanismo bloquear uma mensagem de email. Para obter mais informações, consulte Endereço de email do administrador (página 240).
Notify local user	Notifique os destinatários locais de email sobre o email bloqueado.

5. Para registrar a atividade deste mecanismo em um arquivo de registro, selecione **Log occurrence to this file**. Na caixa de texto, especifique o caminho e o nome do arquivo para um local personalizado no disco onde armazenar o arquivo de registro. Por padrão, os arquivos de registro são armazenados em:

```
<GFI MailEssentials installation path>\GFI\MailEssentials\EmailSecurity\Logs\<Nome do mecanismo>.log
```

Etapa 4: Especificar os usuários aos quais esta regra se aplica

1. Por padrão, a regra será aplicada a todos os usuários de email. No entanto, o GFI MailEssentials permite aplicar essa regra a uma lista personalizada de usuários de email especificados na guia Users / Folders.

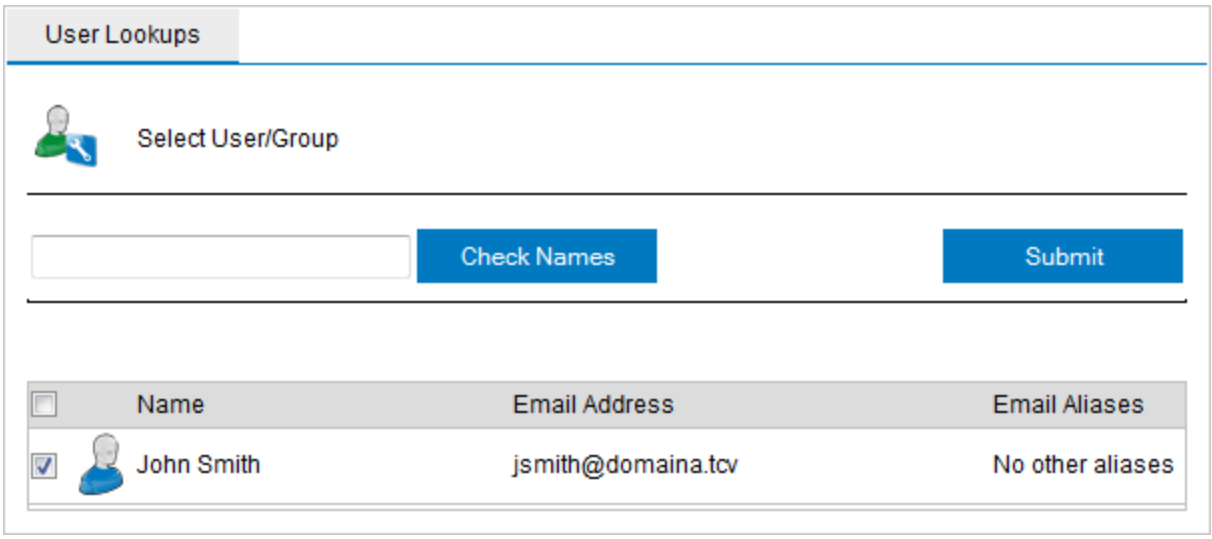


Screenshot 98: Filtragem de conteúdo: Guia Users/Folders

2. Especifique os usuários aos quais aplicar essa regra.

Opção	Descrição
Only this list	Aplique esta regra a uma lista personalizada de usuários de email, grupos ou pastas públicas.
All except this list	Aplique esta regra a todos os usuários de email, exceto aos usuários, grupos ou pastas públicas especificados na lista.

3. Para adicionar os usuários de email, grupos de usuários e/ou pastas públicas à lista, clique em **Add**.



Screenshot 99: Adicionar usuários à regra de Filtragem de conteúdo

4. Na janela **User Lookups**, especifique o nome do usuário de email/grupo de usuários ou pasta pública que você deseja adicionar à lista e clique em **Check Names**. Os usuários, grupos ou pastas públicas correspondentes são listados abaixo.

> **OBS.**
> Você não precisa digitar o nome completo dos usuários, grupos ou pastas públicas. Basta digitar parte do nome. GFI MailEssentials listará todos os nomes que contenham os caracteres especificados. Por exemplo, se você inserir `sco`, o GFI MailEssentials retornará nomes como `Scott Adams` e `Freeman Prescott`, se estiverem disponíveis.

5. Selecione a caixa de seleção ao lado dos nomes que você deseja adicionar à lista e clique em **OK**.

> **OBS.**
> Para remover entradas da lista, selecione o usuário/grupo de usuários/pasta pública que deseja remover e clique em **Remove**.

6. Repita as etapas de 3 a 5 para adicionar todos os usuários necessários para a lista.

7. Clique em **Apply**.

7.1.2 Habilitar/desabilitar regras

Para habilitar/desabilitar regras de filtragem de conteúdo:

1. Acesse **Content Filtering > Keyword Filtering**.

2. Na página **Content Filtering**, selecione as caixas de texto das regras para habilitá-las ou desabilitá-las.

3. Clique em **Enable Selected** ou **Disable Selected** conforme apropriado.

7.1.3 Remover regras de filtragem de conteúdo

> **AVISO**
> Regras excluídas não podem ser recuperadas. Se estiver em dúvida, é recomendável desabilitar uma regra.

1. Acesse **Content Filtering > Keyword Filtering**.

2. Na página Filtragem de conteúdo, selecione as caixas de texto das regras que você deseja remover.

3. Clique em **Remove Selected**.

7.1.4 Como modificar uma regra existente

1. Acesse **Content Filtering > Keyword Filtering**.

2. Na página **Content Filtering**, clique no nome da regra a ser modificada.

3. Execute as alterações necessárias nas propriedades da regra e clique em **Apply**.

7.1.5 Como alterar a prioridade da regra

As regras de filtragem de conteúdo são aplicadas na mesma ordem, de cima para baixo, como listadas na página Content Filtering (isto é, a regra com prioridade 1 é verificada primeiro). Para alterar a sequência/prioridade de regras:

1. Acesse **Content Filtering > Keyword Filtering**.

2. Na página **Content Filtering**, clique nas setas (para cima) ou (para baixo), respectivamente, para aumentar ou diminuir a prioridade da regra selecionada.

3. Repita a etapa 2 até que as regras estejam na sequência desejada.

7.2 Filtragem de anexos

A filtragem de anexos permite configurar regras para filtrar que tipos de anexos de email serão permitidos e bloqueados no servidor de email. Uma regra é composta por:

- Tipos de anexo para bloquear
- Ações a serem realizadas quando uma correspondência de anexo for encontrada
- Os usuários aos quais a regra se aplica.

Para configurar as regras do anexo, acesse **Content Filtering > Attachment Filtering**. Esta página permite visualizar, criar, habilitar, desabilitar ou excluir regras.

7.2.1 Criar uma regra de filtragem de anexos

Para criar uma regra de filtragem de anexos, siga as etapas abaixo:

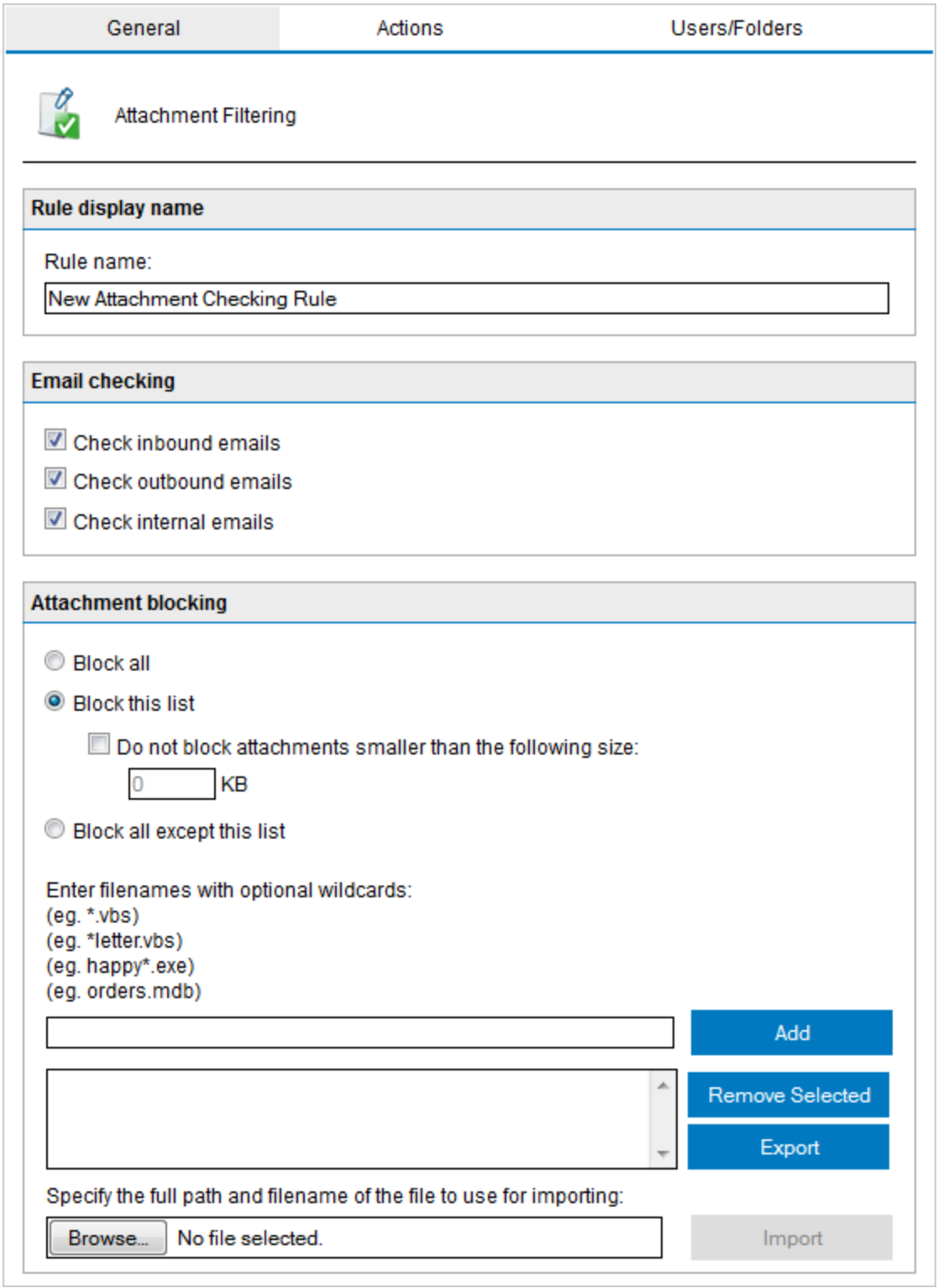
- Etapa 1: Definir configurações de regras básicas e os termos para bloquear
- Etapa 2: Configurar as ações a serem tomadas nos emails detectados

» Etapa 3: Especificar os usuários aos quais aplicar esta regra

Etapa 1: Definir configurações de regras básicas e os termos para bloquear

1. Acesse o nó **Content Filtering > Attachment Filtering .**

2. Clique em **Add Rule...**



Screenshot 100: Filtragem de anexos: Guia General (Geral)

3. Especifique um nome para a regra na caixa de texto **Rule name**.

4. Selecione se deseja fazer a verificação dos emails de entrada, saída e/ou internos.

Opção	Descrição
Check Inbound emails	Selecione esta opção para verificar emails de entrada
Check Outbound emails	Selecione esta opção para verificar emails de saída
Check Internal emails	Selecione esta opção para fazer a verificação de emails internos. **OBS.** Esta opção só estará disponível quando GFI MailEssentials estiver instalado no servidor Microsoft® Exchange

5. Na área **Attachment Blocking**, especifique os tipos de anexos a serem bloqueados:

Opção	Descrição
Block all	Bloqueia todos os anexos de email de qualquer tipo.
Block this list	Bloqueia uma lista personalizada de tipos de anexos. Digite um nome de arquivo e/ou tipo de anexo para bloquear na caixa de texto **Enter filename with optional wildcards** e clique em **Add**. Repita esta etapa para todos os nomes de arquivos e/ou tipos de anexo a serem bloqueados.
Do not block attachments smaller than the following size:	Selecione esta opção para permitir tipos de anexo na lista que sejam menores que um determinado tamanho. Especifique o tamanho (em KB) na caixa de texto fornecida.
Block all except this list	Bloqueia todos os anexos, exceto aqueles especificados na lista. Digite um nome de arquivo e/ou tipo de anexo para permitir na caixa de texto **Enter filename with optional wildcards** e clique em **Add**. Repita esta etapa para todos os nomes de arquivos e/ou tipos de anexo a serem excluídos.

OBS.
Ao especificar os nomes de arquivos e/ou tipos de anexos, você pode usar o caractere curinga asterisco (*). Por exemplo, especificar `*pedidos*.mdb`, se refere a todos os arquivos do tipo **mdb** que contenham a palavra `pedidos` no nome do arquivo. Especificar `*.jpg` bloqueará todas as imagens do tipo **jpg**.

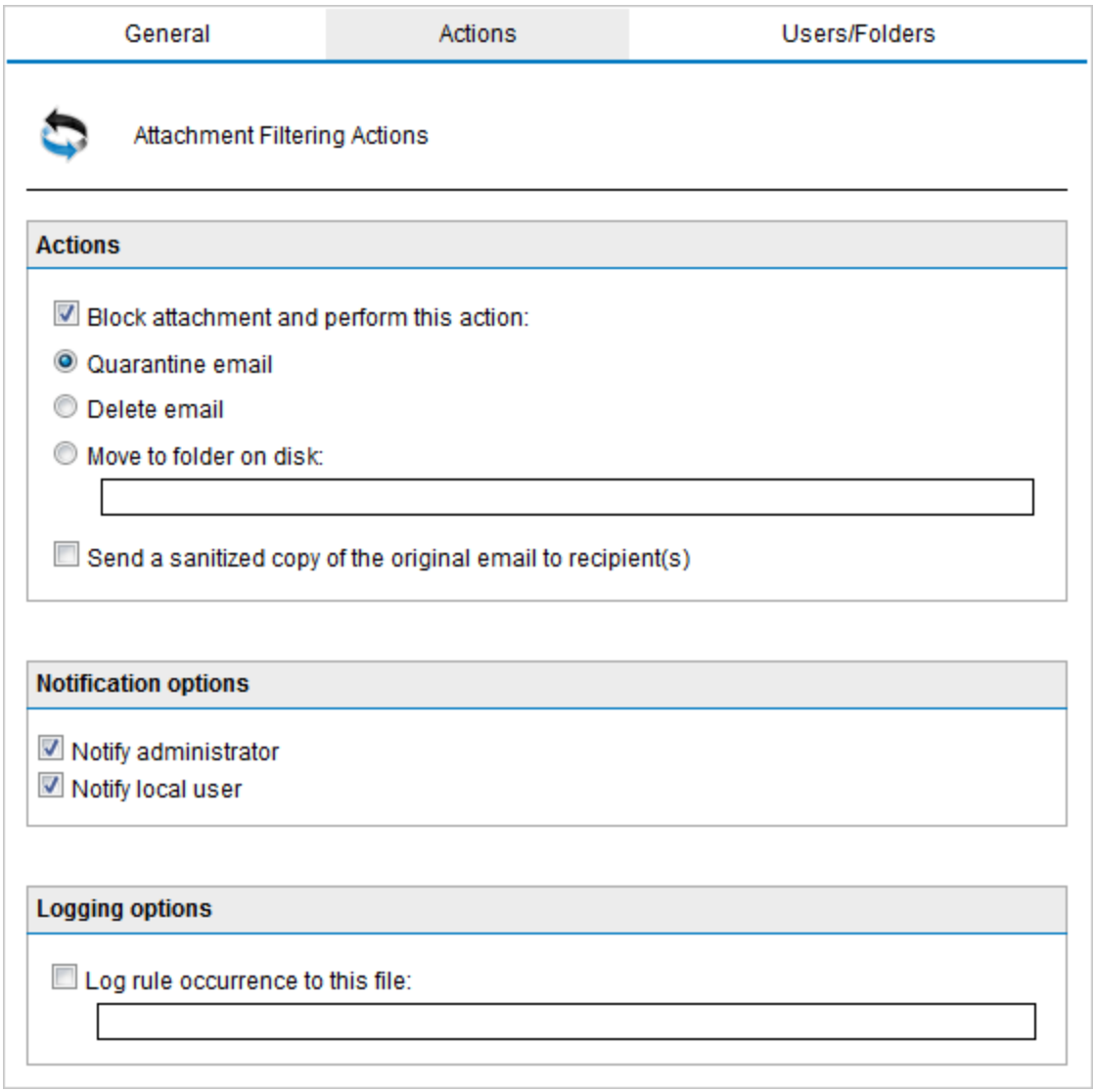
OBS.
Para remover uma entrada da lista, selecione-a e clique em **Remove Selected**.

6. Você também pode bloquear anexos que tenham um tamanho maior que um determinado tamanho. Para ativar essa opção, na área **Options**, selecione **Block all attachments greater than the following size in KB** e especifique o tamanho máximo do anexo (em KB).

OBS.
Esse recurso bloqueia todos os anexos com um arquivo de tamanho maior do que o especificado, independente de o anexo corresponder a uma entrada na lista **Attachment blocking**.

Etapa 2: Definir as ações a serem tomadas nos emails detectados

1. Clique na guia **Actions** para configurar o que acontece quando essa regra é acionada.



Screenshot 101: Filtragem de anexos: Guia Ações

2. Para bloquear uma mensagem de email que coincida com as condições da regra, selecione **Block attachment and perform this action** e selecione uma das seguintes opções:

Opção	Descrição
Quarantine email	Armazena emails bloqueados no armazenamento da quarentena. Em seguida, você pode analisar (aprovar/excluir) todos os emails em quarentena. Para obter mais informações, consulte Quarentena (página 203).
Delete email	Exclui emails bloqueados.
Move to folder on disk	Move o email para uma pasta no disco. Digite o caminho completo da pasta onde guardar os emails bloqueados.

IMPORTANTE

As ações sempre afetam todo o email que contém o conteúdo bloqueado, mesmo se houver outro conteúdo (como anexos) que não acione essa regra.

OBS.
Quando o GFI MailEssentials estiver instalado na mesma máquina do Microsoft® Exchange 2003, o GFI MailEssentials pode não ser capaz de bloquear emails de saída. Em vez disso, ele substitui o conteúdo bloqueado por um relatório de ameaça.

3. Selecione **Send a sanitized copy of the original email to recipient(s)** para escolher se deseja enviar uma cópia do email bloqueado para os destinatários, mas com o conteúdo malicioso removido.

4. O GFI MailEssentials pode enviar notificações por email quando um email acionar esse filtro. Para ativar esse recurso, selecione uma das seguintes opções:

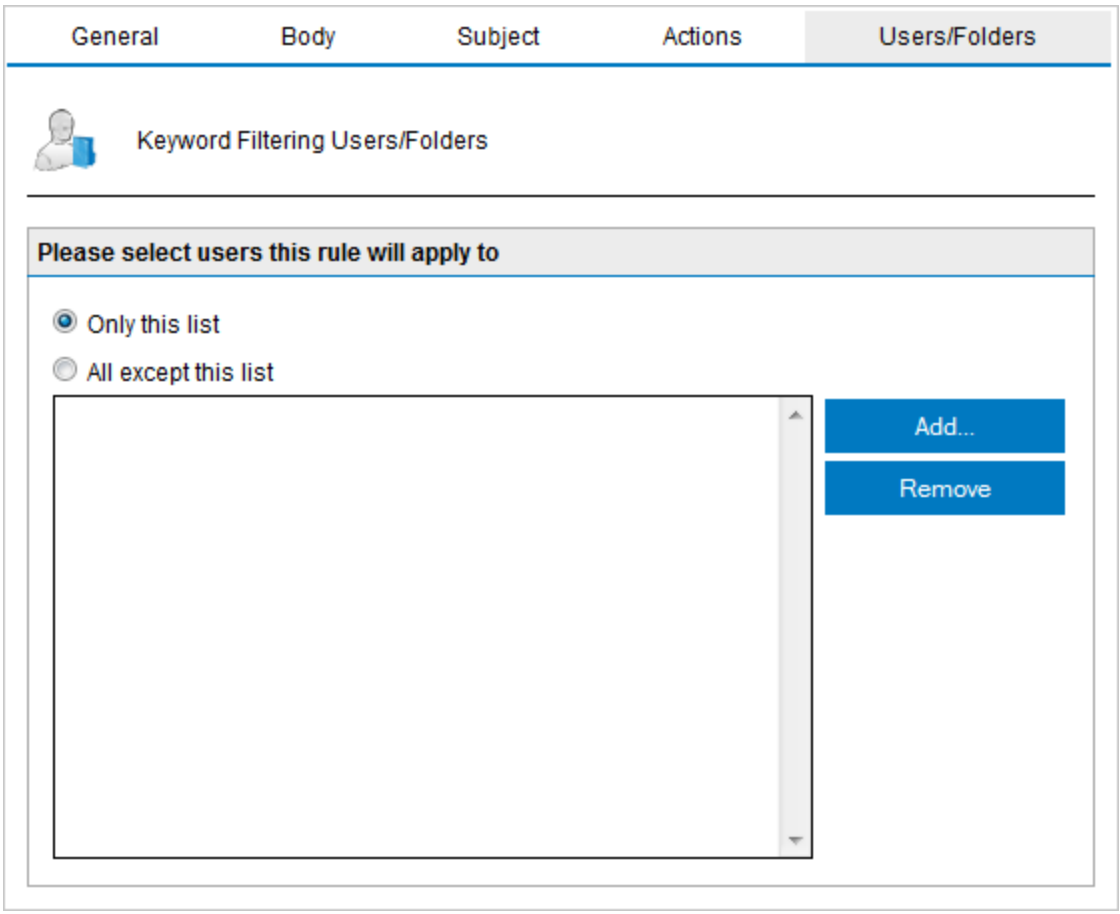
Opção	Descrição
Notify administrator	Notifique o administrador sempre que esse mecanismo bloquear uma mensagem de email. Para obter mais informações, consulte Endereço de email do administrador (página 240).
Notify local user	Notifique os destinatários locais de email sobre o email bloqueado.

5. Para registrar a atividade deste mecanismo em um arquivo de registro, selecione **Log occurrence to this file**. Na caixa de texto, especifique o caminho e o nome do arquivo para um local personalizado no disco onde armazenar o arquivo de registro. Por padrão, os arquivos de registro são armazenados em:

```
<GFI MailEssentials installation path>\GFI\MailEssentials\EmailSecurity\Logs\<Nome do mecanismo>.log
```

Etapa 3: Especificar os usuários aos quais esta regra se aplica

1. Por padrão, a regra será aplicada a todos os usuários de email. No entanto, o GFI MailEssentials permite aplicar essa regra a uma lista personalizada de usuários de email especificados na guia Users / Folders.

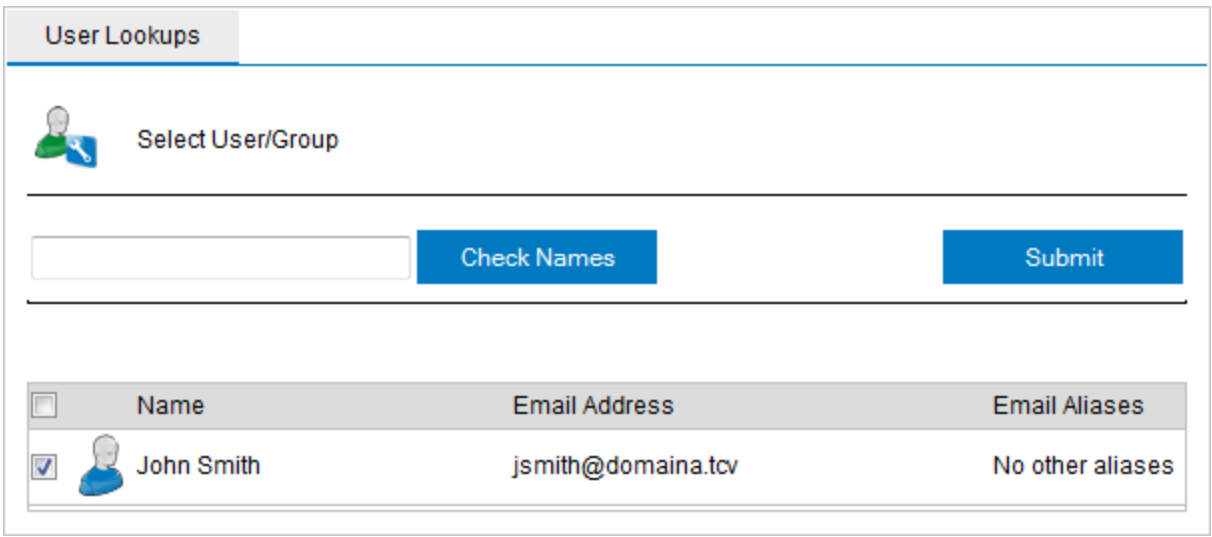


Screenshot 102: Filtragem de conteúdo: Guia Users/Folders

2. Especifique os usuários aos quais aplicar essa regra.

Opção	Descrição
Only this list	Aplique esta regra a uma lista personalizada de usuários de email, grupos ou pastas públicas.
All except this list	Aplique esta regra a todos os usuários de email, exceto aos usuários, grupos ou pastas públicas especificados na lista.

3. Para adicionar os usuários de email, grupos de usuários e/ou pastas públicas à lista, clique em **Add**.



Screenshot 103: Adicionar usuários à regra de Filtragem de conteúdo

4. Na janela **User Lookups**, especifique o nome do usuário de email/grupo de usuários ou pasta pública que você deseja adicionar à lista e clique em **Check Names**. Os usuários, grupos ou pastas públicas correspondentes são listados abaixo.

> **OBS.**
> Você não precisa digitar o nome completo dos usuários, grupos ou pastas públicas. Basta digitar parte do nome. GFI MailEssentials listará todos os nomes que contenham os caracteres especificados. Por exemplo, se você inserir `sco`, o GFI MailEssentials retornará nomes como `Scott Adams` e `Freeman Prescott`, se estiverem disponíveis.

5. Selecione a caixa de seleção ao lado dos nomes que você deseja adicionar à lista e clique em **OK**.

> **OBS.**
> Para remover entradas da lista, selecione o usuário/grupo de usuários/pasta pública que deseja remover e clique em **Remove**.

6. Repita as etapas de 3 a 5 para adicionar todos os usuários necessários para a lista.

7. Clique em **Apply**.

7.2.2 Regras habilitar/desabilitar

Para habilitar ou desabilitar as regras de filtragem:

1. Acesse **Content Filtering > Attachment Filtering**

2. Na página **Attachment Filtering**, selecione a caixa de texto da(s) regra(s) a ser ativada ou desativada.

3. Clique em **Enable Selected** ou **Disable Selected**.

7.2.3 Como remover regras de anexo

> **Aviso**
> Regras excluídas não possam ser recuperadas. Se estiver em dúvida, é recomendável desabilitar uma regra.

1. Acesse **Content Filtering > Attachment Filtering**

2. Na página **Attachment Filtering**, selecione a(s) regra(s) que você deseja remover.

3. Clique em **Remove Selected**.

7.2.4 Como modificar uma regra existente

1. Acesse **Content Filtering > Attachment Filtering**

2. Na página **Attachment Filtering**, clique no nome da regra a ser modificada.

3. Execute as alterações necessárias nas propriedades da regra e clique em **Apply**.

7.2.5 Como alterar a prioridade da regra

As regras de filtragem de anexos são aplicadas na mesma ordem, de cima para baixo, como elas são listadas na página de filtragem de anexos (isto é, a regra com prioridade 1 é assinalada primeiro). Para alterar a sequência/prioridade de regras:

1. Acesse **Content Filtering > Attachment Filtering**

2. Na página Attachment Filtering, clique nas setas (para cima) ou (para baixo) para aumentar ou diminuir a prioridade da regra selecionada, respectivamente.

3. Repita a etapa 2 até que as regras estejam na sequência desejada.

7.3 Filtragem de conteúdo avançada

A filtragem de conteúdo avançada permite fazer a verificação de dados do cabeçalho de emails e de conteúdo usando condições de pesquisa configuráveis avançadas e expressões regulares (regex).

Para configurar regras de conteúdo avançadas, acesse **Content Filtering > Advanced Content Filtering**. Esta página permite visualizar, criar, habilitar, desabilitar ou excluir regras.

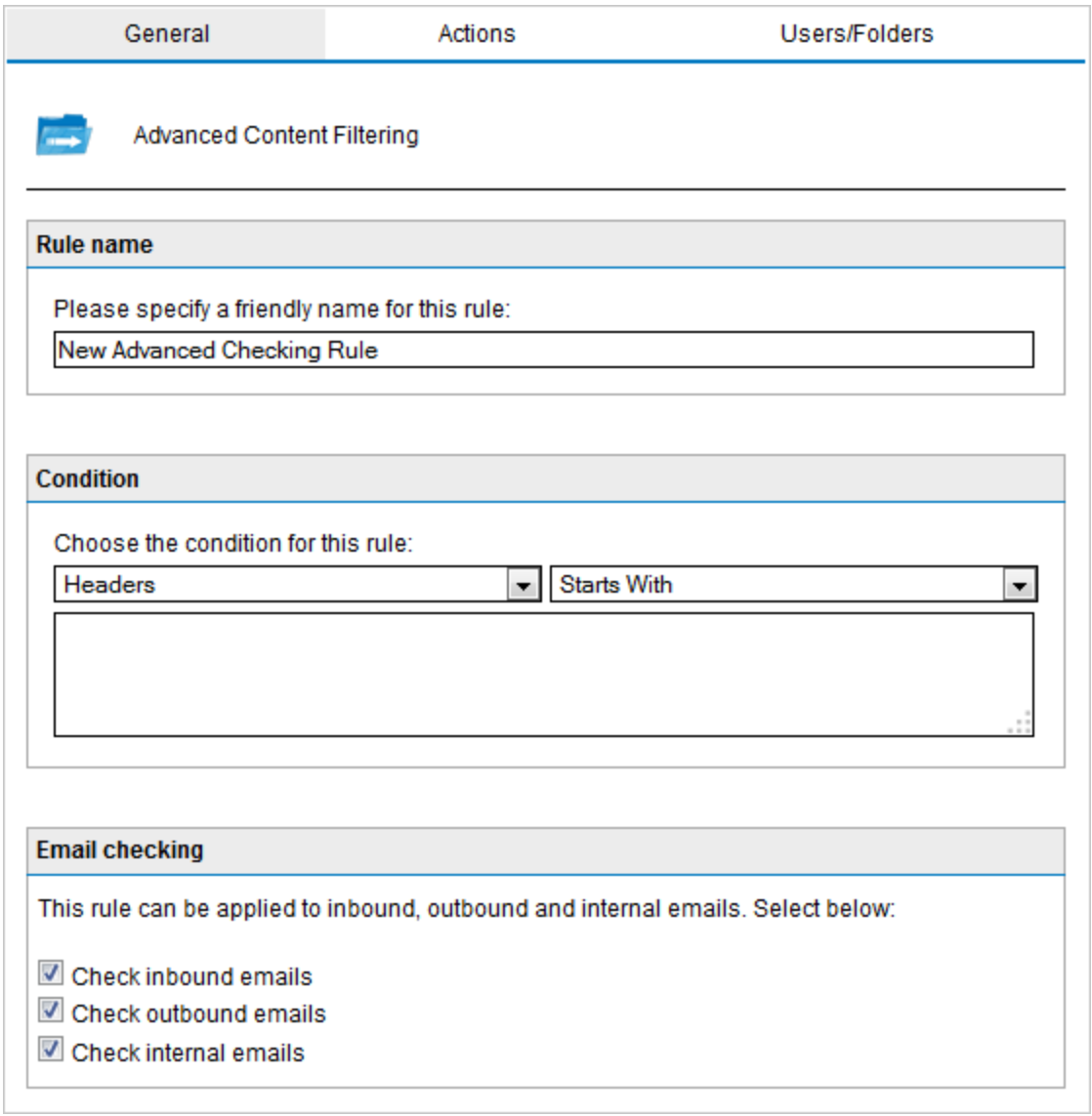
7.3.1 Criar regras de filtragem de conteúdo avançadas

Para criar uma regra de filtragem de conteúdo avançada, siga estas etapas:

- Etapa 1: Configurar definições de regra básicas e condições a serem bloqueadas
- Etapa 2: Configurar as ações a serem tomadas nos emails detectados
- Etapa 3: Especificar os usuários aos quais aplicar esta regra

Etapa 1: Configurar definições de regra básicas e condições para bloquear

1. Acesse **Content Filtering > Advanced Content Filtering** e clique em **Add Rule...**



Screenshot 104: Adicionar uma nova regra de filtragem de conteúdo avançada

2. Na área **Rule Name**, forneça um nome para a nova regra.

3. Na área **Condition**, forneça a condição que o email tem para atender a essa regra. Na lista suspensa, selecione a parte do email (**Header**,**Subject**, **Body**, **Attachment Name** ou **Attachment Content**) e escolha uma condição (**Start with**, **Ends with**, **Contains**, **Matches Exactly**, **Matches Regex**). Na caixa de texto, digite a palavra-chave ou a expressão regular à qual o email deve corresponder.

> **Por exemplo:** Para fazer a correspondência com emails que têm `suíça` no assunto - Selecione **Subject** e **Contains** e digite em `suíça` na caixa de texto.

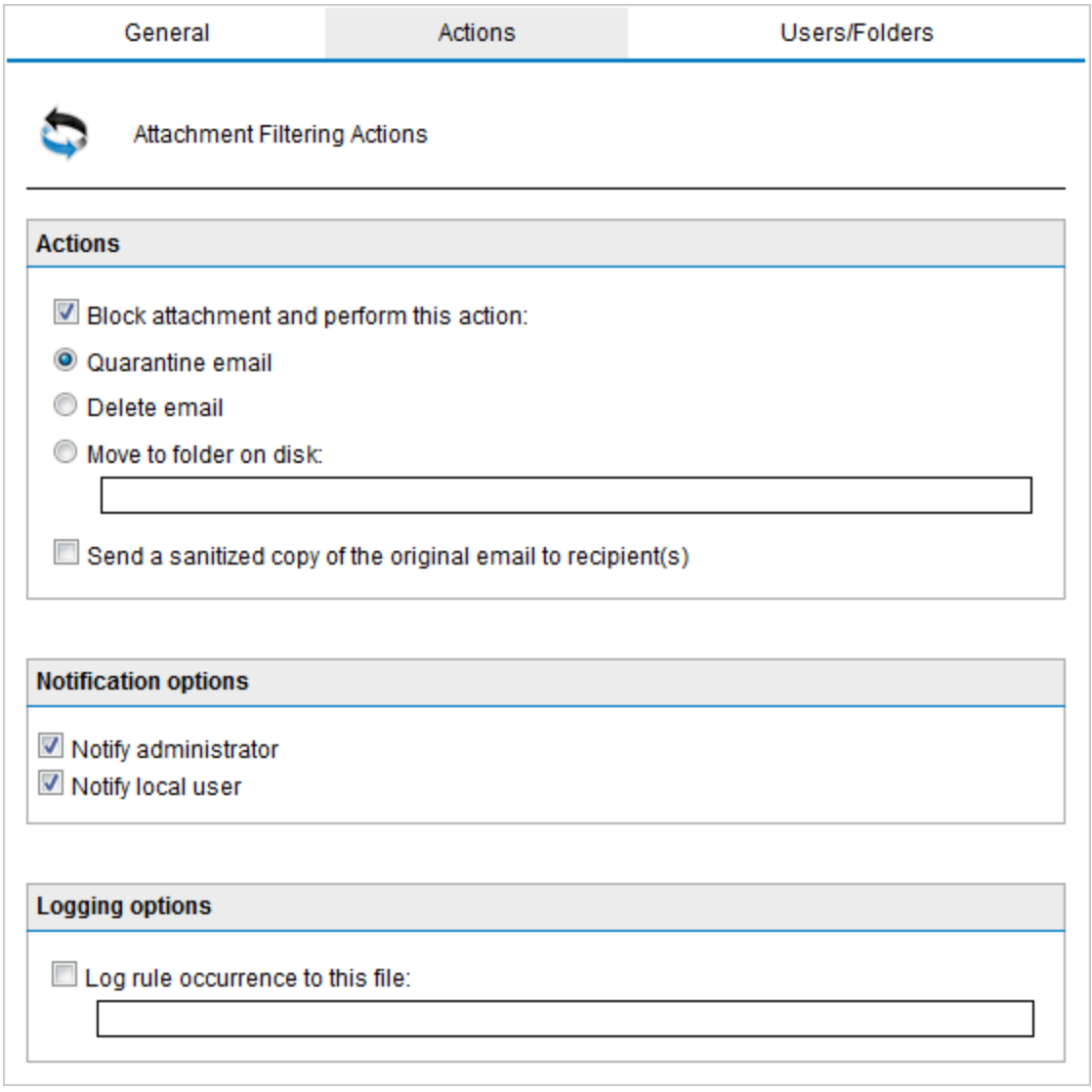
4. Selecione se deseja fazer a verificação dos emails de entrada, saída e/ou internos.

Opção	Descrição
Check Inbound emails	Selecione esta opção para verificar emails de entrada
Check Outbound emails	Selecione esta opção para verificar emails de saída

Opção	Descrição
Check Internal emails	Selecione esta opção para fazer a verificação de emails internos. **OBS.** Esta opção só estará disponível quando GFI MailEssentials estiver instalado no servidor Microsoft® Exchange

Etapa 2: Definir as ações a serem executadas em emails detectados

1. Na guia **Actions**, configure o que acontece quando essa regra for acionada.



Screenshot 105: Guia Ações

2. Para bloquear um email que corresponda às condições da regra, selecione **Block email and perform this action** e uma das seguintes opções:

Opção	Descrição
Quarantine email	Armazena emails bloqueados no armazenamento da quarentena. Em seguida, você pode analisar (aprovar/excluir) todos os emails em quarentena. Para obter mais informações, consulte Quarentena (página 203).

Opção	Descrição
Delete email	Exclui emails bloqueados.
Move to folder on disk	Move o email para uma pasta no disco. Digite o caminho completo da pasta onde guardar os emails bloqueados.

IMPORTANTE

As ações sempre afetam todo o email que contém o conteúdo bloqueado, mesmo se houver outro conteúdo (como anexos) que não acione essa regra.

OBS.

Quando o GFI MailEssentials estiver instalado na mesma máquina do Microsoft® Exchange 2003, o GFI MailEssentials pode não ser capaz de bloquear emails de saída. Em vez disso, ele substitui o conteúdo bloqueado por um relatório de ameaça.

3. Selecione **Send a sanitized copy of the original email to recipient(s)** para escolher se deseja enviar uma cópia do email bloqueado para os destinatários, mas com o conteúdo malicioso removido.

4. O GFI MailEssentials pode enviar notificações por email quando um email acionar esse filtro. Para ativar esse recurso, selecione uma das seguintes opções:

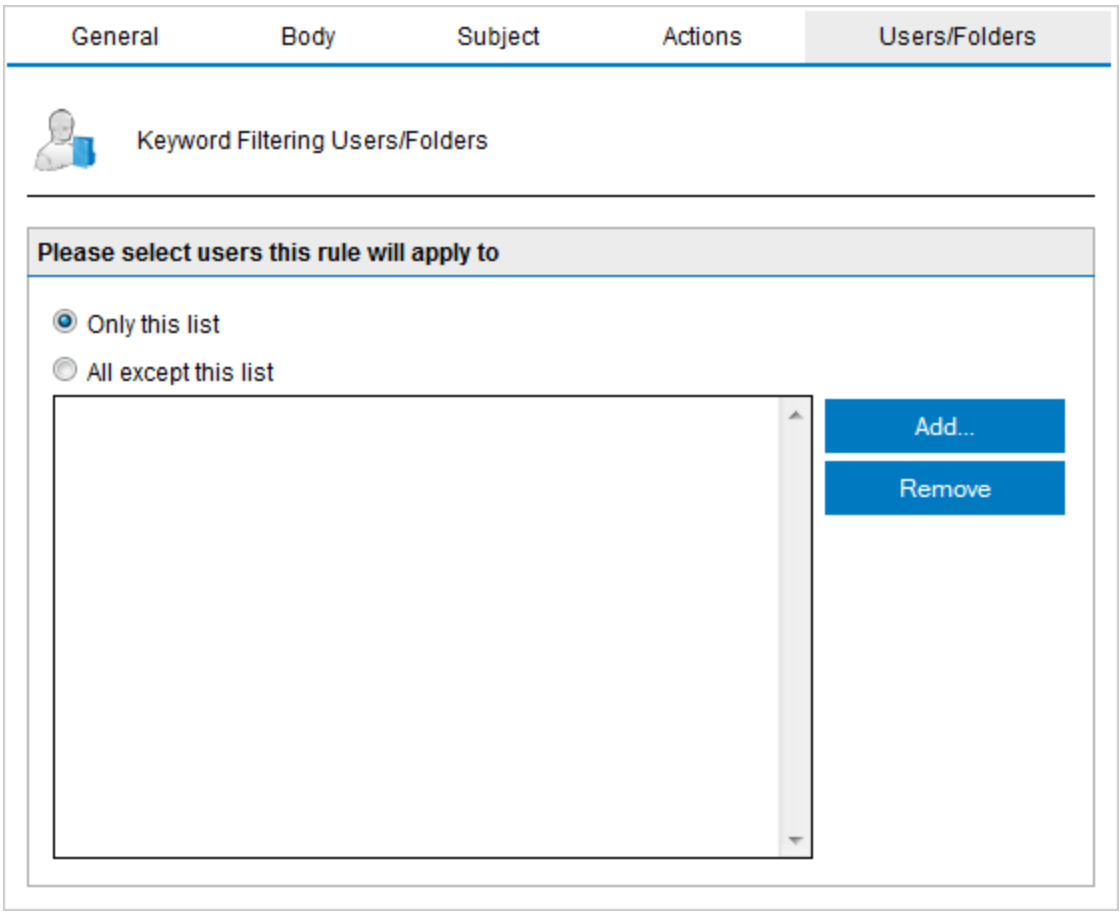
Opção	Descrição
Notify administrator	Notifique o administrador sempre que esse mecanismo bloquear uma mensagem de email. Para obter mais informações, consulte Endereço de email do administrador (página 240).
Notify local user	Notifique os destinatários locais de email sobre o email bloqueado.

5. Para registrar a atividade deste mecanismo em um arquivo de registro, selecione **Log occurrence to this file**. Na caixa de texto, especifique o caminho e o nome do arquivo para um local personalizado no disco onde armazenar o arquivo de registro. Por padrão, os arquivos de registro são armazenados em:

```
<GFI MailEssentials installation path>\GFI\MailEssentials\EmailSecurity\Logs\<Nome do mecanismo>.log
```

Etapa 3: Especificar os usuários aos quais esta regra se aplica

1. Por padrão, a regra será aplicada a todos os usuários de email. No entanto, o GFI MailEssentials permite aplicar essa regra a uma lista personalizada de usuários de email especificados na guia Users / Folders.

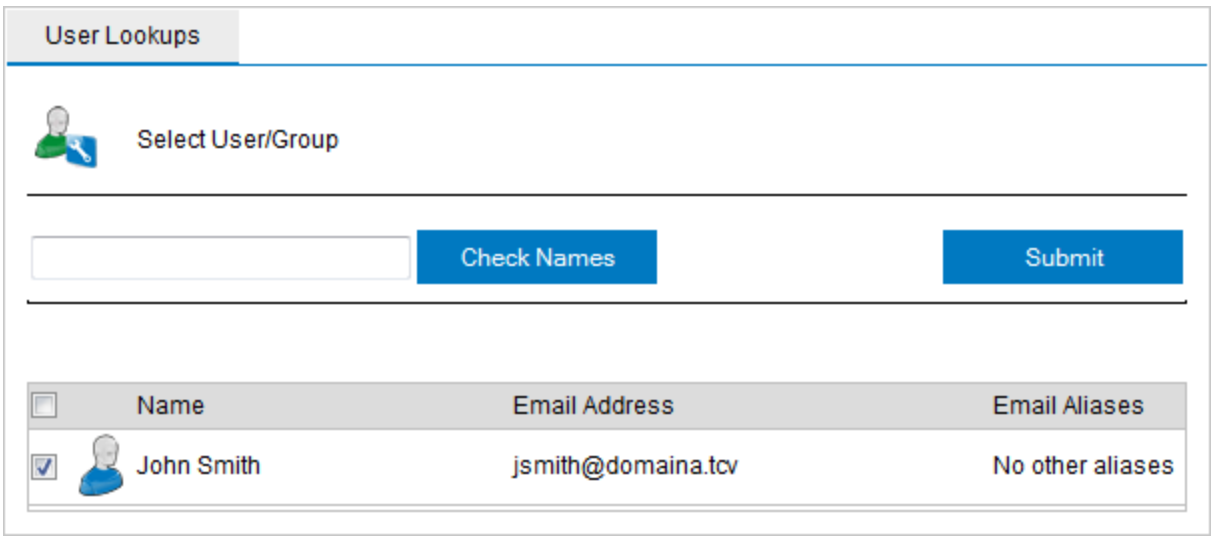


Screenshot 106: Filtragem de conteúdo: Guia Users/Folders

2. Especifique os usuários aos quais aplicar essa regra.

Opção	Descrição
Only this list	Aplique esta regra a uma lista personalizada de usuários de email, grupos ou pastas públicas.
All except this list	Aplique esta regra a todos os usuários de email, exceto aos usuários, grupos ou pastas públicas especificados na lista.

3. Para adicionar os usuários de email, grupos de usuários e/ou pastas públicas à lista, clique em **Add**.



Screenshot 107: Adicionar usuários à regra de Filtragem de conteúdo

4. Na janela **User Lookups**, especifique o nome do usuário de email/grupo de usuários ou pasta pública que você deseja adicionar à lista e clique em **Check Names**. Os usuários, grupos ou pastas públicas correspondentes são listados abaixo.

> **OBS.**
> Você não precisa digitar o nome completo dos usuários, grupos ou pastas públicas. Basta digitar parte do nome. GFI MailEssentials listará todos os nomes que contenham os caracteres especificados. Por exemplo, se você inserir `sco`, o GFI MailEssentials retornará nomes como `Scott Adams` e `Freeman Prescott`, se estiverem disponíveis.

5. Selecione a caixa de seleção ao lado dos nomes que você deseja adicionar à lista e clique em **OK**.

> **OBS.**
> Para remover entradas da lista, selecione o usuário/grupo de usuários/pasta pública que deseja remover e clique em **Remove**.

6. Repita as etapas de 3 a 5 para adicionar todos os usuários necessários para a lista.

7. Clique em **Apply**.

7.3.2 Remover regras

1. Em **Content Filtering > Advanced Content Filtering**, selecione a regra a ser removida.

2. Clique em **Remove Selected**.

7.3.3 Habilitar/desabilitar regras

1. Em **Content Filtering > Advanced Content Filtering**, selecione a regra a ser habilitada/desabilitada.

2. Clique em **Disable Selected** para desativar a regra ou **Enable Selected** para ativá-la.

7.3.4 Ordenação de regras

Regras de filtragem de conteúdo avançadas são aplicadas na mesma ordem, de cima para baixo, como estão listadas na página de filtragem de conteúdo avançada (isto é, a regra com prioridade 1 é verificada primeiro). Para alterar a sequência/prioridade de regras:

1. Acesse o nó **Content Filtering > Advanced Content Filtering**.

2. Clique nas setas (para cima) ou (para baixo), respectivamente, para aumentar ou diminuir a prioridade da regra.

3. Repita a etapa 2 até que as regras estejam na sequência desejada.

7.4 Mecanismo de descompactação

O mecanismo de descompactação extrai e analisa arquivos compactados anexados a um email.

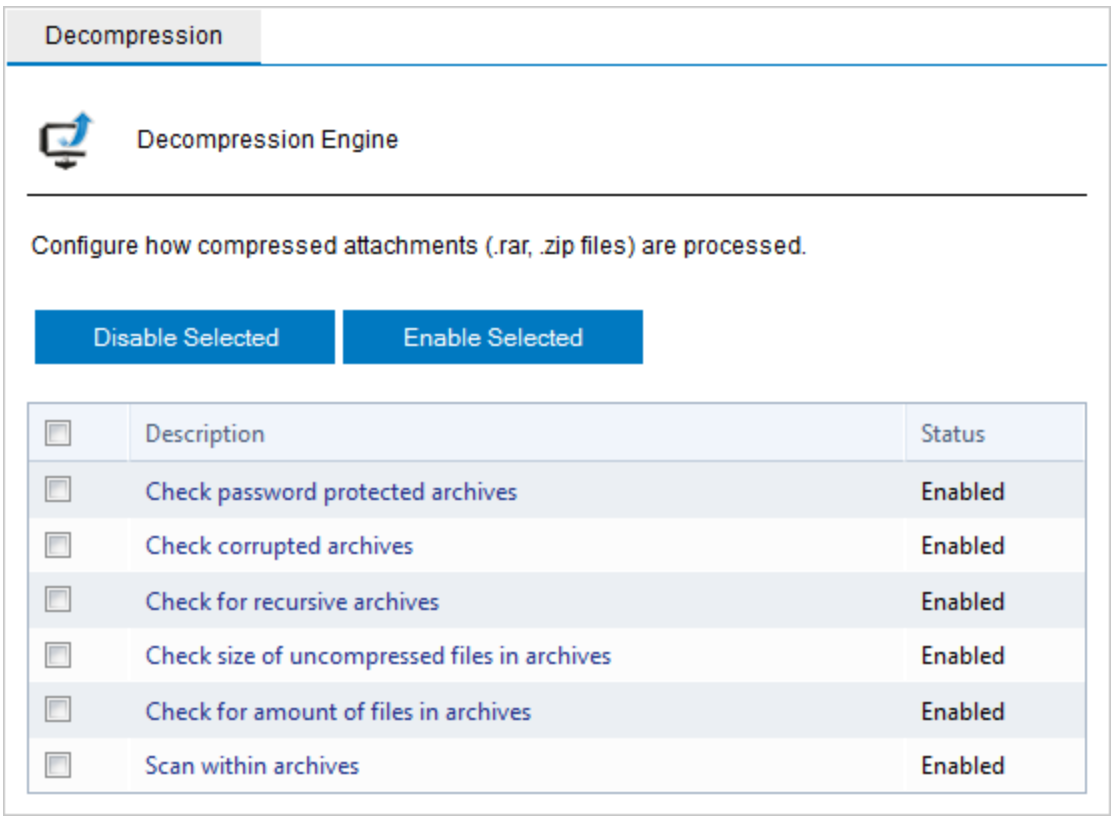
Veja a seguir uma lista de verificações executadas pelo mecanismo de descompactação.

- Arquivos protegidos por senha
- Arquivos corrompidos
- Arquivamento recursivo
- Tamanho dos arquivos descompactados em arquivos compactados
- Quantidade de arquivos compactados
- Como verificar arquivos

7.4.1 Configurar os filtros do mecanismo de descompactação

Para configurar os filtros do mecanismo de descompactação:

1. Acesse o nó **Content Filtering > Decompression**.



Screenshot 108: Verificações do mecanismo de descompactação

2. Clique no filtro de descompactação para configurar:

- Verificar arquivos protegidos por senha
- Verificar arquivos corrompidos
- Verificar arquivos recursivos
- Verificar o tamanho dos arquivos descompactados nos arquivos
- Verificar a quantidade de arquivos arquivados
- Verificar arquivos internos

Verificar arquivos protegidos por senha

1. Acesse o nó **Content Filtering > Decompression**.

2. Na lista de filtros disponíveis, clique em **Check password protected archives**.

3. Para habilitar esse filtro, selecione **Check password protected archives**.

4. Especifique o que deve ser feito quando um email contiver um arquivo que acione este filtro:

Opção	Descrição
Quarantine	Emails bloqueados em quarentena
Automatically Delete	Exclui emails bloqueados

> **OBS.**
> Quando o GFI MailEssentials estiver instalado na mesma máquina do Microsoft® Exchange 2003, o GFI MailEssentials pode não ser capaz de bloquear emails de saída. Em vez disso, ele substitui o conteúdo bloqueado por um relatório de ameaça.

5. Selecione **Send a sanitized copy of the original email to recipient(s)** para escolher se deseja enviar uma cópia do email bloqueado para os destinatários.

6. Clique na guia **Actions** para configurar outras ações.

7. O GFI MailEssentials pode enviar notificações por email quando um email acionar esse filtro. Para ativar esse recurso, selecione uma das seguintes opções:

Opção	Descrição
Notify administrator	Notifique o administrador sempre que esse mecanismo bloquear uma mensagem de email. Para obter mais informações, consulte Endereço de email do administrador (página 240).
Notify local user	Notifique os destinatários locais de email sobre o email bloqueado.

8. Para registrar a atividade deste mecanismo em um arquivo de registro, selecione **Log occurrence to this file**. Na caixa de texto, especifique o caminho e o nome do arquivo para um local personalizado no disco onde armazenar o arquivo de registro. Por padrão, os arquivos de registro são armazenados em:

```
<GFI MailEssentials installation path>\GFI\MailEssentials\EmailSecurity\Logs\<Nome do mecanismo>.log
```

9. Clique em **Apply**.

Como verificar arquivos corrompidos

1. Acesse o nó **Content Filtering > Decompression**.

2. Na lista de filtros disponíveis, clique em **Check corrupted archives**.

3. Para habilitar esse filtro selecione **Check corrupted archives**.

4. Especifique o que deve ser feito quando um email contiver um arquivo que acione este filtro:

Opção	Descrição
Quarantine	Emails bloqueados em quarentena
Automatically Delete	Exclui emails bloqueados

> **OBS.**
> Quando o GFI MailEssentials estiver instalado na mesma máquina do Microsoft® Exchange 2003, o GFI MailEssentials pode não ser capaz de bloquear emails de saída. Em vez disso, ele substitui o conteúdo bloqueado por um relatório de ameaça.

5. Selecione **Send a sanitized copy of the original email to recipient(s)** para escolher se deseja enviar uma cópia do email bloqueado para os destinatários.

6. Clique na guia **Actions** para configurar outras ações.

7. O GFI MailEssentials pode enviar notificações por email quando um email acionar esse filtro. Para ativar esse recurso, selecione uma das seguintes opções:

Opção	Descrição
Notify administrator	Notifique o administrador sempre que esse mecanismo bloquear uma mensagem de email. Para obter mais informações, consulte Endereço de email do administrador (página 240).
Notify local user	Notifique os destinatários locais de email sobre o email bloqueado.

8. Para registrar a atividade deste mecanismo em um arquivo de registro, selecione **Log occurrence to this file**. Na caixa de texto, especifique o caminho e o nome do arquivo para um local personalizado no disco onde armazenar o arquivo de registro. Por padrão, os arquivos de registro são armazenados em:

```
<GFI MailEssentials installation path>\GFI\MailEssentials\EmailSecurity\Logs\<Nome do mecanismo>.log
```

9. Clique em **Apply**

Como verificar arquivos recursivos

Este filtro permite que você coloque em quarentena ou exclua os emails que contêm arquivos recursivos. Arquivos recursivos, também conhecidos como arquivos aninhados, são arquivos que contêm vários níveis de sub-arquivos (ou seja, arquivos dentro de arquivos). Um grande número de níveis de arquivos pode indicar um arquivo mal-intencionado. Arquivos recursivos podem ser utilizados em um ataque DoS (Negação de Serviço), pois os arquivos recursivos consomem os recursos da máquina que estão sendo analisados. Para configurar este filtro:

1. Acesse o nó **Content Filtering > Decompression**.

2. Na lista de filtros disponíveis, clique em **Check for recursive archives**.

3. Para habilitar esse filtro, selecione **Check for recursive archives**.

4. Especifique o número máximo de arquivos de forma recorrente na caixa de texto **Maximum number of recurring archives**. Se um arquivo contiver mais arquivos recorrentes do que um número especificado, o email será definido como mal-intencionado.

5. Especifique o que deve ser feito quando um email contiver um arquivo que acione este filtro:

Opção	Descrição
Quarantine	Emails bloqueados em quarentena
Automatically Delete	Exclui emails bloqueados

> **OBS.**
> Quando o GFI MailEssentials estiver instalado na mesma máquina do Microsoft® Exchange 2003, o GFI MailEssentials pode não ser capaz de bloquear emails de saída. Em vez disso, ele substitui o conteúdo bloqueado por um relatório de ameaça.

6. Selecione **Send a sanitized copy of the original email to recipient(s)** para escolher se deseja encaminhar uma cópia do email bloqueado para os destinatários, mas com o conteúdo mal-intencionado removido.

7. Clique na guia **Actions** para configurar outras ações.

8. O GFI MailEssentials pode enviar notificações por email quando um email acionar esse filtro. Para ativar esse recurso, selecione uma das seguintes opções:

Opção	Descrição
Notify administrator	Notifique o administrador sempre que esse mecanismo bloquear uma mensagem de email. Para obter mais informações, consulte Endereço de email do administrador (página 240).
Notify local user	Notifique os destinatários locais de email sobre o email bloqueado.

9. Para registrar a atividade deste mecanismo em um arquivo de registro, selecione **Log occurrence to this file**. Na caixa de texto, especifique o caminho e o nome do arquivo para um local personalizado no disco onde armazenar o arquivo de registro. Por padrão, os arquivos de registro são armazenados em:

```
<GFI MailEssentials installation path>\GFI\MailEssentials\EmailSecurity\Logs\<Nome do mecanismo>.log
```

10. Clique em **Apply**.

Como verificar o tamanho de arquivos descompactados

Esse filtro permite que você bloqueie ou exclua emails com arquivos que excedam o tamanho físico especificado quando não estiverem compactados. Às vezes, os hackers usam esse método de ataque DoS (Negação de Serviço) enviando um arquivo compactado que pode estar sem compactação para um arquivo muito grande que consome espaço no disco rígido e leva muito tempo para ser analisado pela segurança de conteúdo ou pelo software antivírus.

Para configurar este filtro:

1. Acesse o nó **Content Filtering > Decompression**.

2. Na lista de filtros disponíveis, clique em **Check size of uncompressed files in archives**.

3. Para habilitar esse filtro, selecione **Check size of uncompressed files in archives**.

4. Especifique o tamanho máximo dos arquivos descompactados na caixa de texto **Maximum size of uncompressed files in archive in MB**. Se o tamanho de um arquivo descompactado for maior que o

valor especificado, o email será definido como mal-intencionado.

5. Especifique o que deve ser feito quando um email contiver um arquivo que acione este filtro:

Opção	Descrição
Quarantine	Emails bloqueados em quarentena
Automatically Delete	Exclui emails bloqueados

> **OBS.**
> Quando o GFI MailEssentials estiver instalado na mesma máquina do Microsoft® Exchange 2003, o GFI MailEssentials pode não ser capaz de bloquear emails de saída. Em vez disso, ele substitui o conteúdo bloqueado por um relatório de ameaça.

6. Selecione **Send a sanitized copy of the original email to recipient(s)** para escolher se deseja enviar uma cópia do email bloqueado para os destinatários, mas com o conteúdo malicioso removido.

7. O GFI MailEssentials pode enviar notificações por email quando um email acionar esse filtro. Para ativar esse recurso, selecione uma das seguintes opções:

Opção	Descrição
Notify administrator	Notifique o administrador sempre que esse mecanismo bloquear uma mensagem de email. Para obter mais informações, consulte Endereço de email do administrador (página 240).
Notify local user	Notifique os destinatários locais de email sobre o email bloqueado.

8. Para registrar a atividade deste mecanismo em um arquivo de registro, selecione **Log occurrence to this file**. Na caixa de texto, especifique o caminho e o nome do arquivo para um local personalizado no disco onde armazenar o arquivo de registro. Por padrão, os arquivos de registro são armazenados em:

```
<GFI MailEssentials installation path>\GFI\MailEssentials\EmailSecurity\Logs\<Nome do mecanismo>.log
```

9. Clique em **Apply**.

Como verificar a quantidade de arquivos

Este filtro permite que você coloque em quarentena ou excluía os emails que contenham um excesso de arquivos compactados dentro de um arquivo anexo. Você pode especificar o número de arquivos permitidos nos anexos com arquivos compactados nas opções de configuração desse filtro. Para configurar este filtro:

1. Acesse o nó **Content Filtering > Decompression**.

2. Na lista de filtros disponíveis, clique em **Check for amount of files in archives**.

3. Para habilitar esse filtro, selecione **Check for amount of files in archives**.

4. Especifique o número máximo de arquivos compactados na caixa de texto **If the number of files within archive exceeds**. Se o arquivo compactado contiver mais arquivos que o valor especificado, o email será definido como mal-intencionado.

5. Especifique o que deve ser feito quando um email contiver um arquivo que acione este filtro:

Opção	Descrição
Quarantine	Emails bloqueados em quarentena
Automatically Delete	Exclui emails bloqueados

> **OBS.**
> Quando o GFI MailEssentials estiver instalado na mesma máquina do Microsoft® Exchange 2003, o GFI MailEssentials pode não ser capaz de bloquear emails de saída. Em vez disso, ele substitui o conteúdo bloqueado por um relatório de ameaça.

6. Selecione **Send a sanitized copy of the original email to recipient(s)** para escolher se deseja enviar uma cópia do email bloqueado para os destinatários.

7. Clique na guia **Actions** para configurar outras ações.

8. O GFI MailEssentials pode enviar notificações por email quando um email acionar esse filtro. Para ativar esse recurso, selecione uma das seguintes opções:

Opção	Descrição
Notify administrator	Notifique o administrador sempre que esse mecanismo bloquear uma mensagem de email. Para obter mais informações, consulte Endereço de email do administrador (página 240).
Notify local user	Notifique os destinatários locais de email sobre o email bloqueado.

9. Para registrar a atividade deste mecanismo em um arquivo de registro, selecione **Log occurrence to this file**. Na caixa de texto, especifique o caminho e o nome do arquivo para um local personalizado no disco onde armazenar o arquivo de registro. Por padrão, os arquivos de registro são armazenados em:

```
<GFI MailEssentials installation path>\GFI\MailEssentials\EmailSecurity\Logs\<Nome do mecanismo>.log
```

10. Clique em **Apply**.

Como verificar arquivos internos

Você pode configurar o GFI MailEssentials para aplicar a filtragem de palavra-chave e de anexos a arquivos dentro de arquivos compactados.

1. Acesse o nó **Content Filtering > Decompression**.

2. Na lista de filtros disponíveis, clique em **Scan within archives**.

3. Para ativar a verificação de arquivos compactados, selecione **Apply Attachment and Content Filtering rules within archives**. Para obter mais informações, consulte Filtragem de conteúdo (página 176).

4. Clique em **Apply**.

7.4.2 Habilitar/desabilitar filtros de descompactação

Para ativar ou desativar filtros de descompactação:

1. Acesse o nó **Content Filtering > Decompression**.

2. Na página **Decompression engine**, selecione a caixa de texto dos filtros a serem habilitados ou desabilitados.

3. Clique em **Enable Selected** ou **Disable Selected**.

8 Quarentena

O recurso Quarentena do GFI MailEssentials oferece um repositório central onde todas as mensagens detectadas como spam ou malware são mantidas. Isso garante que os usuários não receberão spam e malware nas caixas de correio e o processamento no servidor de emails será reduzido.

Os administradores de correio eletrônico e os usuários podem analisar emails em quarentena acessando a interface de quarentena a partir de um navegador da Web. GFI MailEssentials também pode enviar relatórios de email regulares para os usuários de email para verificar emails bloqueados.

Consulte as seguintes seções para obter mais informações sobre como configurar a Quarentena do GFI MailEssentials.

8.1 Observações importantes

1. Para colocar em quarentena spam ou emails mal-intencionados, altere os filtros e as ações dos mecanismos para **Quarantine email**.

2. O Quarantine Store requer espaço em disco para reter emails de spam ou malware da organização por um determinado número de dias. A quantidade de espaço em disco necessária depende dos seguintes fatores:

- Quantidade de emails recebidos
- Por quanto tempo são mantidos.

3. Em média, 100.000 mensagens de spam ou malware de 5 KB cada necessitarão de aproximadamente 600 MB de espaço em disco para armazenar os emails e seus metadados.

4. Se o espaço livre em disco em que o Quarantine Store é salvo for 512 MB ou menos, o GFI MailEssentials não interromperá spam e malware. Ele é identificado e enviado para as caixas de correio dos destinatários até que o espaço livre em disco aumente para mais de 512 MB. Isso garante que o disco não ficará sem espaço.

8.2 Como pesquisar na quarentena

O Quarantine Store pode ser acessado a partir da interface do GFI MailEssentials e permite o gerenciamento de emails em quarentena.

Para acessar o Quarantine Store do GFI MailEssentials, acesse **GFI MailEssentials > Quarantine**.

Existem diversas maneiras de pesquisar conteúdo na quarentena do GFI MailEssentials:

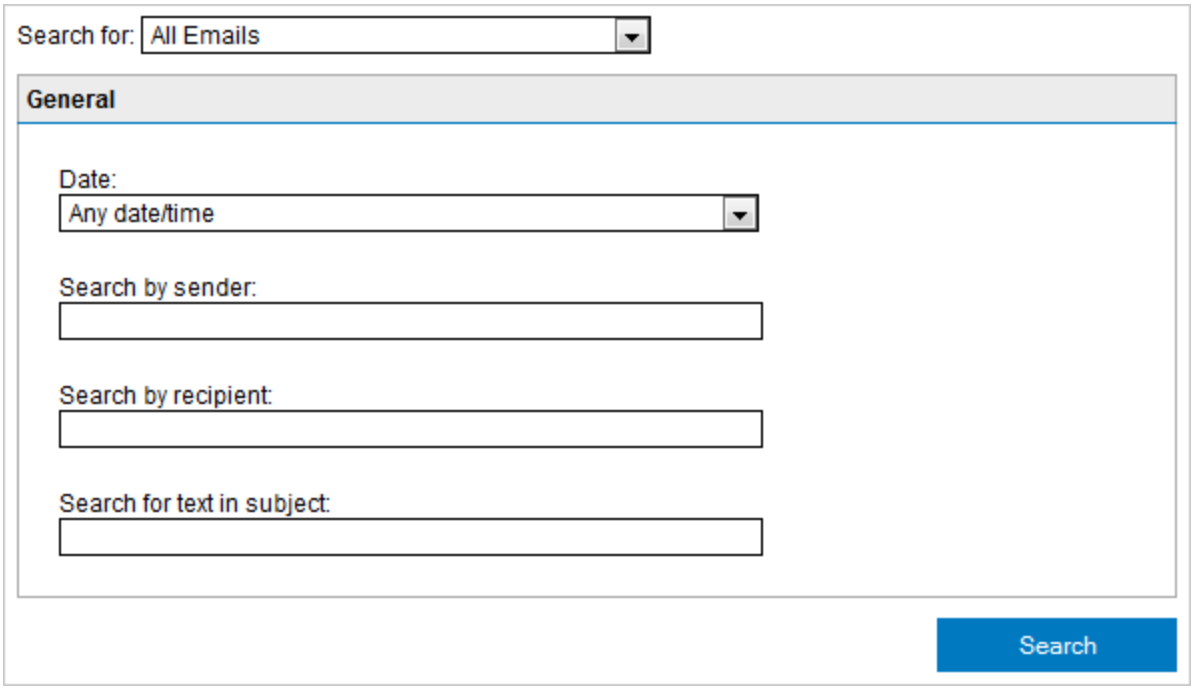
» Pesquisar malware e spam em quarentena

» Pesquisar apenas emails com malware

» Pesquisar apenas emails com spam

Pesquisar emails com malware e spam

1. Acesse **GFI MailEssentials > Quarantine**.



Screenshot 109: Área de pesquisa de malware and spam

2. Na página **Quarantine**, selecione **All Emails** na lista suspensa **Search for**.

3. Especifique o critério de pesquisa.

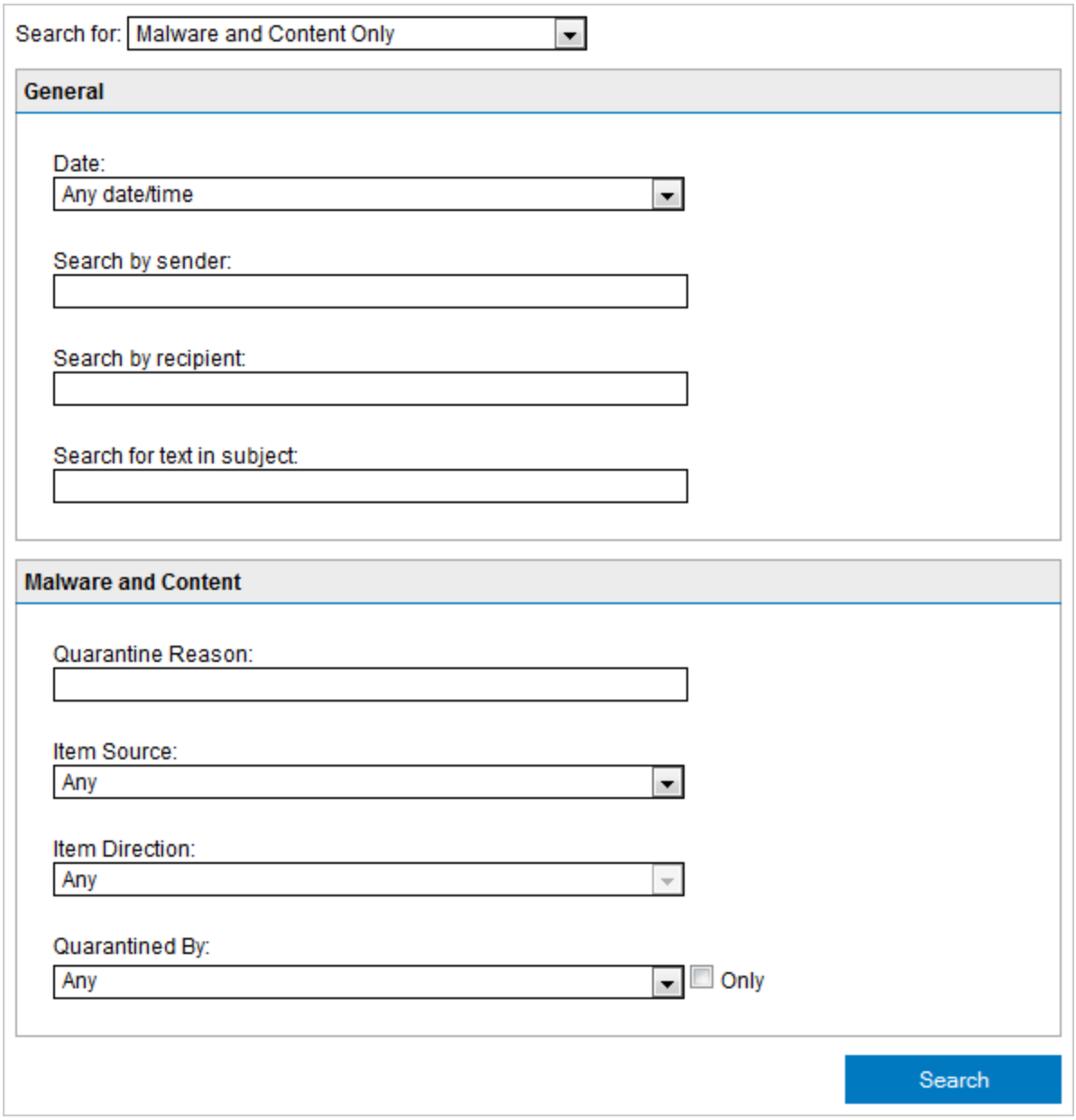
CRITÉRIOS DE PESQUISA	DESCRIÇÃO
Date:	Selecione o intervalo de datas durante o qual o email foi colocado em quarentena. Intervalos de datas disponíveis: » Qualquer data/hora » Desde ontem » Últimos sete dias » Últimos 30 dias » Intervalo de datas personalizado
Search by sender	Especifique o remetente do email colocado em quarentena.
Search by recipient	Especifique o destinatário de email em quarentena.
Search for text in subject	Especifique o texto a ser pesquisado no assunto do email em quarentena.

4. Clique em **Search**.

OBS.
Use os resultados da pesquisa para analisar emails em quarentena. Você pode aprovar falsos positivos para que eles sejam entregues aos destinatários. Para obter mais informações, consulte Trabalhar com emails em quarentena (página 211).

Pesquisar apenas malware e conteúdo

1. Acesse **GFI MailEssentials > Quarantine**.



Screenshot 110: Área de pesquisa de malware e spam

2. Na página **Quarantine**, selecione **Malware and Content Only** na lista suspensa **Search for**.

3. Especifique o critério de pesquisa.

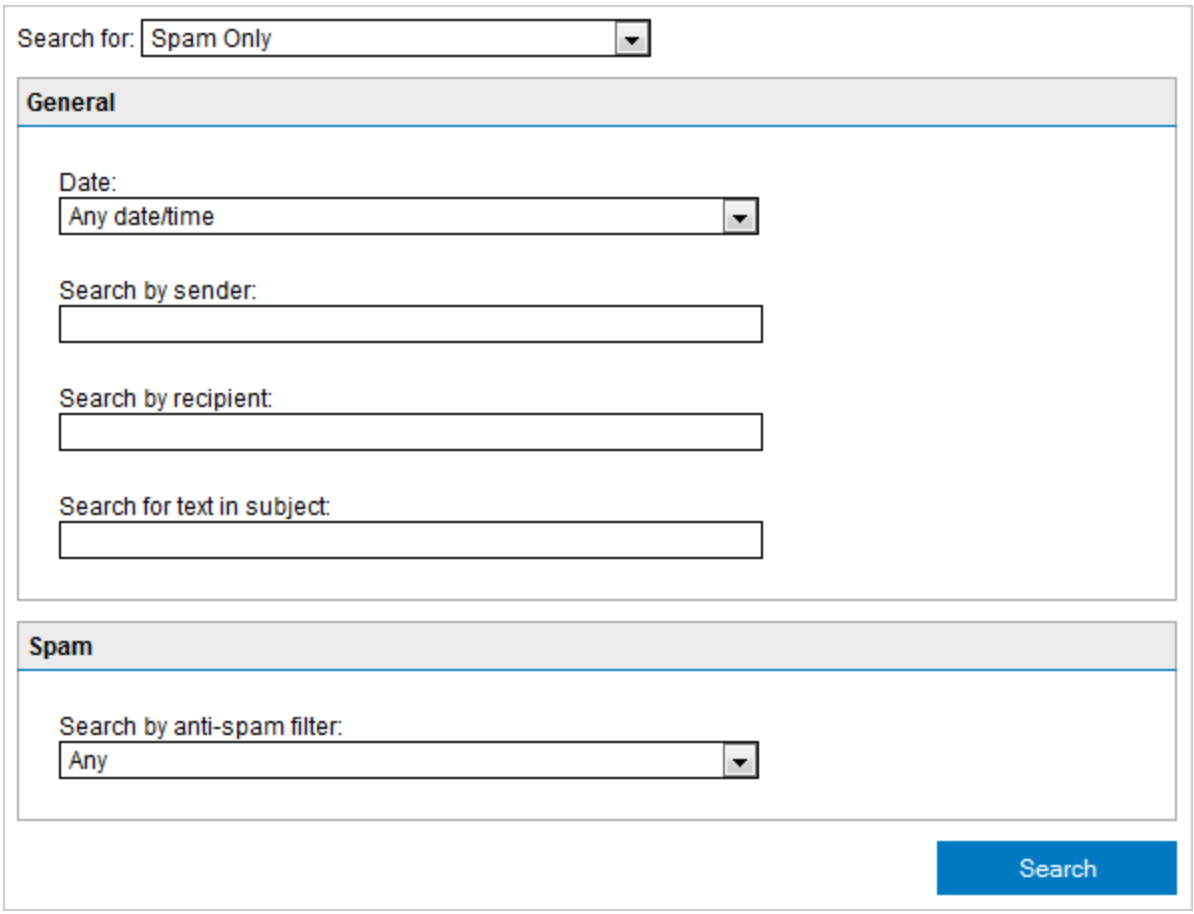
CRITÉRIOS DE PESQUISA	DESCRIÇÃO
Date:	Selecione o intervalo de datas durante o qual o email foi colocado em quarentena. Intervalos de datas disponíveis: » Qualquer data/hora » Desde ontem » Últimos sete dias » Últimos 30 dias » Intervalo de datas personalizado
Search by sender	Especifique o remetente do email colocado em quarentena.
Search by recipient	Especifique o destinatário de email em quarentena.
Search for text in subject	Especifique o texto a ser pesquisado no assunto do email em quarentena.
Quarantine Reason	Digite o motivo pelo qual o email a ser procurado foi colocado em quarentena.
Item Source	Selecione a origem de onde email foi identificado como malware e colocado em quarentena. As opções disponíveis são: » Armazenamento de informações (VSAPI) » Gateway (SMTP) » Armazenamento de informações (Transport)
Item Direction	Selecione a direção dos emails em quarentena a serem pesquisados » Qualquer » Entrada » Saída **OBS.** Esta opção estará disponível apenas se o **Gateway (SMTP)** estiver selecionado em **Item Source**.
Quarantined by	Selecione um dos filtros do GFI MailEssentials que colocaram o email em quarentena. Selecione a caixa de seleção **Only** para pesquisar somente emails colocados em quarentena por um filtro específico.

4. Clique em **Search**.

OBS.
Use os resultados da pesquisa para analisar emails em quarentena. Você pode aprovar falsos positivos para que eles sejam entregues aos destinatários. Para obter mais informações, consulte Trabalhar com emails em quarentena (página 211).

Pesquisar apenas spam

1. Acesse **GFI MailEssentials > Quarantine**.



Screenshot 111: Área de pesquisa Spam Only

2. Na página **Quarantine**, selecione **Spam Only** na lista suspensa **Search for**.

3. Especifique o critério de pesquisa. As opções disponíveis são:

CRITÉRIOS DE PESQUISA	DESCRIÇÃO
Date:	Selecione o intervalo de datas durante o qual o email foi colocado em quarentena. Intervalos de datas disponíveis: » Qualquer data/hora » Desde ontem » Últimos sete dias » Últimos 30 dias » Intervalo de datas personalizado
Search by sender	Especifique o remetente do email colocado em quarentena.
Search by recipient	Especifique o destinatário de email em quarentena.
Search for text in subject	Especifique o texto a ser pesquisado no assunto do email em quarentena.
Search by anti-spam filter	Selecione o filtro anti-spam que identificou o email a ser pesquisado como spam.

4. Clique em **Search**.

OBS.
Use os resultados da pesquisa para analisar emails em quarentena. Você pode aprovar falsos positivos para que eles sejam entregues aos destinatários. Para obter mais informações, consulte Trabalhar com emails em quarentena (página 211).

8.3 Pesquisar pastas

Uma pasta de pesquisa é uma pasta que possui uma consulta de pesquisa personalizada associada e exibe todos os emails em quarentena que correspondem à consulta de pesquisa.

Exemplos de pastas de pesquisa:

» Uma pasta de pesquisa que mostra apenas os emails em quarentena enviados pelos mecanismos de verificação de vírus.

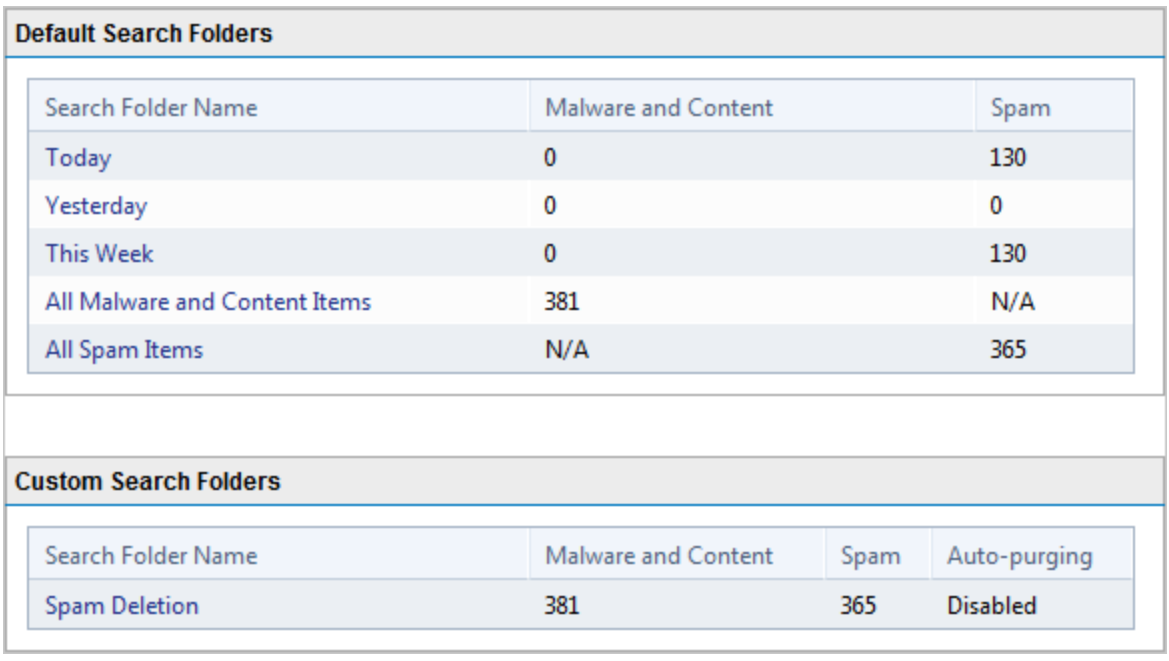
» Uma pasta de pesquisa que exibe os emails de entrada em quarentena em um determinado intervalo de datas e endereçados a um determinado usuário.

» Uma pasta de pesquisa que exibe emails que atendem a determinados critérios de pesquisa

» Uma pasta de pesquisa que exibe os resultados de uma pesquisa definida por uma consulta anterior.

Para exibir emails em uma determinada pasta de pesquisa:

1. Acesse o nó **Quarantine**.



Screenshot 112: Pastas de pesquisa padrão e personalizadas

2. Clique em uma pasta de pesquisa nas áreas **Default Search Folders** ou **Custom Search Folders**. Como alternativa, selecione um dos nós de pasta de pesquisa no nó **Quarantine** e **Quarantine > Search Folders**.

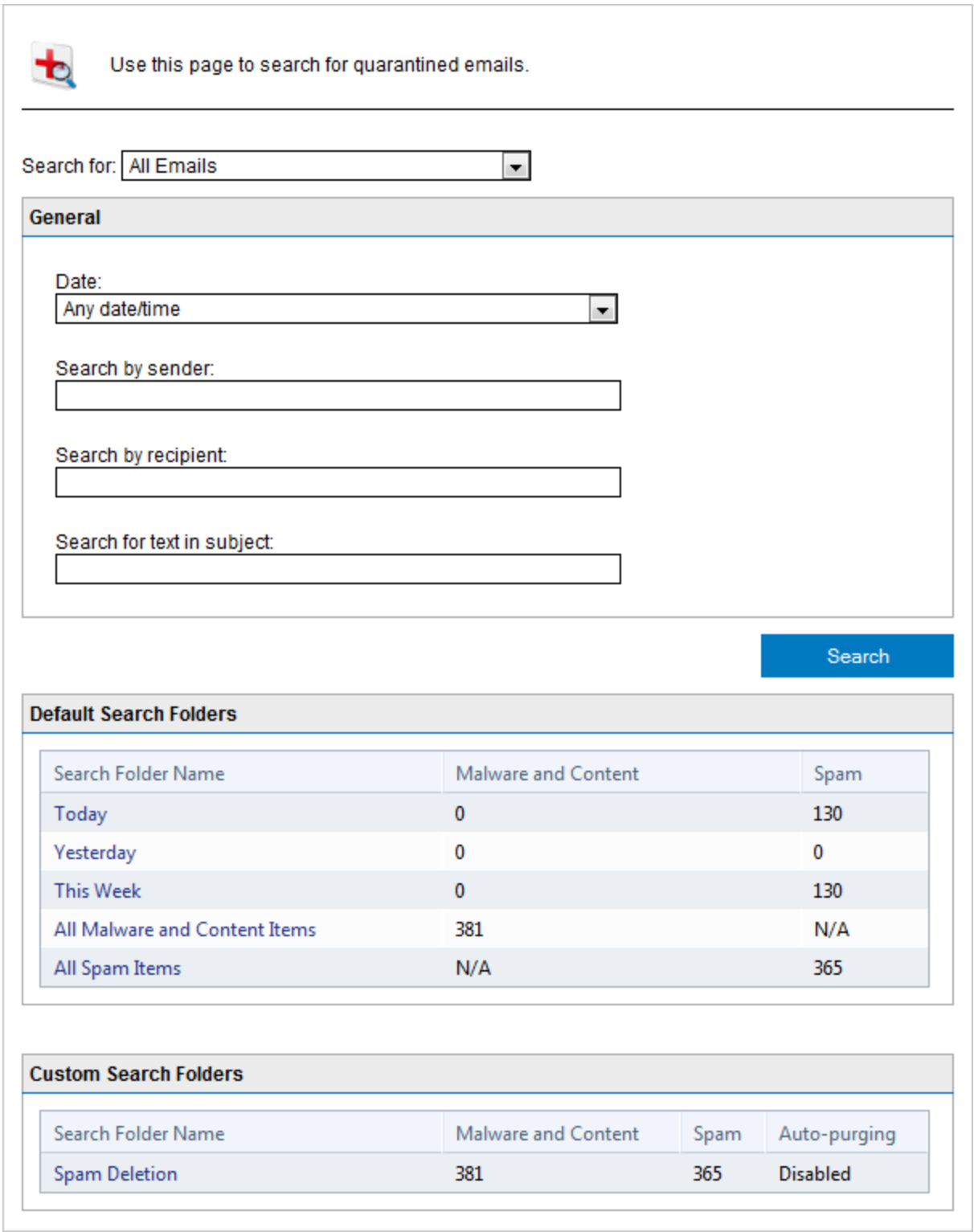
OBS.

Use os resultados da pesquisa para analisar emails em quarentena. Você pode aprovar falsos positivos para que eles sejam entregues aos destinatários. Para obter mais informações, consulte Trabalhar com emails em quarentena (página 211).

8.3.1 Pastas de pesquisa padrão

As pastas de pesquisa padrão são pastas pré-configuradas que permitem acessar emails em quarentena de acordo com períodos de tempo específicos ou um tipo específico de emails em quarentena. Para usar as pastas de pesquisa padrão:

1. Acesse o nó **Quarantine**.



Screenshot 113: Pastas de pesquisa padrão

2. Selecione uma pasta de pesquisa na área **Default Search Folders** ou em um nó do nó **Quarantine** para acessar a pasta de pesquisa.GFI MailEssentials procurará automaticamente e exibirá todos os emails em quarentena que atendam aos critérios de pesquisa da pasta de pesquisa padrão.

As pastas de pesquisa padrão disponíveis são:

» **Baseada em hora:**

- Hoje

- Ontem
- Esta semana

» **Baseada em categoria:**

- Todos os itens com malware e conteúdo
- Todos os itens com spam

> **OBS.**
> Use os resultados da pesquisa para analisar emails em quarentena. Você pode aprovar falsos positivos para que eles sejam entregues aos destinatários. Para obter mais informações, consulte Trabalhar com emails em quarentena (página 211).

8.3.2 Criar, editar e remover pastas de pesquisa personalizadas de pesquisas

1. Acesse o nó **Quarantine**.

2. Crie uma nova pesquisa para emails em quarentena. Para obter mais informações, consulte Como pesquisar na quarentena (página 203).

3. Na página de resultados, clique em **Save as Search Folder** e digite um nome de pasta facilmente identificável para a nova pasta de pesquisa.

A pasta de pesquisa recém-criada fica listada no nó **Quarantine > Search Folders**.

> **OBS.**
> Para editar ou excluir uma pasta de pesquisa criada anteriormente, acesse-a e clique em **Edit Search Folder** ou **Delete Search folder**.

8.3.3 Usar o nó Search Folders para limpar automaticamente os emails em quarentena

O nó **Search Folders** permite que você crie pastas de pesquisa e defina um valor que limpe automaticamente (em dias). Quando um email em quarentena exceder o número de dias especificados em quarentena, o email será excluído.

1. Selecione o nó **Quarantine > Search Folders**.

2. Configure uma nova pasta de pesquisa para que os emails sejam excluídos regularmente usando as instruções neste capítulo.

3. Selecione **EnableAuto-purging** e forneça o número de dias para manter os emails.

4. Clique em **Save Folder**.

8.4 Trabalhar com emails em quarentena

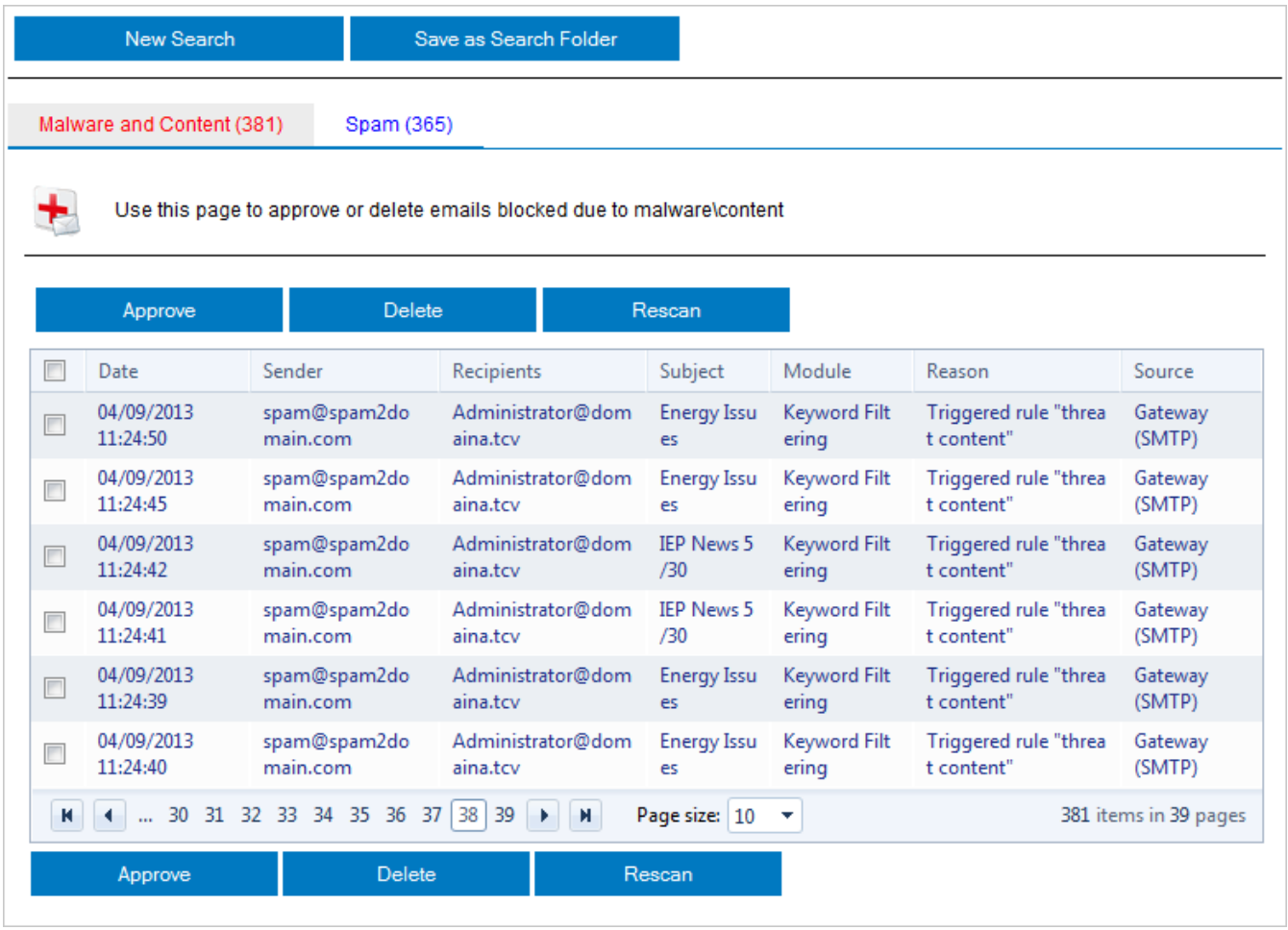
No GFI MailEssentials, há um determinado número de ações que podem ser executadas para emails em quarentena.

O armazenamento da quarentena pode ser acessado na interface do GFI MailEssentials e o administrador pode gerenciar mensagens em quarentena.

Para acessar o Quarantine Store do GFI MailEssentials, acesse **GFI MailEssentials > Quarantine**.

8.4.1 Como exibir emails em quarentena

Pesquisar na quarentena ou usar as pastas de pesquisa padrão ou personalizadas retorna uma lista de emails em quarentena.



Screenshot 114: Resultados da pesquisa

OBS.
A página de resultados pode ser dividida em duas guias:

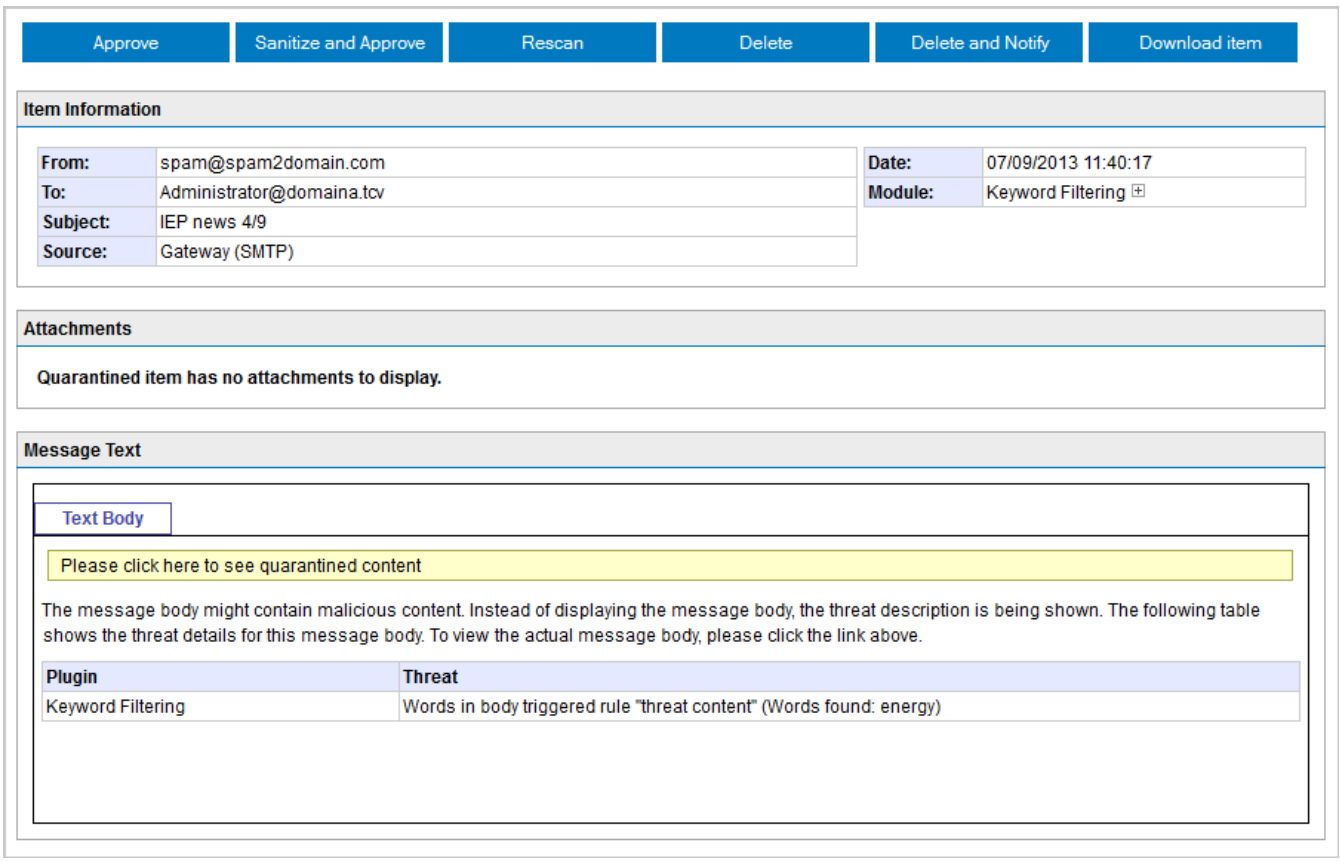
» **Malware and Content**: emails bloqueados pelo mecanismo anti-malware e por regras de filtragem de conteúdo.

» **Spam**: emails bloqueados por filtros de spam.

1. Escolha a guia **Malware and Content** ou a guia **Spam** para exibir um tipo específico de emails em quarentena. A página de resultados fornece as seguintes funções e detalhes:

Opção	Descrição
Back	Retorna à tela anterior.
Approve	Permite que você aprove um único email ou diversos emails. Para obter mais informações, consulte Aprovar os emails em quarentena (página 214).
Delete	Exclui um único email ou diversos emails. Para obter mais informações, consulte Excluir permanentemente emails em quarentena (página 214).
Rescan	Repete a verificação de emails usando as assinaturas atuais do antivírus (que pode estar mais atualizadas que as assinaturas de antivírus que colocaram o email em quarentena). Selecione uma ou mais mensagens de email e clique em **Rescan** para fazer uma nova verificação.
Module	O módulo que identificou o email como um email que deve ser colocado em quarentena.
Reason	O motivo/regra que acionou a ação de colocar o email em quarentena.
Sender	O endereço de email do remetente
Recipients	O endereço de email do destinatário
Subject	O assunto do email como enviado pelo remetente.
Date	A data na qual o email foi colocado em quarentena
Source	O local a partir do qual o email foi colocado em quarentena
Item Source	Permite selecionar uma fonte para filtrar a exibição. As opções disponíveis são: » Exibir tudo » Armazenamento de informações (VSAPI) » Gateway (SMTP) » Armazenamento de informações (Transport)
Page size	Permite personalizar quantos emails podem ser visualizados por página. Escolha um número para exibir o número máximo de itens por página.

2. Clique em uma linha para acessar detalhes de emails individuais.



Screenshot 115: Quarantined Items details

Na página **Quarantined Items details**, leia os detalhes do email e execute as ações a seguir.

Ação	Descrição
Approve	Aprove o email. Para obter mais informações, consulte Aprovar os emails em quarentena (página 214).
Sanitize and Approve	Limpar e aprovar emails. Para obter mais informações, consulte Aprovar os emails em quarentena (página 214).
Rescan	Repete a verificação de emails usando as assinaturas atuais do antivírus (que pode estar mais atualizadas que as assinaturas de antivírus que colocaram o email em quarentena).
Delete	Exclui o email. Para obter mais informações, consulte Excluir permanentemente emails em quarentena (página 214).
Delete and Notify	Exclui emails e notifica o usuário. Para obter mais informações, consulte Excluir permanentemente emails em quarentena (página 214).
Download Item	Faz o download do email em quarentena para uma localização que você escolheu no formato .eml. **Aviso:** **Os emails no armazenamento de quarentena podem ter conteúdo mal-intencionado. Use este recurso com cuidado.**

8.4.2 Aprovar os emails em quarentena

Em alguns casos, você pode querer aprovar um email bloqueado pelo GFI MailEssentials. GFI MailEssentials permite que o administrador aprove um email em quarentena para que ele seja liberado do armazenamento da quarentena e distribuído para os destinatários.

Para aprovar emails:

1. Use os recursos de pesquisa descritos nas seções anteriores para retornar uma lista de emails em quarentena.

2. Selecione a caixa de seleção próxima aos emails em quarentena a serem aprovados e clique em **Approve**.

Limpar e aprovar emails

O GFI MailEssentials também permite que você remova o item que fez com que o email fosse colocado em quarentena e envie o email para o destinatário.

Para limpar e aprovar emails:

1. Use os recursos de pesquisa descritos nas seções anteriores para retornar uma lista de emails em quarentena.

2. Clique em um email para exibir seus detalhes.

3. Clique em **Sanitize and Approve**.

> **OBS.**
> Os emails colocados em quarentena pelo Information Store (VSAPI) não podem ser limpos.

8.4.3 Excluir permanentemente emails em quarentena

1. Use os recursos descritos nas seções anteriores para retornar uma lista de emails em quarentena

2. Selecione a caixa de seleção ao lado dos emails em quarentena e clique em **Delete**.

Como excluir emails em quarentena e notificar o usuário

O recurso Excluir e notificar permite avisar aos destinatários ao excluir emails de quarentena.

Excluir e notificar os destinatários:

1. Use os recursos de pesquisa descritos nas seções anteriores para retornar uma lista de emails em quarentena.

2. Clique em um email para exibir seus detalhes.

3. Clique em **Delete and Notify**.

8.5 Feeds RSS de quarentena

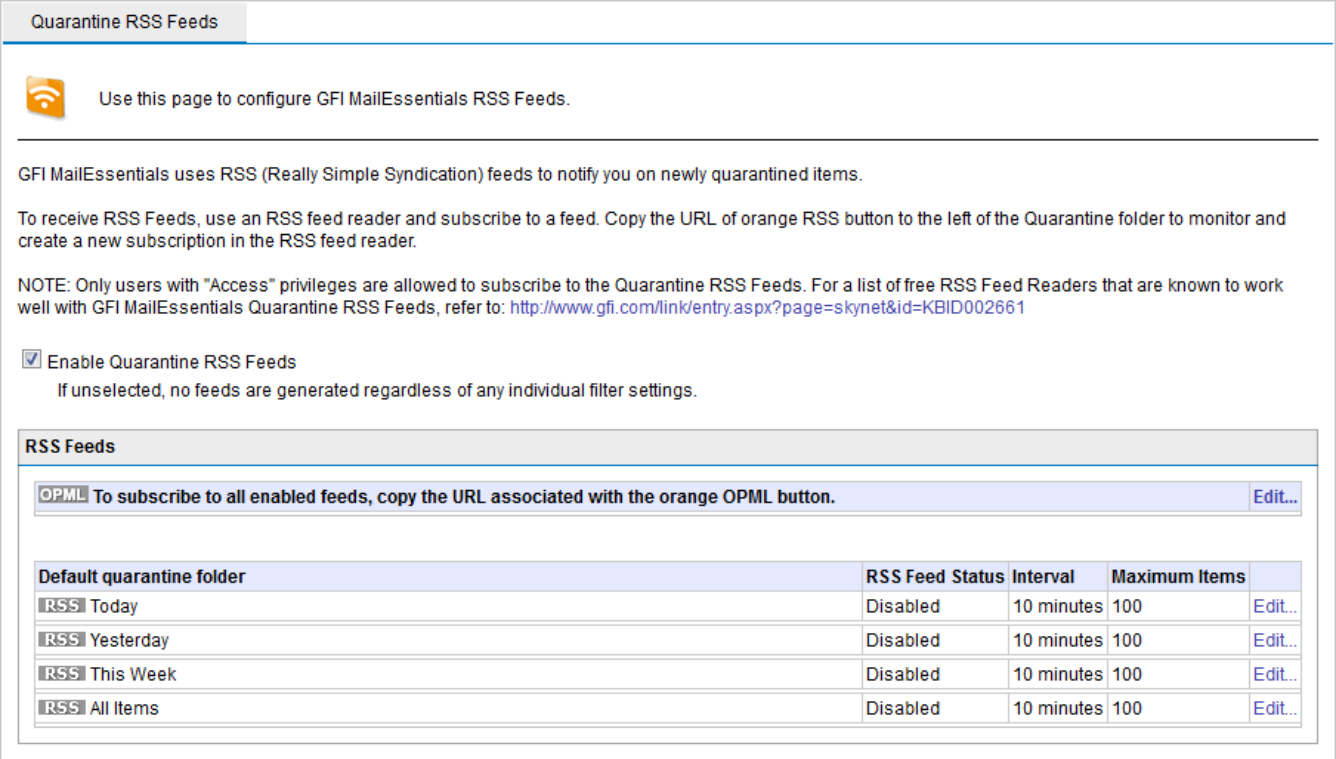
O RSS (Really Simple Syndication) é um protocolo utilizado para distribuir os conteúdos atualizados com frequência ou feeds (por exemplo, notícias) para seus assinantes. Um RSS Feed Reader é necessário para os assinantes exibirem os feeds RSS. Os feeds RSS geralmente incluem um resumo do conteúdo e um link para visualizar o artigo completo.

Feeds RSS podem ser usados para facilitar o monitoramento dos emails em quarentena. O recurso Quarantine RSS feed do GFI MailEssentials exibe emails em quarentena para análise e permite que os usuários aprovem ou excluam emails em quarentena.

> **OBS.**
> O recurso Quarantine RSS feeds do GFI MailEssentials pode ser utilizado na maioria dos RSS Feed Readers. Para obter uma lista de RSS Feed Readers disponíveis testados com o recurso Fe do GFI MailEssentials, consulte:
> http://kbase.gfi.com/showarticle.asp?id=KBID002661

8.5.1 Habilitar o Feeds RSS de quarentena

1. Acesse **GFI MailEssentials > Quarantine > Quarantine RSS Feeds**.



Screenshot 116: Feeds RSS de quarentena

2. Marque a caixa de seleção **Enable Quarantine RSS Feeds**.

3. Na área **RSS Feeds**, clique em **Edit** à direita da pasta de pesquisa da quarentena para habilitar RSS feeds.

4. Marque a caixa de seleção **Enable Quarantine RSS feeds on this folder**.

5. Especifique o intervalo de atualização em minutos na caixa de texto **Refresh feed content every**. O valor padrão é 10 minutos.

6. Especifique o número máximo de itens que você deseja que o feed inclua na caixa de texto **Feed should contain at most**. O valor padrão é 100 itens.

> **OBS.**
> Para alterar o URL de um feed RSS, clique em **Reset Feed URL**. Para alterar o URL de todos os feeds RSS habilitados, clique em **Edit** à direita da entrada **OPML** e clique em **Reset all the URLs**. Quando alterar URLs, certifique-se de atualizar todas as assinaturas.
> A redefinição do URL do feed deve ser feita no caso de acesso não autorizado

7. Clique em **Apply**.

8.5.2 Como assinar feeds RSS de quarentena

Como assinar todos os feeds RSS de quarentena habilitados

1. Acesse **GFI MailEssentials > Quarantine > Quarantine RSS Feeds**.

2. Na área RSS Feed, clique com o botão direito do mouse no ícone OPML e clique em **Copy Shortcut** para copiar o URL do feed RSS.

3. Use o URL copiado no aplicativo de leitura de Feed RSS para criar uma nova assinatura de Feed RSS.

Assinar um feed RSS de quarentena de uma pasta de pesquisa

Para assinar um feed RSS de uma pasta de pesquisa padrão ou personalizada:

1. Acesse **GFI MailEssentials > Quarantine > Quarantine RSS Feeds**.

2. Na área RSS Feeds, clique com o botão direito do mouse no ícone do RSS ao lado da pasta de pesquisa a ser assinada e clique em **Copy Shortcut** para copiar o URL do feed RSS.

3. Use o URL copiado no aplicativo de leitura de Feed RSS para criar uma nova assinatura de Feed RSS.

8.5.3 Proteger o acesso aos feeds RSS da quarentena do GFI MailEssentials

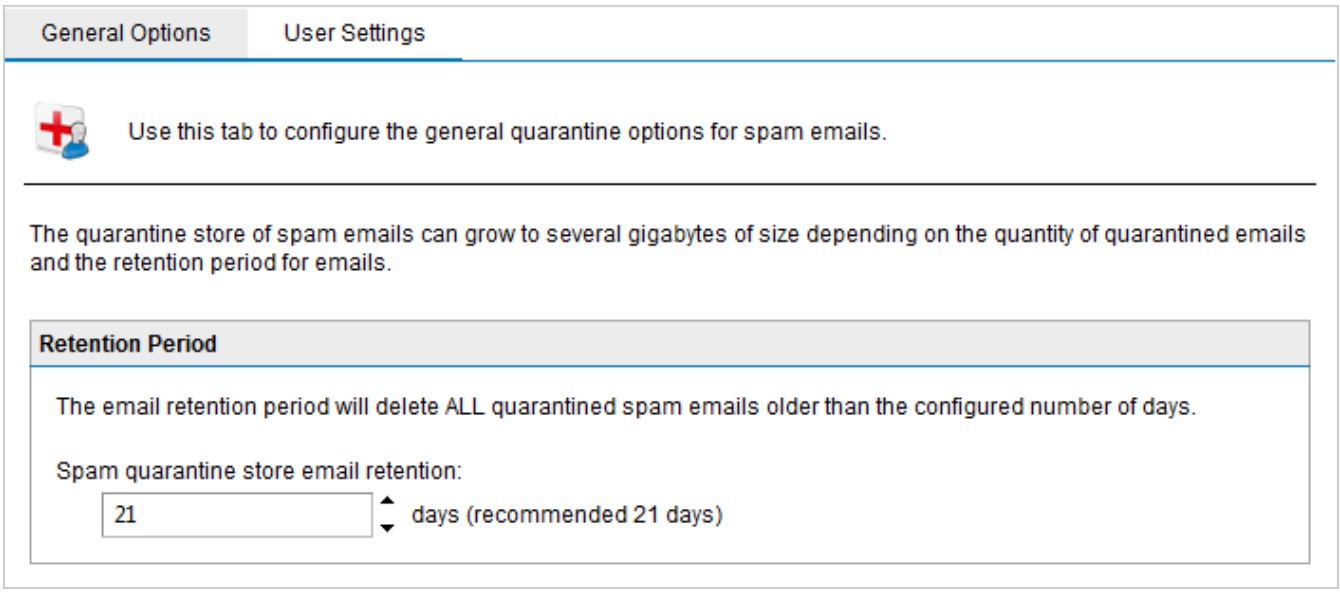
Defina quem pode assinar feeds RSS da quarentena no nó Access Control em GFI MailEssentials Configuration. Para obter mais informações, consulte Controle de acesso (página 247).

8.6 Opções de quarentena

Use as Quarantine Options para configurar as opções Quarantined Spam retention, User Reporting e Quarantined Malware non-existent user setup.

8.6.1 Opções de spam

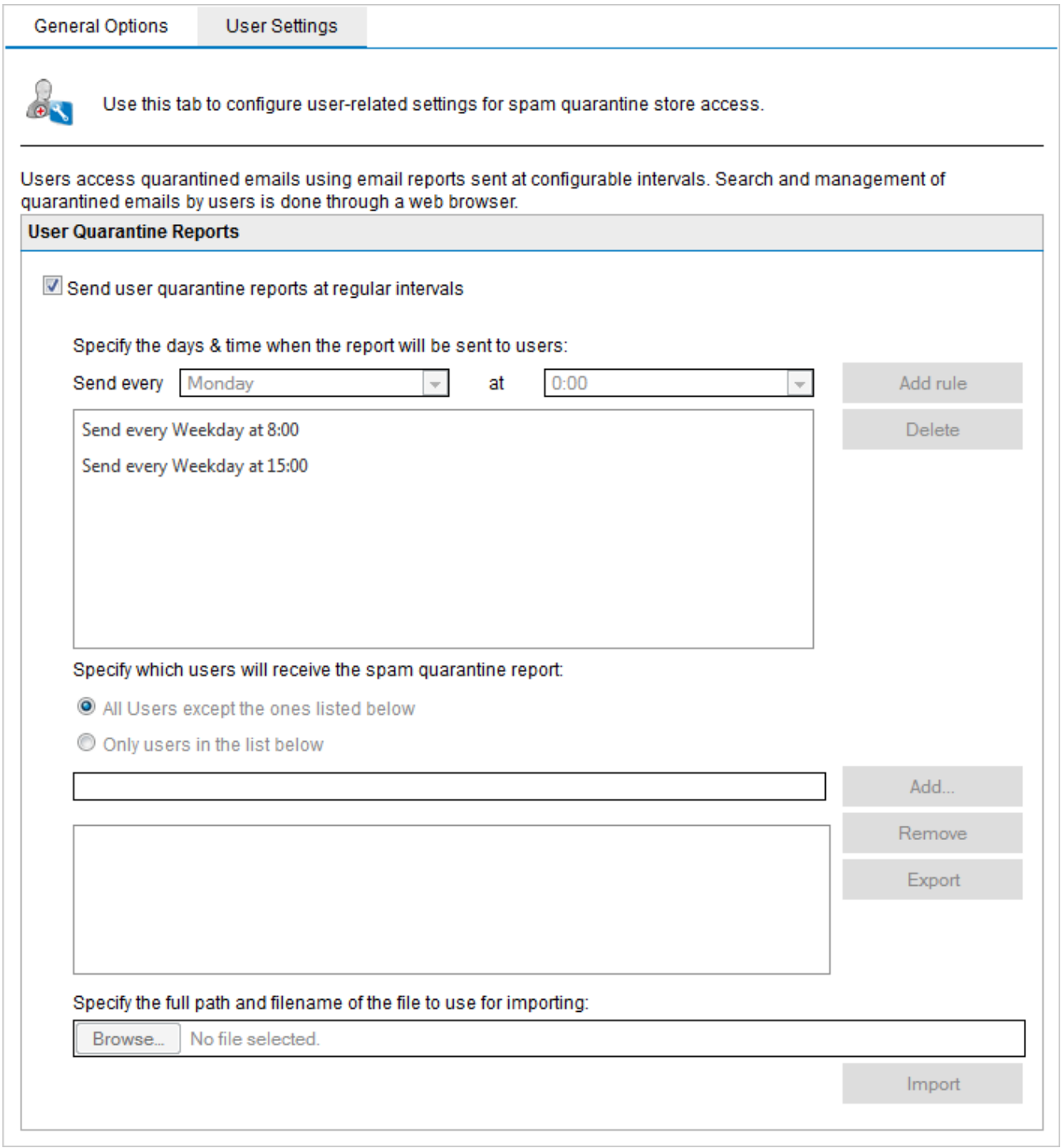
1. Acesse **Quarantine > Quarantine Options > Spam Options**.



Screenshot 117: Opções de Spam - guia General Options

2. Na guia **General Options**, altere ou confirme o período **Spam quarantine store email retention**.

3. Clique na guia **User Settings**.



Screenshot 118: Opções de Spam - guia User Settings

4. Selecione **Send user quarantine reports at regular intervals** para ativar o envio de relatórios de quarentena do usuário.

> **OBS.**
> Relatórios de quarentena do usuário são emails enviados para usuários regularmente com uma lista de spam bloqueado para esse usuário. Usando essa lista, os usuários podem verificar e aprovar quaisquer emails legítimos. Emails bloqueados pelos filtros Malware and Content Filtering não são mostrados nesses emails.

5. Configure a frequência na qual o relatório será enviado. Para adicionar a programação pre-definida, selecione a data e a hora e clique em **Add rule.** Selecione uma data e uma hora e clique em **Delete** para excluir selecionado data/hora.

6. Configure os usuários que receberão os relatórios Quarantined Spam. Selecione **All Users except the ones listed below** ou **Only users in the list below** e forneça o endereço de email dos usuários a serem incluídos ou excluídos.

> **OBS.**
> Clique em **Browse** para selecionar um arquivo de uma lista de endereços de email a ser importada e clique em **Import**.

7. Clique em **Apply**.

8.6.2 Opções de malware

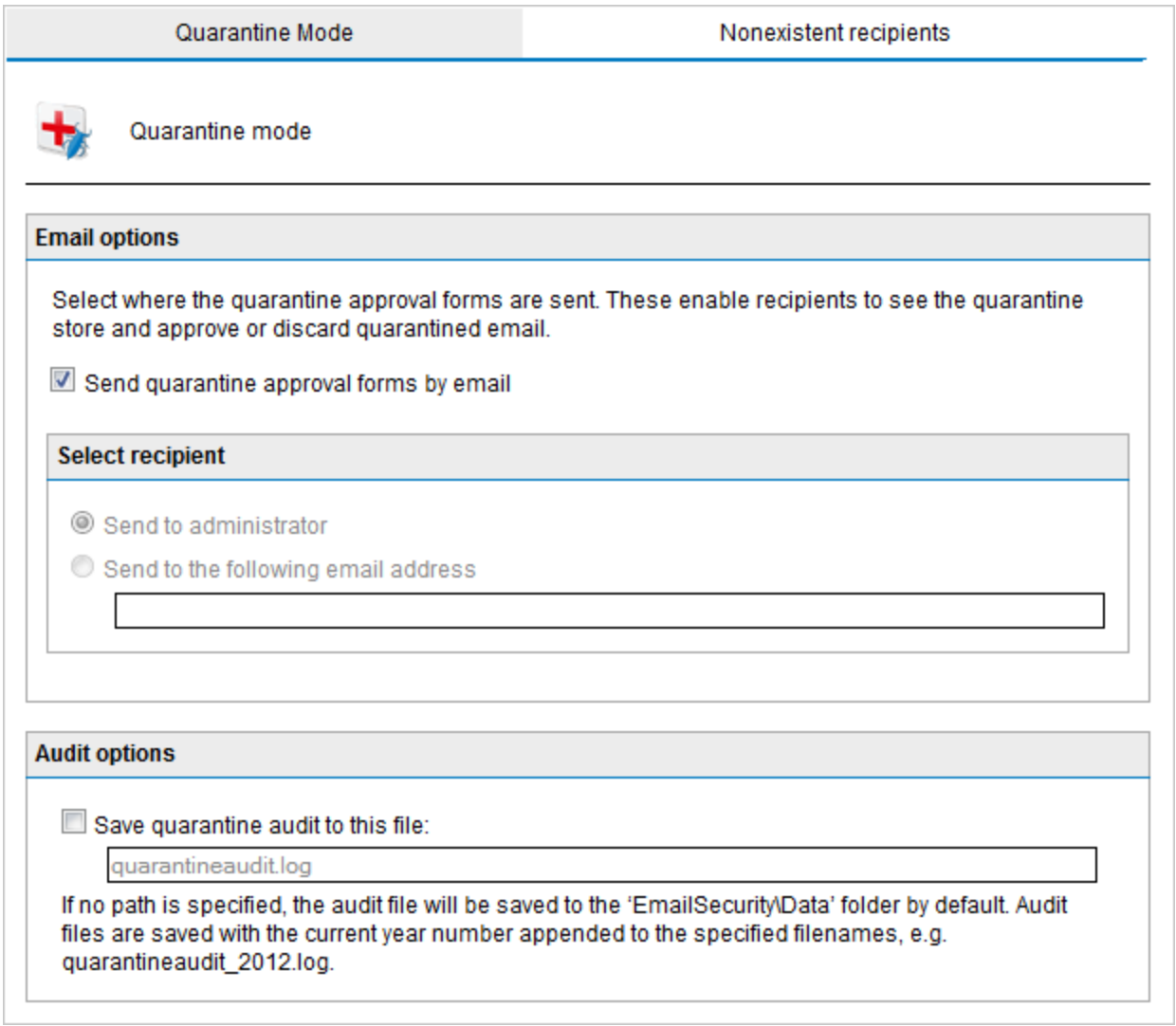
O GFI MailEssentials também pode ser configurado para notificar o administrador ou usuários autorizados por email (Quarantine Action Form) sempre que um email for colocado em quarentena.

O Quarantine Approval Form contém os detalhes relacionados com o email em quarentena, incluindo o motivo que foram bloqueados e os anexos que foram incluídos no email. O administrador pode executar ações no email em quarentena (por exemplo, aprovar o email) diretamente no cliente de email.

> **OBS.**
> Para excluir automaticamente emails mais antigos do que um número especificado de dias, crie uma nova pasta de pesquisa e defina o recurso Auto-purging para enviar emails depois de um número de dias. Para obter mais informações, consulte Usar o nó Search Folders para limpar automaticamente os emails em quarentena (página 211).

Habilitar formulários de aprovação de quarentena

1. Acesse **Quarantine > Quarantine Options > Malware Options**.



Screenshot 119: Modo Quarentena

2. Na guia **Quarantine Mode**, selecione a caixa de texto **Send quarantine approval forms by email** para ativar o envio de Formulários de aprovação de quarentena.

3. Na área **Select recipient**, especifique o destino dos Formulários de aprovação de quarentena:

Opção	Descrição
Send to administrator	Envia Formulários de aprovação de quarentena para o administrador, como definido no nó **General Settings**. Para obter mais informações, consulte Endereço de email do administrador (página 240).
Send to the following email address	Envia Formulários de aprovação de quarentena para outro endereço de email. Digite o destinatário na caixa de texto fornecida.

4. Opcional - Selecione **Save quarantine audit to this file** e configure um nome do arquivo onde salvar uma cópia do registro de quarentena.

5. Clique em **Apply**.

Destinatários não existentes

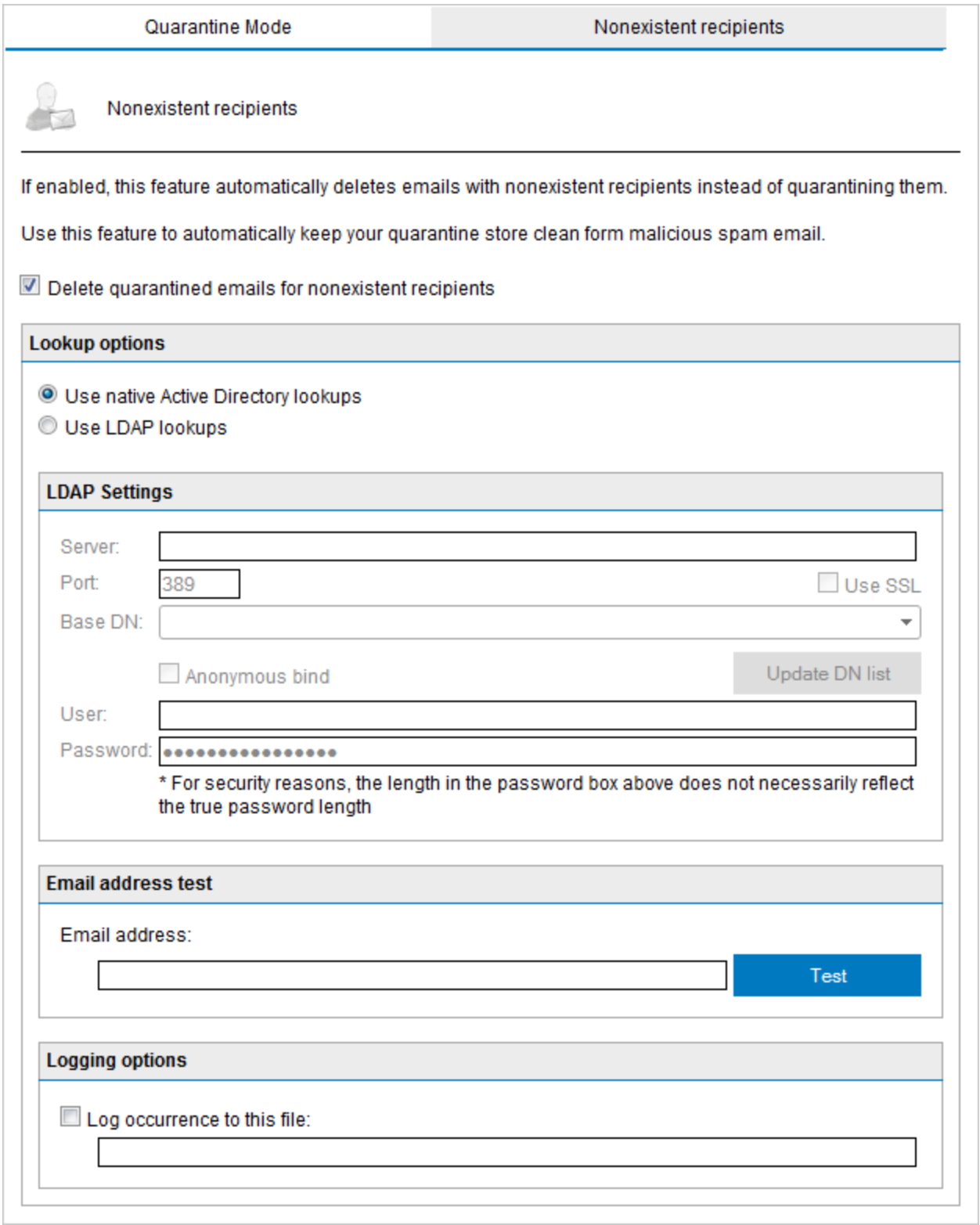
O recursos Nonexistant recipients do GFI MailEssentials faz a verificação de endereços de emails locais inexistentes antes que sejam armazenados no Armazenamento de quarentena. Se um email

contiver endereços de emails locais inexistentes, ele será excluído permanentemente. Isso reduz o número de emails para análise administrativa.

Configurar Destinatários não existentes

O filtro Destinatários não existentes requer o acesso à lista de endereços locais. Isso é feito através do Active Directory ou se a comunicação com o Active Directory não for possível, por meio de um servidor LDAP.

1. Acesse **Quarantine > Quarantine Options > Malware Options**.



Screenshot 120: Destinatários não existentes

2. Na guia **Nonexistent Recipients**, selecione a caixa de verificação **Delete quarantined emails for nonexistent recipients.**

3. Selecionar método de busca de usuário para usar:

Opção	Descrição
Use native Active Directory lookups	Selecione esta opção se o GFI MailEssentials estiver instalado no modo Active Directory e tiver acesso a TODOS os usuários no Active Directory. Pule para a etapa 8. **OBS.** Quando o GFI MailEssentials estiver instalado no modo do usuário do Active Directory em um DMZ, o AD de DMZ normalmente não inclui todos os usuários da rede (destinatários de emails). Nesse caso, configure o GFI MailEssentials para usar pesquisas LDAP. **OBS.** Quando o GFI MailEssentials estiver protegido por um firewall, esse recurso pode não ser capaz de se conectar diretamente ao Active Directory interno por causa das configurações de firewall. Use as pesquisas LDAP para estabelecer uma conexão com o Active Directory interno de sua rede e certifique-se de habilitar a porta padrão 389 em seu firewall.
Use LDAP lookups	Selecione esta opção quando o GFI MailEssentials for instalado no modo SMTP e/ou quando o GFI MailEssentials não tiver acesso direto à lista completa de usuários.

4. Especifique o nome do servidor LDAP ou o endereço IP na caixa de texto **Server**.

> **OBS.**
> Em um ambiente Active Directory, o servidor LDAP normalmente é o Domain Controller ou Global Catalog.

5. Especifique o número da porta, padrão 389, na caixa de texto **Port**. Se a conexão com o servidor LDAP for através de SSL, selecione **Use SSL** e a porta padrão será alterada para 636.

> **OBS.**
> Certifique-se de que a porta seja ativada no Firewall.

6. Clique em **Update DN list** para preencher a lista **Base DN** e selecione o Base DN (isto é, o nível superior na hierarquia do Active Directory).

7. Se seu servidor LDAP exigir autenticação, especifique **User** e **Password**. Como alternativa, se nenhuma autenticação for necessária, selecione **Anonymous bind**.

8. Teste suas definições de configuração especificando um endereço de email válido na caixa **Email address** e clique em **Test**. Se o endereço de email não for encontrado, verifique as definições de configuração.

9. Para registrar a atividade Nonexistent Recipient de um arquivo de registro, selecione **Log occurrence to this file** e especifique a localização e o nome do arquivo (incluindo a extensão .txt) para um local personalizado no disco no qual armazenar o arquivo de registro. Alternativamente, especifique o nome do arquivo (incluindo a extensão .txt) e o arquivo de registro será armazenado na seguinte localização padrão

```
<GFI MailEssentials installation
path>\GFI\MailEssentials\\EmailSecurity\Logs\<nome de arquivo>.txt
```

10. Clique em **Apply**.

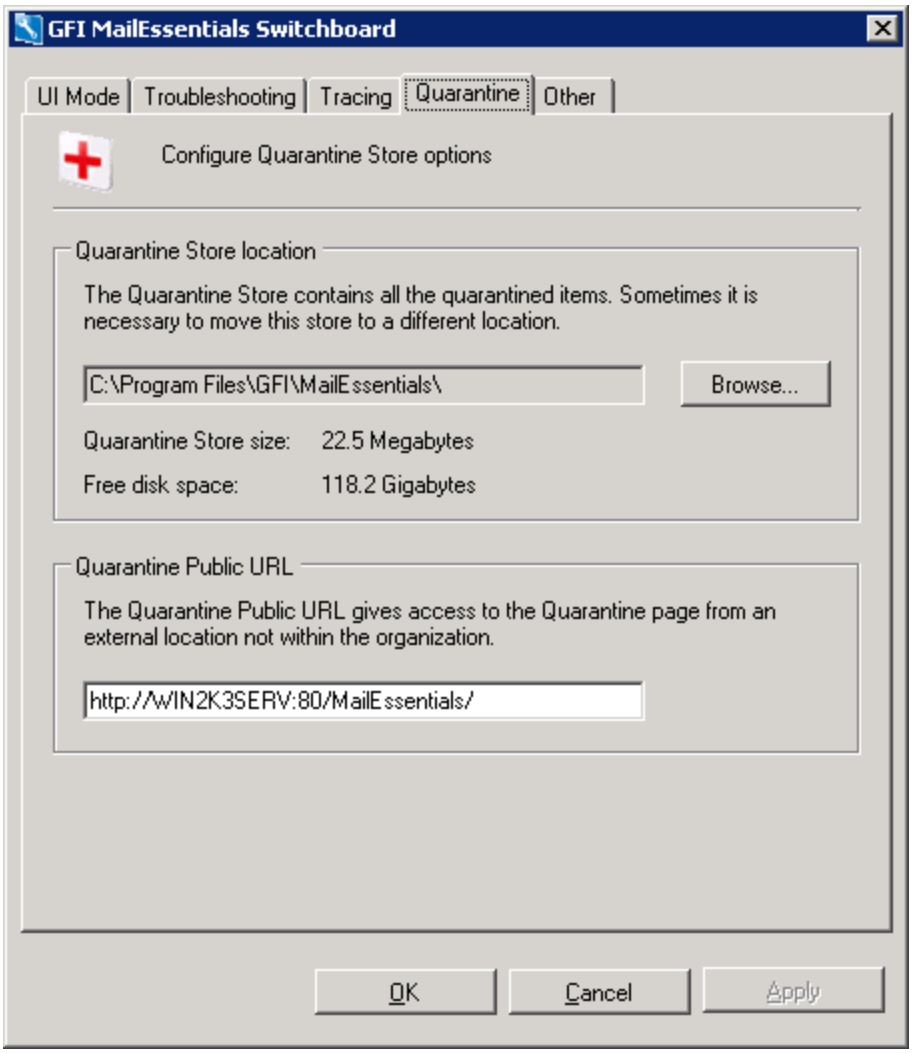
8.7 Local do armazenamento da quarentena e URL público

Use o Menu de controle doGFI MailEssentials para configurar o local do armazenamento da quarentena e o URL público da quarentena.

A localização do armazenamento da quarentena é onde os emails em quarentena são armazenados. Por padrão, ele fica localizado no caminho de instalação do GFI MailEssentials. No entanto, ele pode precisar ser movido para um local alternativo quando, por exemplo, estiver acabando o espaço no disco.

O URL público da quarentena permite acessar a página da quarentena a partir de uma localização externa. Por padrão, ele é baseado nas configurações de diretório virtual do ISS do GFI MailEssentials que você forneceu durante a instalação. No entanto, ele poderá precisar ser alterado se você enviar emails de resumo de quarentena ou notificações acessados fora da rede interna. Nesse caso, o URL deve ser alterado para ser acessado pela Internet.

1. Inicie o GFI MailEssentials Switchboard a partir de **Iniciar > Programas > GFI MailEssentials > Switchboard**.



Screenshot 121: Local de armazenamento e URL público da quarentena

2. Na guia **Quarantine**, clique em **Browse** para selecionar um local alternativo para o armazenamento da quarentena.

IMPORTANTE

Certifique-se de que a partição do disco onde o armazenamento da quarentena foi salvo tenha espaço suficiente no disco. Emails de spam não serão colocados em quarentena se o espaço livre no disco for menor que 512 MB. Quando o espaço livre no disco for inferior a 512 MB, a operação dos emails em quarentena será interrompida e o spam será identificado e enviado para as caixas de entrada dos destinatários até que o espaço livre no disco passe de 512 MB

3. Forneça um URL alternativo para acessar a quarentena de uma localização externa fora de sua organização.

4. Clique em **OK** para salvar a configuração.

9 Gerenciamento de email

O GFI MailEssentials inclui várias ferramentas que facilitam o gerenciamento de emails de entrada e saída.

Tópicos deste capítulo:

9.1 Avisos de isenção de responsabilidade

Avisos de isenção de responsabilidade são conteúdo padrão adicionado à parte inferior ou superior de emails enviados por motivos legais e/ou de marketing. Esses avisos ajudam as empresas a se proteger contra possíveis ameaças legais resultantes do conteúdo de uma mensagem de email e adicionar descrições de produtos/serviços.

» Configurar avisos de isenção de responsabilidade

» Como desabilitar e habilitar avisos de isenção de responsabilidade

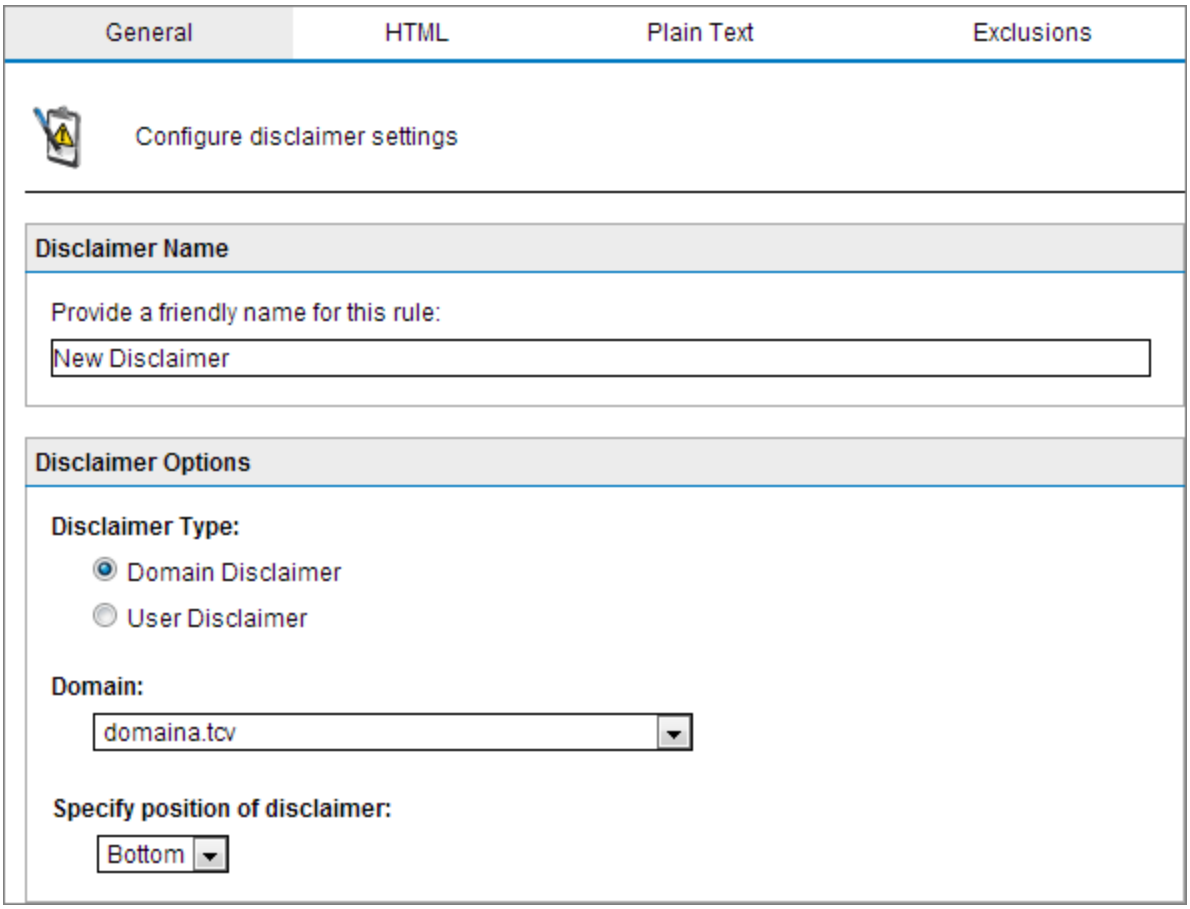
» Como classificar avisos de isenção de responsabilidade por prioridade

9.1.1 Configurar avisos de isenção de responsabilidade

Para personalizar ou criar um novo aviso de isenção de responsabilidade:

1. Acesse **Email Management > Disclaimers**.

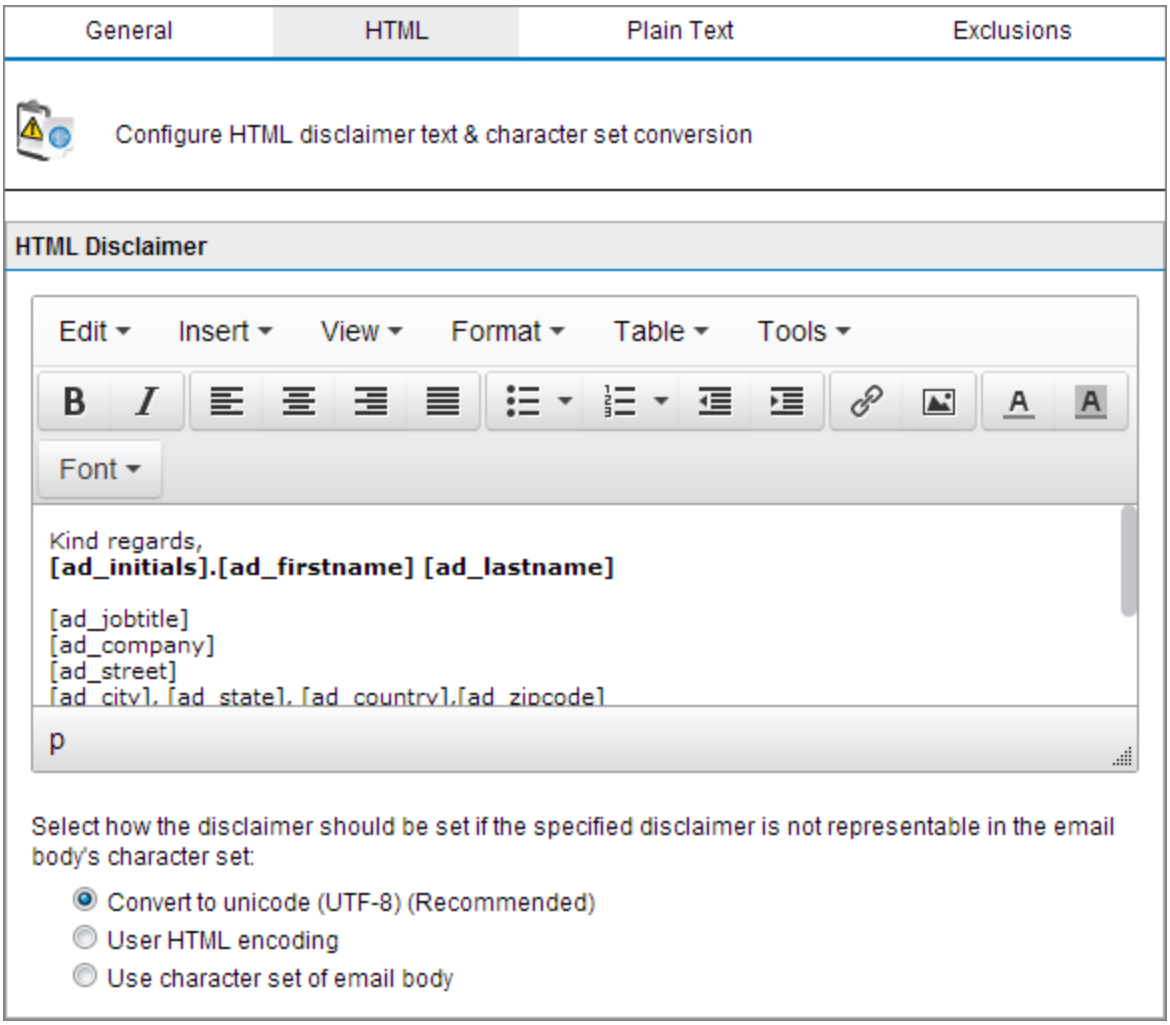
2. Clique em um aviso de isenção de responsabilidade para editar as configurações ou clique em **Add Disclaimer** para criar um novo aviso de isenção de responsabilidade.



Screenshot 122: Adicionar um novo aviso de isenção de responsabilidade

3. Na guia **General**, configure:

Opção	Descrição
Disclaimer Name	Digite um nome exclusivo e fácil de lembrar para o aviso de isenção de responsabilidade.
Disclaimer Type	Escolha a quais usuários aplicar este aviso de isenção de responsabilidade: » **Domain disclaimer**: O aviso de isenção de responsabilidade será adicionado a todos os emails enviados de um domínio. Selecione o domínio na lista suspensa **Domain**. » **Aviso de isenção de responsabilidade de usuário/grupo**: Clique em **Search User/Group** para selecionar um usuário ou um grupo de usuários para os quais o aviso de isenção de responsabilidade será adicionado aos emails de saída. Se o GFI MailEssentials estiver no modo Active Directory, selecione usuários ou grupos diretamente no Active Directory. Caso contrário, especifique o endereço de email SMTP do usuário.
Posição de Aviso de isenção de responsabilidade	Selecione a opção **Top** ou **Bottom** para configurar se o aviso de isenção de responsabilidade deverá ficar localizado na parte superior ou inferior da mensagem.



Screenshot 123: Aviso de isenção de responsabilidade HTML

4. Na guia **HTML**, use o editor HTML para criar um aviso de isenção de responsabilidade personalizado no formato HTML. Para adicionar campos de email ou campos do Active Directory (variáveis) ao aviso de isenção de responsabilidade, acesse **Insert > Variable…**. Selecione a variável a ser adicionada e clique em **Add**.

> **OBS.**
> O nome de exibição e as variáveis do endereço de email do destinatário só serão incluídos se o email for enviado para um único destinatário. Se os emails forem enviados para vários destinatários, as variáveis serão substituídas por "destinatários".

5. Selecione a codificação para o aviso de isenção de responsabilidade HTML se o conjunto de caracteres no corpo da mensagem de email não for HTML:

Opção	Descrição
Converter para Unicode	Faça a conversão do corpo da mensagem de email e dos avisos isenção de responsabilidade para Unicode para que ambos sejam exibidos corretamente. (Recomendado)
Usar a codificação HTML	Use para definir os conjuntos de caracteres para o corpo do email e o aviso de isenção de responsabilidade.
Usar o conjunto de caracteres do corpo do email	O aviso de isenção de responsabilidade é convertido para o conjunto de caracteres do corpo do email. **OBS.:** Se esta opção for selecionada, parte do texto do aviso de isenção de responsabilidade pode não ser exibida corretamente.

6. Selecione a guia **Plain Text** e insira o texto a ser usado em emails com texto simples diretamente no campo **Text Disclaimer**. Opcionalmente, adicione variáveis ao aviso de isenção de responsabilidade clicando em **Variable…** As variáveis que podem ser adicionadas são campos de email (nome do remetente, endereço de email do destinatário…) ou campos do Active Directory (nome, título, números de telefone, etc...). Selecione a variável a ser adicionada e clique em **Add**.

> **OBS.**
> O nome de exibição e as variáveis do endereço de email do destinatário só serão incluídos se o email for enviado para um único destinatário. Se os emails forem enviados para vários destinatários, as variáveis serão substituídas por "destinatários".

7. Especifique a codificação que será usada para o aviso de isenção de responsabilidade com texto simples se o conjunto de caracteres do corpo da mensagem de email não for texto simples:

Opção	Descrição
Converter para Unicode	Converte o corpo do e-mail e os avisos de isenção de responsabilidade para Unicode para que ambos sejam exibidos corretamente
Usar o conjunto de caracteres do corpo do email	O aviso de isenção de responsabilidade é convertido para o conjunto de caracteres do corpo do e-mail **OBS.:** Se esta opção for selecionada, parte do texto do aviso de isenção de responsabilidade pode não ser exibida corretamente.

8. Na guia **Exclusions**, especifique os remetentes ou destinatários aos quais não aplicar este aviso de isenção de responsabilidade. Digite um endereço de email ou clique em **Search** para procurar endereços de email do Active Directory. Clique em **Add** para adicionar o endereço de email à lista de exclusões.

> **OBS.**
> Todos os destinatários deverão ser incluídos na lista de exclusão para não adicionar um aviso de isenção de responsabilidade ao email.

9. Clique em **Apply** para salvar as configurações.

9.1.2 Desabilitar e habilitar avisos de isenção de responsabilidade

Por padrão, os avisos de isenção de responsabilidade são habilitados automaticamente. Para desabilitar ou habilitar um aviso de isenção de responsabilidade:

1. Acesse **Email Management > Disclaimers**.

2. Selecione os avisos de isenção de responsabilidade a serem habilitados/desabilitados e clique em **Disable selected** ou **Enable selected** para executar a ação desejada.

9.1.3 Classificar avisos de isenção de responsabilidade por prioridade

A ordem na qual os avisos de isenção de responsabilidade são aplicados a mensagens de saída pode ser personalizada. Se vários avisos de isenção de responsabilidade forem habilitados e aplicados ao mesmo usuário, o aviso de isenção de responsabilidade com a maior prioridade será aplicado a esse usuário.

Para personalizar a prioridade de avisos de isenção de responsabilidade:

1. Acesse **Email Management > Disclaimers**.

2. Para alterar a prioridade do aviso de isenção de responsabilidade, ao lado do aviso, clique no botão ↑ (para cima), para atribuir uma prioridade maior, ou no botão ↓(para baixo), para atribuir uma prioridade mais baixa.

9.2 Respostas automáticas

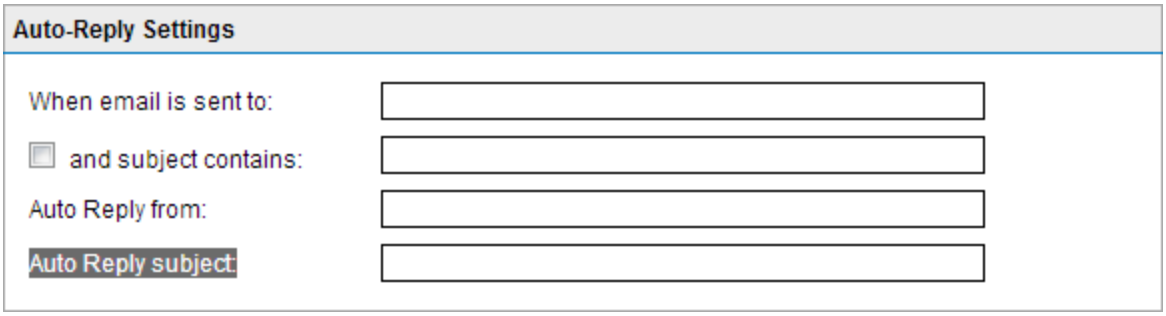
As respostas automáticas permitem o envio de respostas automáticas a emails de entrada específicos. Uma resposta automática diferente para cada endereço de email ou assunto pode ser especificada. Variáveis também podem ser usadas em uma resposta automática para personalizar emails.

Para habilitar respostas automáticas, acesse **Email Management > Auto-Replies** e selecione **Enable Auto-Replies**.

9.2.1 Configurar respostas automáticas

1. Acesse **Email Management > Auto-Replies**.

2. Clique em **Add Auto-Reply**.



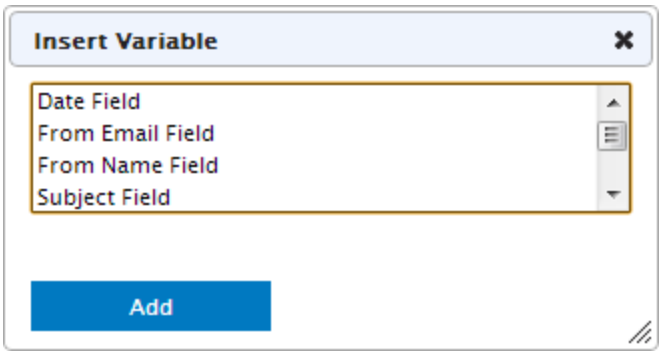
Screenshot 124: Configurações de resposta automática

3. Em **Auto-Reply Settings**, configure as seguintes opções:

Opção	Descrição
When email is sent to:	Digite o endereço de email que envia respostas automáticas quando recebe emails. **Exemplo**: se "vendas @dominio-mestre.com" for usado, os remetentes que enviarem mensagens para esse endereço de email receberão uma resposta automática.
and subject contains:	Esta opção permite respostas automáticas somente para emails que contenham um texto específico no campo de assunto.
Auto Reply from:	Especifique um endereço de email caso seja necessário enviar uma resposta automática de um endereço de email diferente do endereço de email ao qual o email de entrada foi endereçado.
Auto Reply subject:	Especifique o assunto do email de resposta automática.

4. Em **Auto Reply text**, especifique o texto a ser exibido no email de resposta automática.

> **OBS.**
> Importe o texto da resposta automática a partir de um arquivo de texto usando o botão **Import**. Clique em **Export** para fazer o download do texto da resposta automática para um arquivo de texto.



Screenshot 125: Caixa de diálogo Variables

5. Clique em **Variable...** para personalizar respostas automáticas usando variáveis. Selecione o campo da variável a ser inserida e clique em **OK**. As variáveis disponíveis são:

Opção	Descrição
Date Field	Insere a data de envio do email.
From Email Field	Insere o endereço de email do remetente.
From Name Field	Insere o nome de exibição do remetente.
Subject Field	Insere o assunto do email.
To Email Field	Insere o endereço de email do destinatário.
To Name Field	Insere o nome de exibição do destinatário.
Tracking Number	Insere o número de rastreamento (se gerado).

6. Na área **Anexos**, selecione os anexos a serem enviados com o e-mail de resposta automática. Especifique a localização do anexo e clique em **Adicionar**. Remova os anexos usando a opção **Remover**.

7. Em **Other Settings**, configure:

Opção	Descrição
Generate tracking number in subject	Gera um número de rastreamento exclusivo na resposta automática. Por padrão, os números de rastreamento são gerados com o seguinte formato: `ME_AAMMDD_nnnnnn` Onde: » `ME`:GFI MailEssentialsmarca. » `AAMMDD`: data com ano, mês e o formato da data. » `nnnnnn`: número de rastreamento gerado automaticamente.
Incluir email enviado	Selecione para incluir o email de entrada na resposta automática.

8. Clique em **Apply**.

9.3 Servidor de lista

Servidores de lista permitem a criação de dois tipos de listas de distribuição:

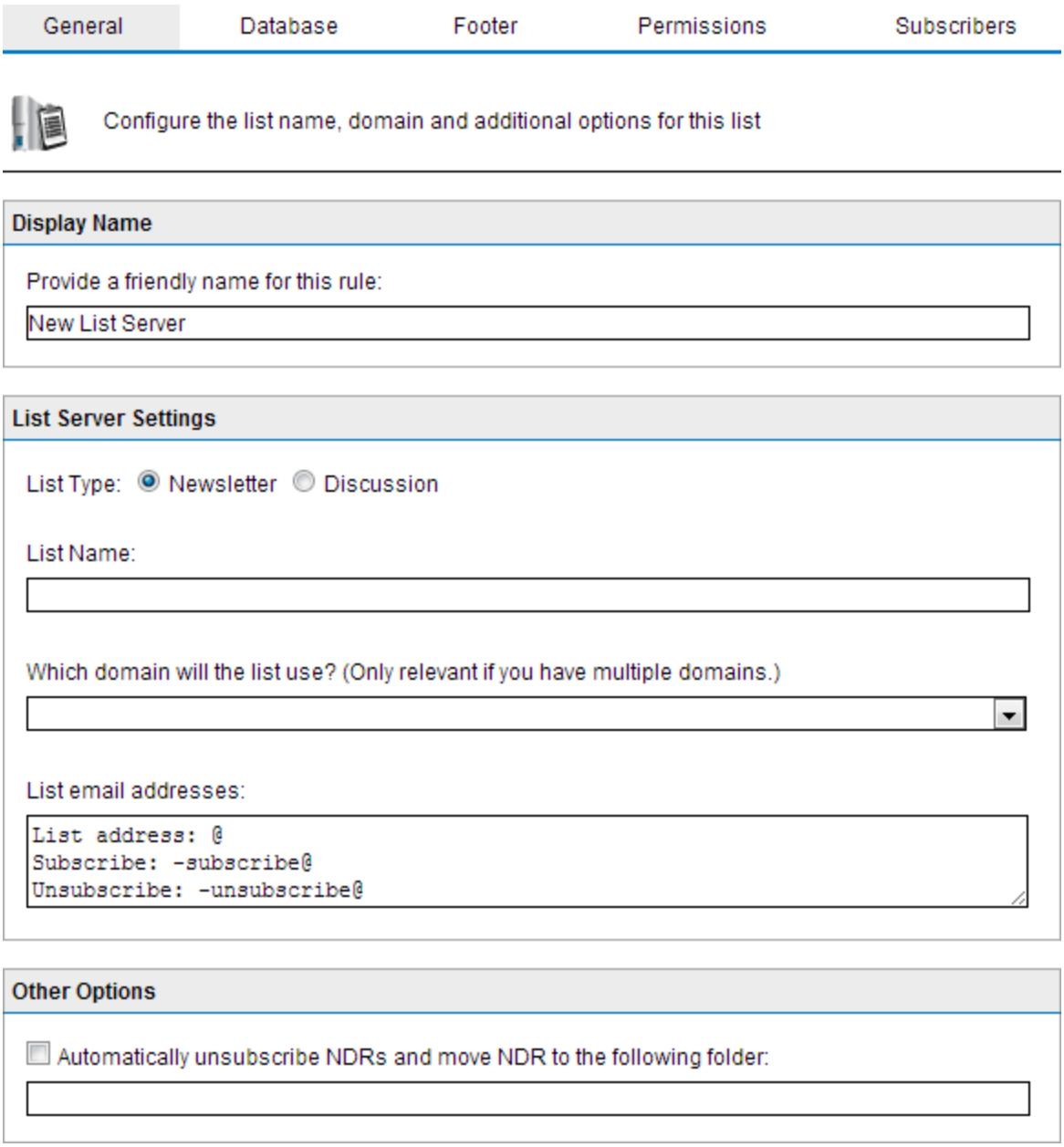
» **Newsletter**: usado para criar listas de assinatura de boletins informativos empresariais ou de produtos, para que os usuários possam fazer a assinatura ou cancelá-la.

» **Discussion**: permite que grupos de pessoas mantenham discussões por email, sendo que cada membro da lista recebe os emails enviados pelos outros membros.

9.3.1 Criar um boletim informativo ou uma lista de discussão

Para criar um novo boletim informativo ou uma lista de discussão:

1. Acesse **Email Management > List Server** e clique em **Add List**.



Screenshot 126: Criar uma nova lista

2. Configure as seguintes opções:

Opção	Descrição
Display Name	Digite um nome fácil de lembrar para a nova lista.
List type	Selecione o tipo de lista de discussão a ser criada: » **Newsletter**: usado para criar listas de assinatura de boletins informativos empresariais ou de produtos, para que os usuários possam fazer a assinatura ou cancelá-la. » **Discussion**: permite que grupos de pessoas mantenham discussões por email, sendo que cada membro da lista recebe os emails enviados pelos outros membros.

Opção	Descrição
List Name	O nome da lista é usado nos campos de endereço da lista de emails. Por exemplo, se o nome da lista for `Meuboletiminformativo`, o endereço de email da lista será `Meuboletiminformativo@meudominio.com`
List domain	O domínio a ser usado para a lista. A lista de domínios é extraída da lista Local Domains. O servidor de lista utiliza esse domínio para obter os endereços da lista exibidos na caixa **List email addresses**.
Automatically unsubscribe NDRs and move NDR to the following folder:	Quando uma notificação de falha na entrega for recebida de um assinante da lista, sua assinatura será cancelada automaticamente e a notificação de falha na entrega movida para uma pasta personalizada.

3. Na guia **Database**, selecione **Microsoft Access** ou **Microsoft SQL Server/MSDE** como o banco de dados. Configure o tipo de banco de dados selecionado para armazenar a lista de assinantes do boletim informativo/lista de discussão. Opções disponíveis:

Opção	Descrição
Microsoft Access	Especifique o nome e o local de um banco de dados. GFI MailEssentials cria automaticamente um banco de dados.
Microsoft SQL Server	Especifique o nome do servidor SQL, o banco de dados e as credenciais de logon usados para armazenar a lista de assinantes do boletim informativo/lista de discussão. Clique em Test para garantir que o GFI MailEssentials pode estabelecer uma conexão com o Microsoft SQL Server especificado.

> **OBS.**
> Você pode utilizar o Microsoft Access para listas de até 5000 membros.

4. Personalize a lista de distribuição. Para obter mais informações, consulte Configurar as propriedades avançadas do boletim informativo/da lista de discussão (página 234).

5. Clique em **Apply**.

9.3.2 Usar boletins informativos/listas de discussão

Depois de criar um boletim informativo/lista de discussão, os usuários devem se inscrever para fazer parte da lista.

Ação	Descrição
Como assinar a lista	Solicite que os usuários enviem um email para `<nome do boletim informativo>-subscribe@seudominio.com`
Como concluir o processo de assinatura	Ao receber a solicitação, o servidor de lista envia um email de confirmação. Os usuários devem confirmar a assinatura através de uma resposta de email para serem adicionados como assinantes. **OBS.:** O email de confirmação é um requisito e não pode ser desativado.
Como enviar uma postagem de boletim informativo/lista de discussão	Membros com permissões para enviar emails para a lista precisam enviar o email para o endereço do boletim informativo: `<newslettername>@seudominio.com`
Como cancelar a assinatura da lista	Para cancelar a assinatura da lista, os usuários devem enviar um email para: `<newslettername>-unsubscribe@seudominio.com`

OBS.
Para permitir que os usuários assinem facilmente boletins informativos, adicione um formulário da Web perguntando o nome e endereço de email e gere automaticamente um email no qual o remetente seja o endereço de email do novo usuário e o destinatário seja:
`<newslettername>-subscribe@seudominio.com`

9.3.3 Configurar as propriedades avançadas do boletim informativo/da lista de discussão

Depois de criar uma nova lista, mais opções podem ser configuradas que possibilitam a personalização de elementos e do comportamento da lista. As opções incluem:

- Criar um rodapé personalizado para a lista
- Definir permissões para a lista
- Adicionar manualmente assinantes à lista
- Importar assinantes para a estrutura da lista/do banco de dados

Criar um rodapé personalizado para a lista

1. Na guia **Footer**, configure um rodapé de lista de discussão personalizado. Um rodapé é adicionado a cada email enviado para a lista.

2. Use o editor de HTML para adicionar uma versão HTML do rodapé. Para adicionar campos de variável ao rodapé da lista, acesse **Insert > Variables**. Selecione a variável a ser adicionada e clique em **Add List**.

3. Você também pode inserir um texto simples de rodapé para as listas de texto simples. Clique em **Variable...** para adicionar campos de variável.

4. Clique em **Apply**.

Dica
Você pode usar os rodapés para mostrar como os usuários podem assinar a/cancelar a assinatura da lista e/ou a promover seus canais nas redes sociais.

Definir permissões para boletins informativos

Especifique os usuários que podem enviar boletins informativos.

OBS.
Permissões não são configuráveis para listas de discussão.

1. Abra uma lista existente ou crie uma nova lista e acesse a guia **Permissions**.

2. Digite um endereço de email que possa enviar boletins informativos e clique em **Add Email**. O endereço de email será adicionado à lista.

3. Uma senha protege o acesso ao boletim informativo caso outra pessoa use o cliente de email ou detalhes da conta de um usuário permitido. Para habilitar as senhas, marque a caixa de seleção **Password required:** e forneça uma senha.

> **OBS.**
> Ao enviar emails para o boletim informativo, os usuários precisam se autenticar com a senha no campo de assunto do email. A senha deve ser especificada no campo do assunto da seguinte forma:
> `[SENHA:<senha>] <Assunto do e-mail>`
> **Exemplo:** `[SENHA:letmepost]Oferta especial.`
> Se a senha estiver correta, o servidor de lista removerá automaticamente os detalhes da senha do assunto e retransmitirá o email para os assinantes do boletim.

4. Clique em **Apply**.

Adicionar manualmente assinantes à lista

Adicione manualmente usuários a boletins informativos/listas de discussão sem qualquer ação em seu nome.

> **OBS.**
> É recomendável que os usuários se inscrevam na lista, enviando um email para o endereço de assinatura do boletim informativo/lista de discussão. Certifique-se de que você tenha a autorização dos usuários antes de adicioná-los manualmente à lista.

1. Abra uma lista existente ou crie uma nova lista e acesse a guia **Subscribers**.

2. Digite os detalhes do assinante nos campos **Email Address** (obrigatório), **First name**, **Last name** e **Company** e clique em **Add Email**. O endereço de email do novo assinante será adicionado à lista.

3. Para remover usuários da tabela da lista de assinatura quando cancelar a inscrição da lista (e não apenas marcá-los como cancelamento de assinatura), selecione a caixa de seleção **Delete from database when user unsubscribes**.

4. Clique em **Apply**.

Importar assinantes para a estrutura de lista/banco de dados

Quando um novo boletim informativo ou lista de discussão é criado, uma tabela "listname_ subscribers" com os campos a seguir é criada no banco de dados.

Para importar os dados para a lista, preencha o banco de dados com dados nos campos a seguir.

Nome de campo	Tipo	Valor padrão	Sinalizadores	Descrição
Ls_id	Varchar(100)		PK	Subscriber ID
Ls_first	Varchar(250)			Nome
Ls_last	Varchar(250)			Sobrenome
Ls_email	Varchar(250)			Email
Ls_unsubscribed	Int	0	NOT NULL	Unsubscribe flag
Ls_company	Varchar(250)			Nome da empresa

9.4 Monitoramento de email

O monitoramento de email permite copiar mensagens enviadas para ou de um endereço de email local específico para outro endereço de email. Isso permite a criação do armazenamento central de comunicações por email para determinadas pessoas ou departamentos.

9.4.1 Adicionar novas regras de monitoramento de email

1. Acesse **Email management > Mail Monitoring**.

2. Clique em **Add Rule...**.

3. Na guia **General**, configure as seguintes opções:

Opção	Descrição
Mail Monitor Name	Digite um nome de regra de monitoramento de email fácil de lembrar.
Inbound ou **Outbound**	Selecione se deseja aplicar a regra a emails de entrada ou saída.
Copy monitored email to user or email address	O endereço de email ou a caixa de email de destino para onde copiar os emails. Selecione **Email Address** para digitar manualmente um endereço de email ou selecione **User** para procurar
If sender is	Especifique o endereço de email do remetente a ser monitorado. Clique em **All Domains** para monitorar emails enviados por todos os usuários.
and recipient is	Especifique o endereço de email do destinatário a ser monitorado. Clique em **All Domains** para monitorar emails recebidos por todos os usuários.

4. Clique em **Add** para adicionar a regra configurada.

5. Repita as etapas acima para especificar vários filtros.

6. Na guia **Exceptions**, especifique os usuários e os endereços de email aos quais a regra não se aplicará. Opções disponíveis:

Opção	Descrição
Except if sender is	Exclui os remetentes especificados do monitoramento de emails. Para as regras de monitoramento de entrada, digite endereços de email não locais. Para as regras de monitoramento de saída, todos os endereços da lista são locais. Clique em **Search User** para localizar endereços de email locais e clique em **Add**.
Except if recipient is	Exclui os destinatários especificados da lista. Para as regras de monitoramento de entrada, todos os endereços da lista são locais. Clique em **Search User** para localizar endereços de email locais e clique em **Add**. Para as regras de monitoramento de saída, digite endereços de email não locais.

7. Clique em **Apply**.

9.4.2 Usar o monitoramento de email

Consulte a tabela abaixo para obter informações sobre como configurar o monitoramento de email para diferentes necessidades e situações:

O que monitorar	Descrição
All email sent by a particular user	Crie uma regra de saída e especifique o remetente do email ou selecione o usuário (se usar o AD) no campo de remetente. Clique em **All Domains** no campo do destinatário.
All email sent to a particular user	Crie uma regra de entrada e especifique o endereço de email do destinatário ou selecione o usuário (se usar o AD) no campo de destinatário. Clique em **All Domains** no campo do remetente.
Mail sent by a particular user to an external recipient	Crie uma regra de saída, especifique o remetente ou selecione o usuário (se usar o AD) no campo de remetente. Digite o email do destinatário externo no campo de destinatário.
Mail sent to a particular user by an external sender	Crie uma regra de entrada e especifique o endereço de email do remetente externo no campo de remetente. Digite o endereço de email ou selecione o usuário (se usar o AD) no campo de destinatário.
Mail sent by a particular user to a company or domain	Crie uma regra de saída e especifique o remetente ou selecione o usuário (se usar o AD) no campo de remetente. Especifique o domínio da empresa no campo de destinatário.
Mail sent to a particular user by a company or domain	Crie uma regra de entrada e especifique o domínio da empresa no campo de remetente. Selecione o domínio quando clicar no botão do remetente e insira o nome do usuário ou o endereço de email do usuário no de destinatário.

9.4.3 Habilitar/desabilitar as regras de monitoramento de email

1. Acesse **Email management > Mail Monitoring**.

2. Selecione a regra a ser habilitada/desabilitada.

3. Clique em **Enable Selected** ou **Disable Selected** para habilitar ou desabilitar a regra selecionada, respectivamente.

4. Clique em **OK** para salvar as alterações.

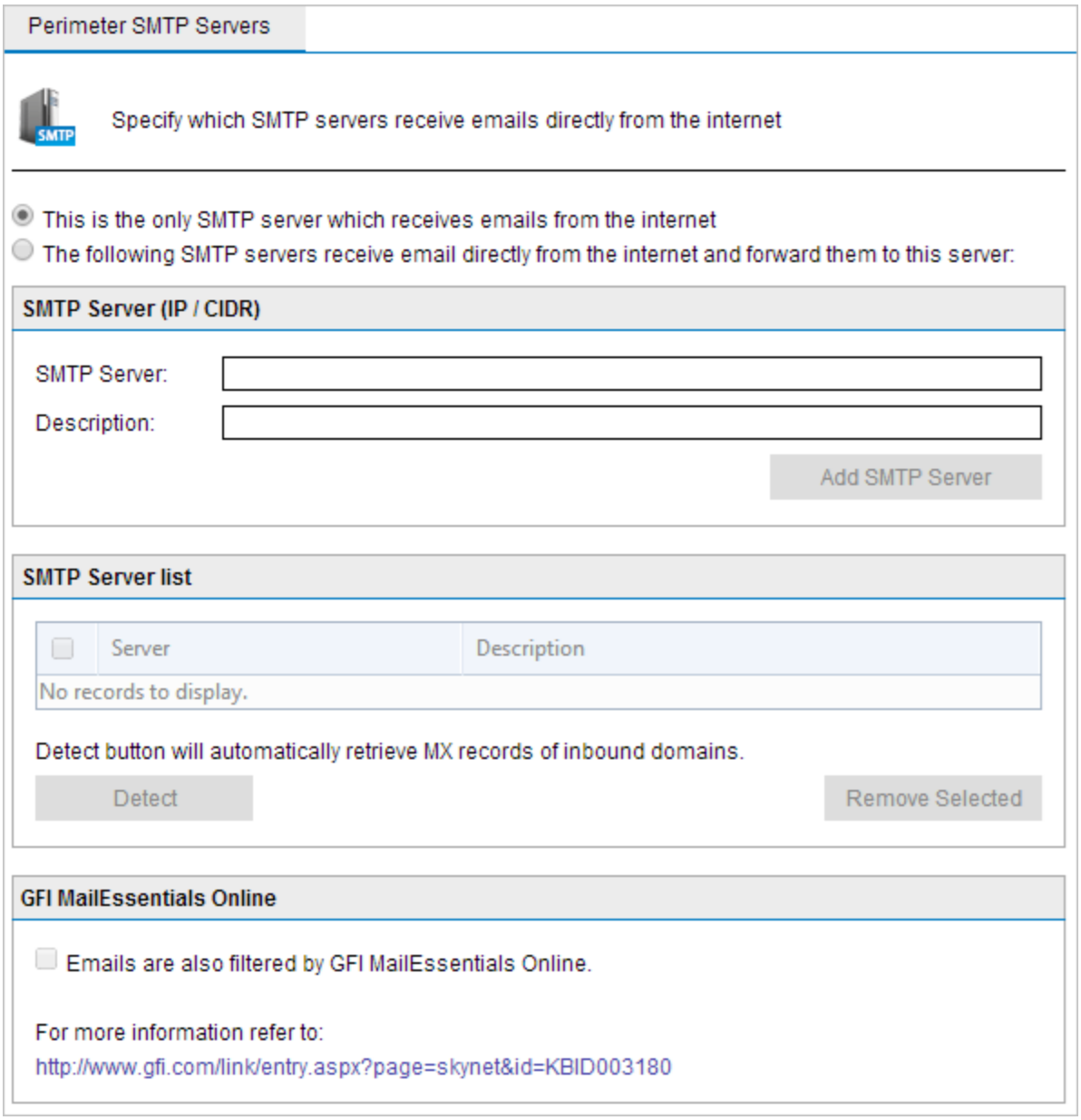
10 Configurações gerais

Tópicos deste capítulo:

10.0.1 Configurações do servidor SMTP de perímetro

Servidores SMTP que retransmitem emails para o servidorGFI MailEssentials devem ser especificados.

1. A partir das Configurações do GFI MailEssentials, acesse **General Settings > Perimeter SMTP Servers**.



Screenshot 127: Configurações do servidor SMTP de perímetro

2. Configure as seguintes opções:

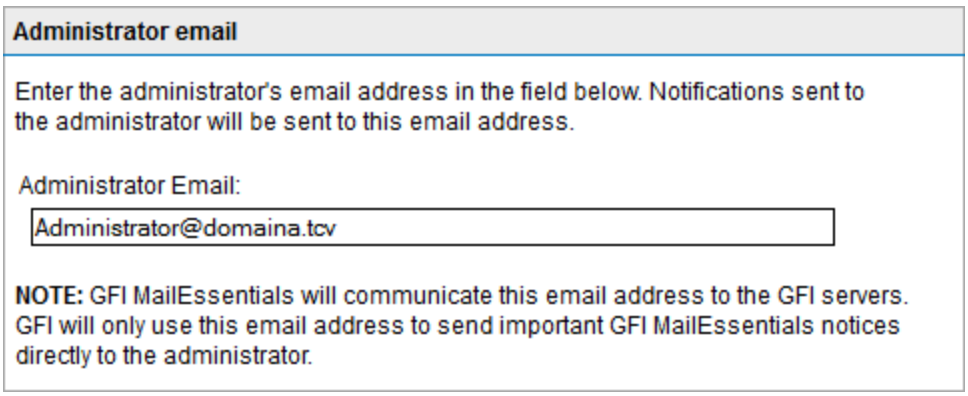
Opção	Descrição
This is the only SMTP server which receives emails from the Internet	Selecione esta opção, quando o GFI MailEssentials for instalado somente no servidor SMTP que recebe emails externos diretamente pela Internet.
The following SMTP servers receive emails directly from the Internet and forward them to this server	Emails são retransmitidos para o servidor do GFI MailEssentials de outros servidores SMTP. Adicionar este servidor SMTP na lista de servidor SMTP: **Detecção automática:** Para detectar automaticamente os servidores SMTP recuperando registros MX de domínios de entrada, clique em **Detect**. **Adição manual:** Para adicionar manualmente os IPs de outros servidores SMTP que retransmitem emails para o servidor do GFI MailEssentials, clique no endereço IP ou em um intervalo de endereços IP (utilizando anotação de CIDR) e clique em **Add SMTP Server**
Os emails também são filtrados por GFI MailEssentials Online	Selecione se usar os produtos de segurança de email hospedados GFI MailEssentials Online Para obter mais informações, consulte: http://go.gfi.com/?pageid=ME_MAXMPME

3. Clique em **Apply**.

10.1 Endereço de email do administrador

O GFI MailEssentials envia notificações importantes para o administrador por email. Para configurar o endereço de email do administrador:

1. Em GFI MailEssentialsConfiguration, acesse **General Settings > Settings** e selecione a guia **General**.



Screenshot 128: Especificar o endereço de email do administrador

2. Digite o endereço de email do administrador na área **Administrator email**.

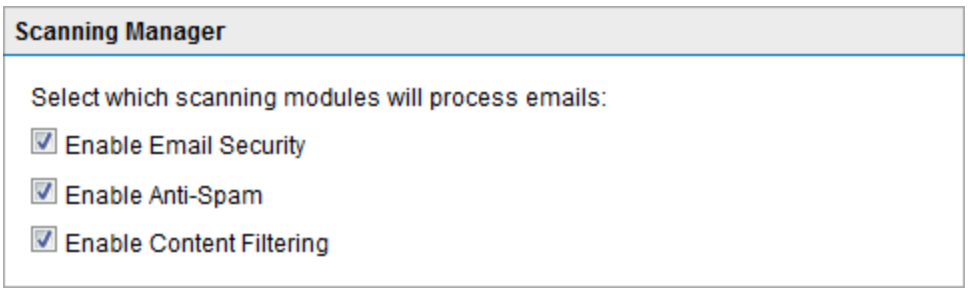
3. Clique em **Apply**.

10.2 Habilitar/desabilitar módulos de verificação

No GFI MailEssentials, você pode habilitar ou desabilitar a verificação de módulos de email específicos. Isso permite a ativação e desativação de mecanismos de verificação ou filtros em lote.

> **OBS.**
> Esse recurso habilita ou desabilita somente mecanismos de verificação específicos. Mecanismos desabilitados não processam emails de entrada, saída e/ou internos. Todos os outros recursos do GFI MailEssentials, como o armazenamento em quarentena, continuarão funcionando.

1. Em GFI MailEssentials Configuration, acesse **General Settings > Settings** e selecione a guia **General**.



Screenshot 129: Gerenciador de verificação

2. Habilite ou desabilite a verificação de módulos:

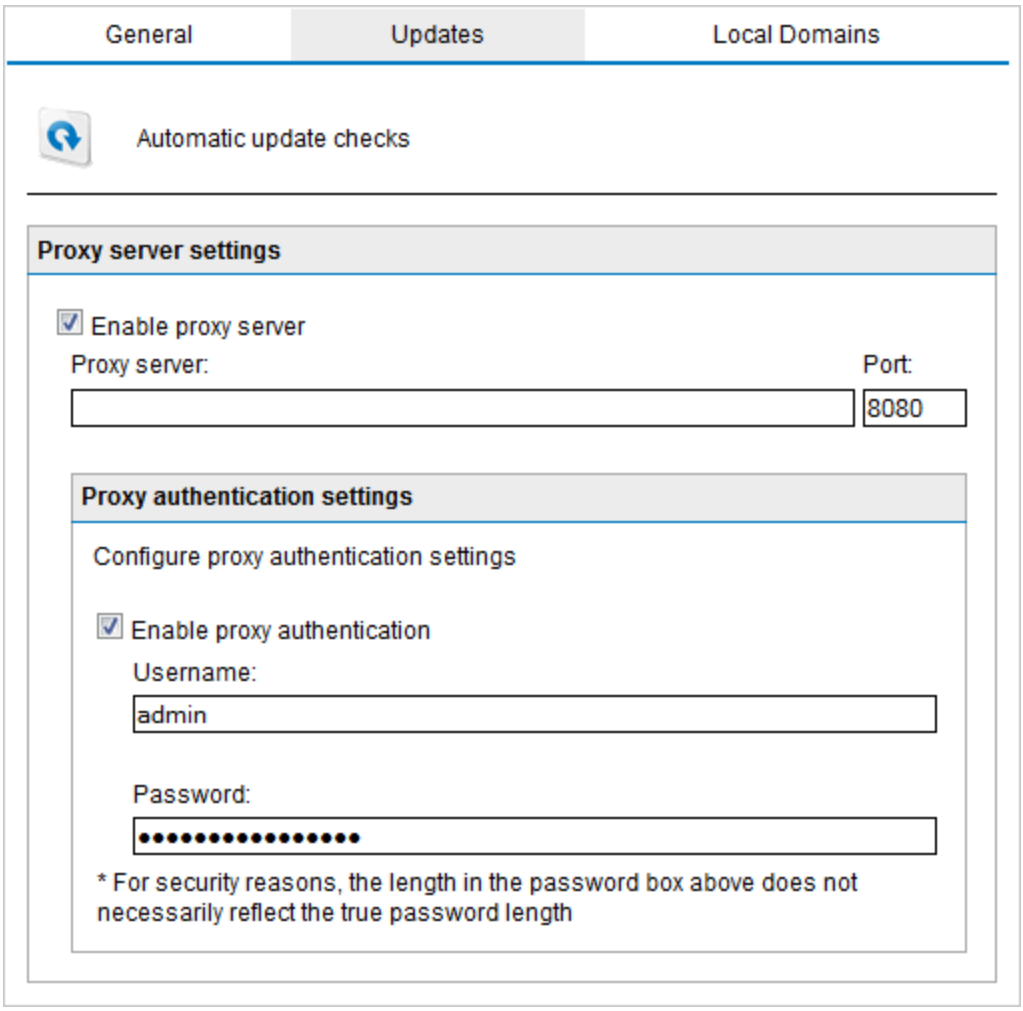
Opção	Descrição
Enable Email Security	Habilita/desabilita os seguintes mecanismos de verificação: » Mecanismos de verificação de vírus » Proteção de armazenamento de informações » Verificador de Cavalo de Troia e Executáveis » Mecanismo de exploração de email » HTML Sanitizer
Enable Anti-Spam	Habilita/desabilita os seguintes filtros anti-spam: » SpamRazer » Anti-phishing » Coleta de diretório » Lista de bloqueio por email » Lista de bloqueio de IP » Lista de bloqueio de DNS de IP » Lista de bloqueio DNS URI » Estrutura de políticas do remetente » Anti-falsificação » Lista de exclusão temporária » Detecção de idioma » Verificação de cabeçalho » Verificação de palavras-chave de spam » Análise bayesiana » Lista de permissão » Novos remetentes
Enable Content Filtering	Habilita/desabilita os seguintes mecanismos de filtragem de conteúdo: » Filtragem de palavra-chave » Filtragem de anexos » Mecanismo de descompactação » Filtragem de conteúdo avançada

3. Clique em **Apply**.

10.3 Configurações de proxy

O GFI MailEssentials verifica automaticamente e faz o download de atualizações (por exemplo, atualizações de definições de vírus e definições do SpamRazer) da Internet. Se o servidor no qual o GFI MailEssentials está instalado estabelecer uma conexão com a Internet por meio de um servidor proxy, defina as configurações de servidor proxy da seguinte forma:

1. Em GFI MailEssentials Configuration, acesse **General Settings > Settings** e selecione a guia **Updates**.



Screenshot 130: Configurações de atualização do servidor proxy

2. Marque a caixa de seleção **Enable proxy server**.

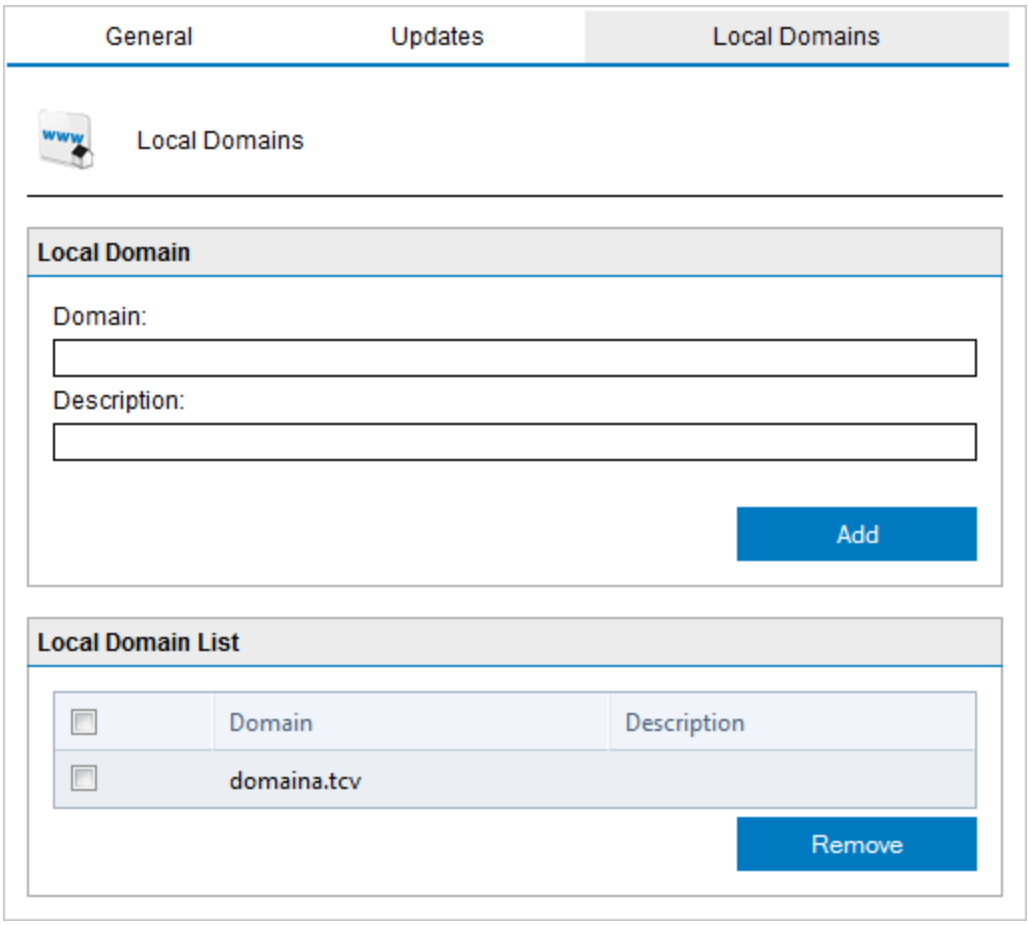
3. No campo **Proxy server**, digite o nome ou o endereço IP do servidor proxy.

4. No campo **Port**, digite a porta na qual se conectar (o valor padrão é 8080).

5. Se o servidor proxy precisar de autenticação, selecione **Enable proxy authentication** e preencha **Username** e **Password**.

6. Clique em **Apply**.

10.4 Domínio local



Screenshot 131: Lista de Domínios locais

O GFI MailEssentials requer a lista de domínios locais a serem habilitados para distinguir entre emails de entrada, saída ou internos. Durante a instalação ou a execução do assistente de pós-instalação, o GFI MailEssentials importa automaticamente os domínios locais no serviço SMTP do IIS ou no Microsoft® Exchange Server. Em alguns casos, no entanto, os domínios locais podem precisar ser adicionados manualmente.

IMPORTANTE
O GFI MailEssentials filtra somente os emails destinados a domínios locais em busca de spam. Algumas regras de filtro também são baseadas na direção. Isso é determinado pelos domínios locais

Para adicionar ou remover domínios locais após a instalação, siga estas etapas:

1. Acesse **General Settings > Settings** e selecione a guia **Local Domains**.
2. Digite o nome e a descrição do domínio a ser adicionado nas caixas de texto **Domain** e **Description**.
3. Clique em **Add** para incluir o domínio indicado na lista de **Local domains**.

OBS.
Para remover um domínio indicado, selecione-o na lista e clique em **Remove**.

4. Clique em **Apply**.

10.5 Gerenciar usuários locais

O GFI MailEssentials usa três formas de recuperação de usuários dependendo do ambiente de instalação.

> **OBS.**
> O número de usuários recuperados também é usado para fins de licenciamento.

10.5.1 GFI MailEssentials instalado no modo Active Directory

Quando o GFI MailEssentials não estiver instalado na mesma máquina do servidor de email e do Active Directory, o GFI MailEssentials recuperará os usuários com email habilitado no domínio do Active Directory do qual a máquina do GFI MailEssentials faz parte.

10.5.2 GFI MailEssentials instalado em uma máquina com o Microsoft® Exchange

Quando o GFI MailEssentials estiver instalado na mesma máquina do Microsoft® Exchange, o GFI MailEssentials recuperará os usuários do Active Directory que possuam uma caixa de correio no mesmo Microsoft® Exchange Server.

10.5.3 GFI MailEssentials instalado no modo SMTP

Quando você optar por instalar o GFI MailEssentials no modo SMTP, a lista de usuários locais será armazenada em um banco de dados gerenciado pelo GFI MailEssentials.

Para preencher e gerenciar a lista de usuários quando o GFI MailEssentials for instalado no modo SMTP, acesse **General > Settings** e selecione a guia **User Manager**.

A guia **User Manager** exibe a lista de usuários locais e permite que você adicione ou remova usuários locais. A lista de usuários locais é usada para configurar regras baseadas em usuários, como regras **Attachment Filtering** e **Content Filtering**.

> **OBS.**
> O GFI MailEssentials preenche automaticamente a lista de usuários locais usando o endereço de email do remetente nos emails de saída.

Para adicionar um novo usuário local:

1. Digite o endereço de email na caixa **Email address**.
2. Clique em **Add**.
3. Repita para adicionar mais usuários locais e clique em **Apply**.

Para remover um usuário local:

1. Selecione o usuário local que você deseja remover na lista **Local Users** e clique em **Remove**.
2. Repita para remover mais usuários locais e clique em **Apply**.

10.6 Licenciamento

Adquira uma licença que seja equivalente ao número de caixas de correio ou usuários protegidos pelo GFI MailEssentials.

Digite a chave de licença adquirida durante a instalação ou em GFI MailEssentials Configuration. Acesse **General Settings > Licensing** e digite sua chave de licença na caixa de texto **License key**. Clique em **Apply**.

10.6.1 Informações sobre a chave de licença

Para analisar as informações da licença, incluindo a data de expiração da assinatura acesse **General Settings > Licensing** e analise os detalhes em **License key information**.

Label (Rótulo)	Descrição
Edição do produto	A edição do GFI MailEssentials dependendo do tipo de assinatura adquirida: » **Anti-spam** – habilita a funcionalidade do filtro anti-spam. Os mecanismos de segurança e anti-malware são desabilitados. » **EmailSecurity** – habilita os mecanismos de verificação de segurança e anti-malware. Os filtros anti-spam são desabilitados. » **UnifiedProtection** – inclui ambas as funcionalidades: anti-spam e segurança de email.
Anti-spam	Mostra se a funcionalidade anti-spam possui licença.
EmailSecurity	Indica se as funcionalidades de segurança e anti-malware possuem licença.
Status da assinatura	A data em que a assinatura expira. Quando a licença expira, o seu servidor de email não estará mais protegido. GFI MailEssentials para de verificar emails e para de baixar as atualizações.
Número de usuários licenciados	O número máximo de usuários permitidos pela licença adquirida.
Número atual de usuários	O número de usuários que estão sendo protegidos pelo GFI MailEssentials.

10.6.2 Como determinar os requisitos de licença

O GFI MailEssentials conta o total de caixas de correio/endereços de email dependendo do ambiente. Para determinar o número de usuários em seu ambiente, acesse http://go.gfi.com/?pageid=ME_RetrieveAndCountUsers.

10.7 Associações do servidor virtual SMTP

O GFI MailEssentials sempre estabelece uma conexão com o primeiro servidor virtual SMTP configurado no IIS. Se houver vários servidores virtuais SMTP, o GFI MailEssentials talvez precise estabelecer uma conexão com um servidor virtual SMTP novo ou diferente.

> **OBS.**
> A guia SMTP Virtual Server Bindings não será exibida se você tiver instalado o GFI MailEssentials em uma máquina com o Microsoft® Exchange Server 2007/2010.

10.7.1 Como estabelecer a conexão do GFI MailEssentials a outro servidor virtual SMTP

> **OBS.**
> Alguns serviços são temporariamente interrompidos quando esta operação é executada. Isso pode afetar o fluxo de emails e/ou a verificação de emails.

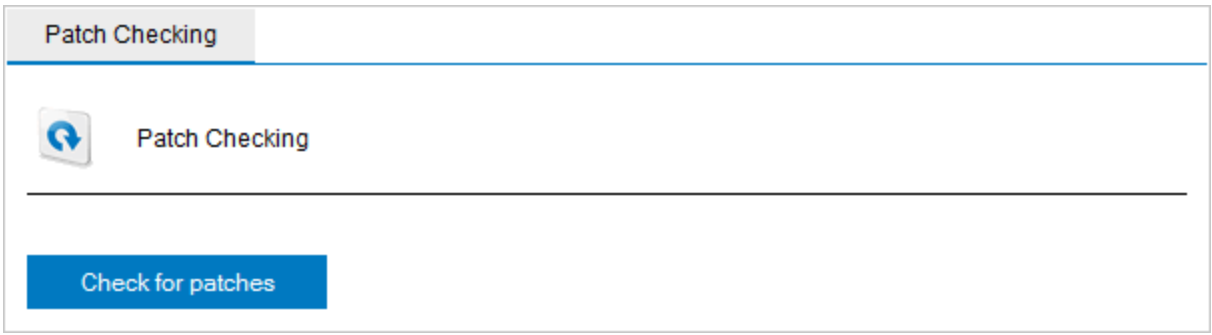
1. Acesse **General Settings > Settings** e clique na guia **Bindings**.
2. Selecione o servidor virtual SMTP ao qual deseja conectar o GFI MailEssentials.
3. Clique em **Apply**.
4. GFI MailEssentials pedirá para reiniciar os serviços para que as novas configurações tenham efeito.

10.8 Verificação de patch

O recurso Patch Checking verifica se há correções de software disponíveis para sua versão do GFI MailEssentials, estabelecendo diretamente uma conexão com os GFI Update Servers.

> **OBS.**
> É altamente recomendável verificar periodicamente se há correções para manter o GFI MailEssentials atualizado.

1. Acesse **General Settings > Patch Checking**.



Screenshot 132: Como verificar correções de produtos

2. Clique em **Check for patches** para estabelecer uma conexão com o GFI Update Server e verificar se há atualizações disponíveis.
3. Clique no link **Download** das correções para fazer o download.
4. Ao concluir, instale as atualizações obtidas por download.

> **OBS.**
> Para acessar as instruções de instalação e outras informações aplicáveis a uma correção, clique no link de informações fornecidas na lista de atualizações disponíveis. Uma instalação de correção incorreta poderá fazer com que o produto funcione incorretamente ou degradar o desempenho.

10.9 Controle de acesso

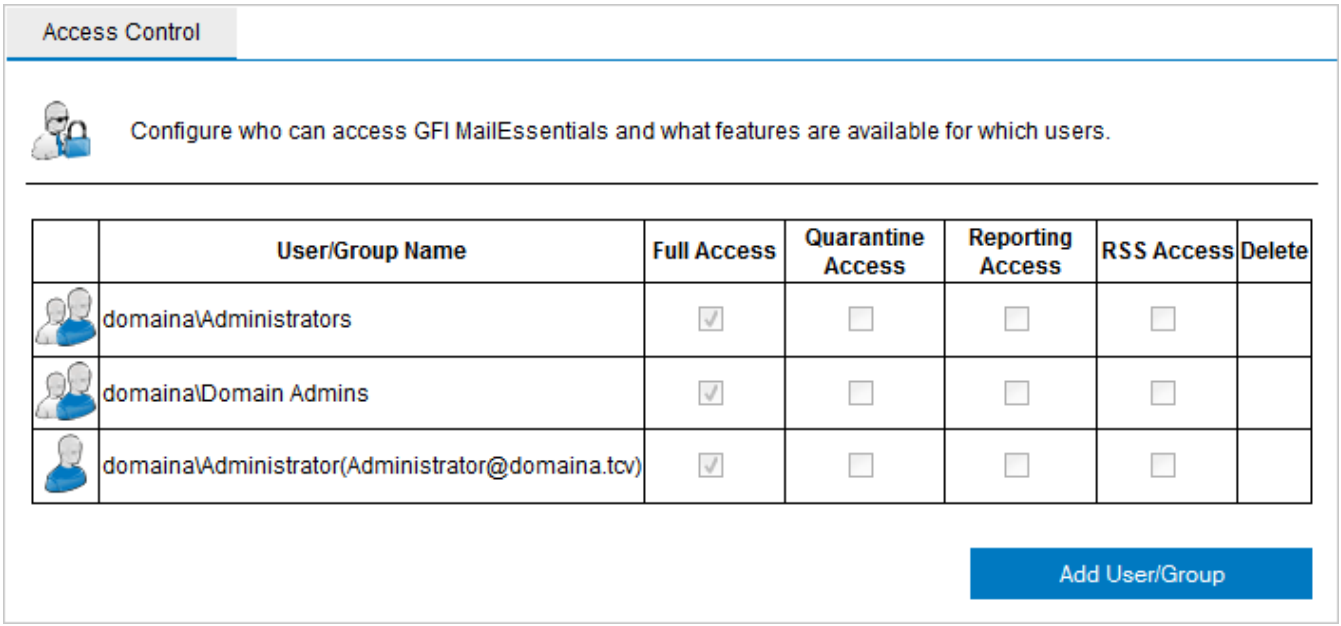
Permita ou bloqueie o acesso a vários recursos do GFI MailEssentials para determinados usuários de domínio ou grupos. Os usuários podem acessar a interface de usuário da Web do GFI MailEssentials usando as credenciais do domínio. Os recursos exibidos para usuários conectados dependem da configuração do controle de acesso.

> **OBS.**
> A configuração do controle de acesso da interface de usuário da Web, só é possível quando o GFI MailEssentials é executado no modo IIS e pode ser acessado pela rede. O controle de acesso pode ser configurado no Menu de controle quando o GFI MailEssentialsé executado no modo local. Para obter mais informações, consulte Lista de controle de acesso (página 252).

O grupo **Admins. do Domínio** (em um ambiente do Active Directory) e a conta/grupo do administrador do servidor recebem privilégios de acesso total a todos os recursos do GFI MailEssentials.

Outros usuários ou grupos podem receber acesso total ou parcial a determinados recursos do GFI MailEssentials . Para adicionar usuários à Lista de controle de acesso:

1. Em GFI MailEssentials Configuration, acesse **General Settings > Access Control**. Adicione usuários de domínio ou grupos e selecione os recursos do produto aos quais permitir o acesso.



Screenshot 133: Configurações do controle de acesso

2. Clique em **Add User/Group**.

3. No diálogo **User Lookups**, digite o nome do usuário ou grupo para adicionar e clique em **Check Names**.

4. GFI MailEssentials exibe a lista de usuários/grupos encontrados. Selecione os usuários/grupos para adicionar e clique em **Submit**.

5. Para os novos usuários/grupos adicionados, selecione os recursos aos quais permitir o acesso.

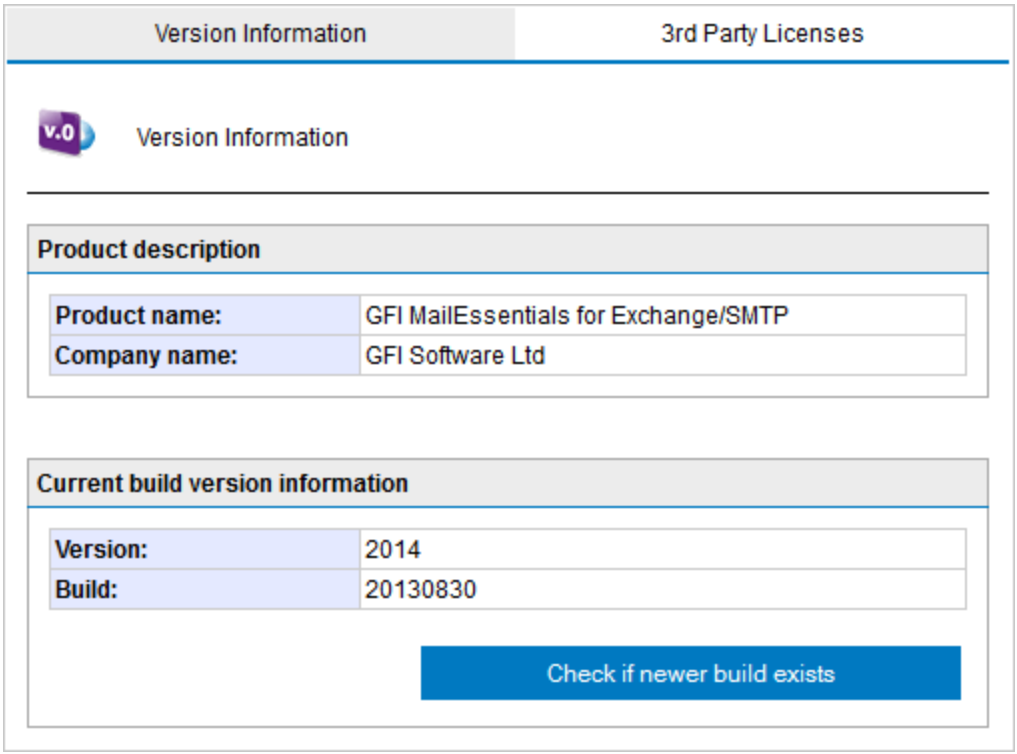
Permissão	Descrição
Full Access	O usuário pode acessar e configurar todos os recursos do produto.
Quarantine Access	Permite o acesso à pesquisa de quarentena e pastas de pesquisa.
Reporting Access	Permite que os usuários gerem relatórios.
RSS Access	Permite que os usuários assinem feeds RSS em quarentena.

6. Clique em **Apply**.

11 Tópicos diversos

Tópicos deste capítulo:

11.1 Informações sobre a instalação



Screenshot 134: Página de informações de versão

Para visualizar as informações da versão do GFI MailEssentials, acesse o nó **About**. A guia **Version Information** exibe a versão de instalação e o número da compilação do GFI MailEssentials.

Para verificar se você tem a compilação mais recente do GFI MailEssentials instalada em seu computador, clique em **Check if newer build exists**.

> **OBS.**
> Sempre informe a versão do GFI e as informações da compilação quando entrar em contato com o suporte da GFI.

A guia **3rd Party Licenses** lista os componentes de terceiros usados pelo GFI MailEssentials.

11.2 Nomes de diretório virtual

Os nomes do diretório virtual padrão de GFI MailEssentials e do Quarantine RSS são **MailEssentials** e **MailEssentialsRSS**, respectivamente. Os nomes de diretórios virtuais são personalizáveis. Contudo, é recomendado que eles não sejam alterados.

> **OBS.**
> Se o GFI MailEssentials estiver configurado para ser acessado apenas na máquina local, o diretório virtual GFI MailEssentialsConfiguration não é configurável.

1. Inicie o GFI MailEssentials Switchboard a partir de **Start > Programs > GFI MailEssentials > Switchboard**.

2. Na área **IIS user interface mode options**, especifique nomes personalizados de diretório virtual para:

» GFI MailEssentials Configuração: digite um nome personalizado no campo **Diretório virtual**.

» Diretório virtual de RSS em quarentena: digite um nome personalizado no campo **RSS Virtual directory**.

3. Clique em **Apply**.

4. Clique em **OK** e aguarde enquanto as novas configurações são aplicadas.

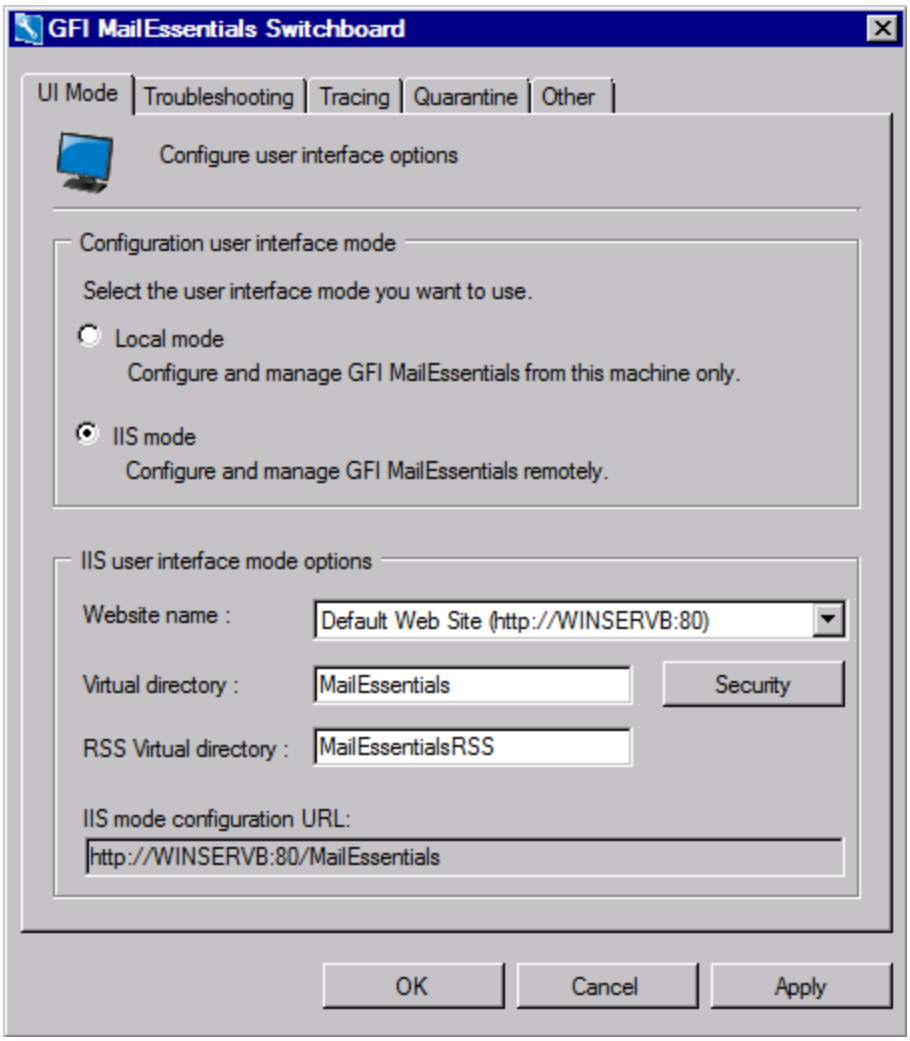
5. Quando o processo terminar, clique em **OK**.

11.3 Modo da interface de usuário

A interface de usuário do GFI MailEssentials pode ser carregada somente na máquina de instalação (modo local) ou acessada pela rede via HTTP (modo IIS).

Para selecionar o modo:

1. Inicie o GFI MailEssentialsSwitchboard a partir de **Start > Programs > GFI MailEssentials > Switchboard**.



Screenshot 135: Menu de controle do GFI MailEssentials - Modo de interface do usuário

2. Na área **UI mode**, selecione:

Opção	Descrição
Local mode	O GFI MailEssentials carrega um aplicativo visualizador de HTML, acessível na máquina em que o GFI MailEssentials está instalado. **OBS.** Se usar o modo local: » Os links de resumo de spam não funcionarão » Portal de usuário não estará disponível: os usuários não serão capazes de gerenciar listas de permissão e listas de bloqueio pessoais e a quarentena pessoal. Para obter mais informações, consulte Ações do usuário final (página 21).
IIS mode (recommended)	O GFI MailEssentials é carregado em seu navegador da Web padrão usando as definições de configuração do IIS definidas durante a instalação. A interface do usuário também pode ser acessada na rede via HTTP. **OBS.** As definições de configuração do IIS podem ser alteradas usando o nome do site da Web, o diretório virtual e os campos RSS do diretório virtual. As opções **Security** permitem a configuração de uma Lista de controle de acesso e a Autenticação do IIS.

OBS.
Alguns serviços são temporariamente interrompidos quando esta operação é executada. Isso pode afetar o fluxo de emails e/ou a verificação de emails.

3. Clique em **Yes** para reiniciar os serviços exibidos.

4. Clique em **OK**.

11.3.1 Configurações de segurança do IIS

O botão **Security** na guia do modo de interface do usuário permite configurar uma Lista de controle de acesso e um Método de autenticação.

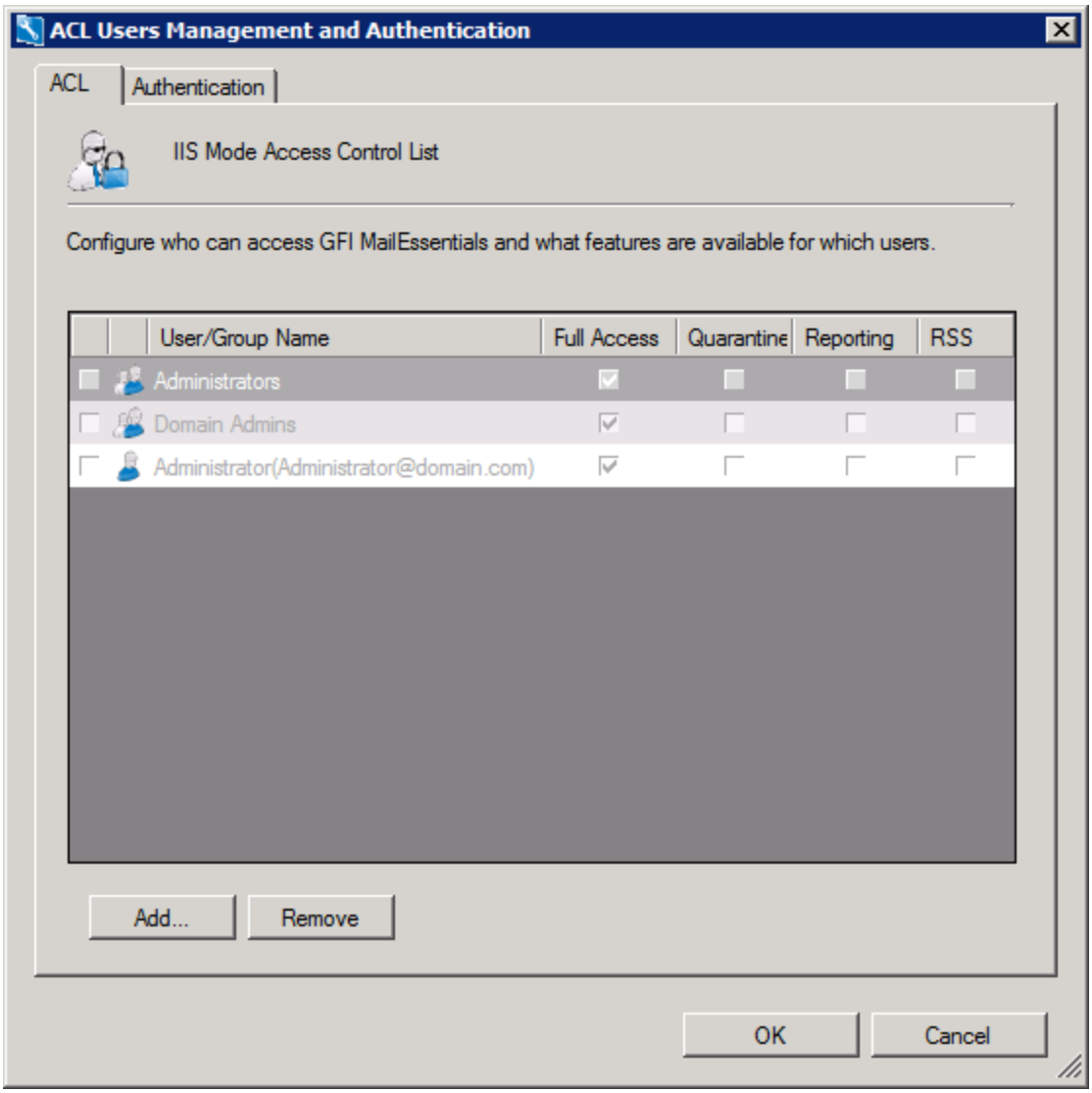
Lista de controle de acesso

A lista de controle de acesso especifica quem pode acessar o GFI MailEssentials e quais recursos estão disponíveis para quais usuários ou grupos. Por padrão, os administradores têm acesso total ao GFI MailEssentials. No entanto, você pode definir usuários ou grupos específicos com diferentes tipos de acesso.

Para adicionar um usuário:

1. Para carregar o Menu de controle, clique em **Iniciar > Programas > GFI MailEssentials > Switchboard**.

2. Selecione a guia **UI Mode**. Clique em **IIS Mode** e selecione **Security**.



Screenshot 136: IIS Security - Guia ACL

3. Clique em **Add...** e forneça o nome do usuário ou grupo que deseja adicionar à lista.

4. Selecione o tipo de acesso que deve ser concedido. As opções disponíveis são:

Permissão	Descrição
Full Access	O usuário pode acessar e configurar todos os recursos do produto.
Quarantine Access	Permite o acesso à pesquisa de quarentena e pastas de pesquisa.
Reporting Access	Permite que os usuários gerem relatórios.
RSS Access	Permite que os usuários assinem feeds RSS em quarentena.

5. Clique em **OK** para finalizar a configuração.

Para remover o acesso de um usuário ou grupo, selecione o item para remover e clique em **Remove**.

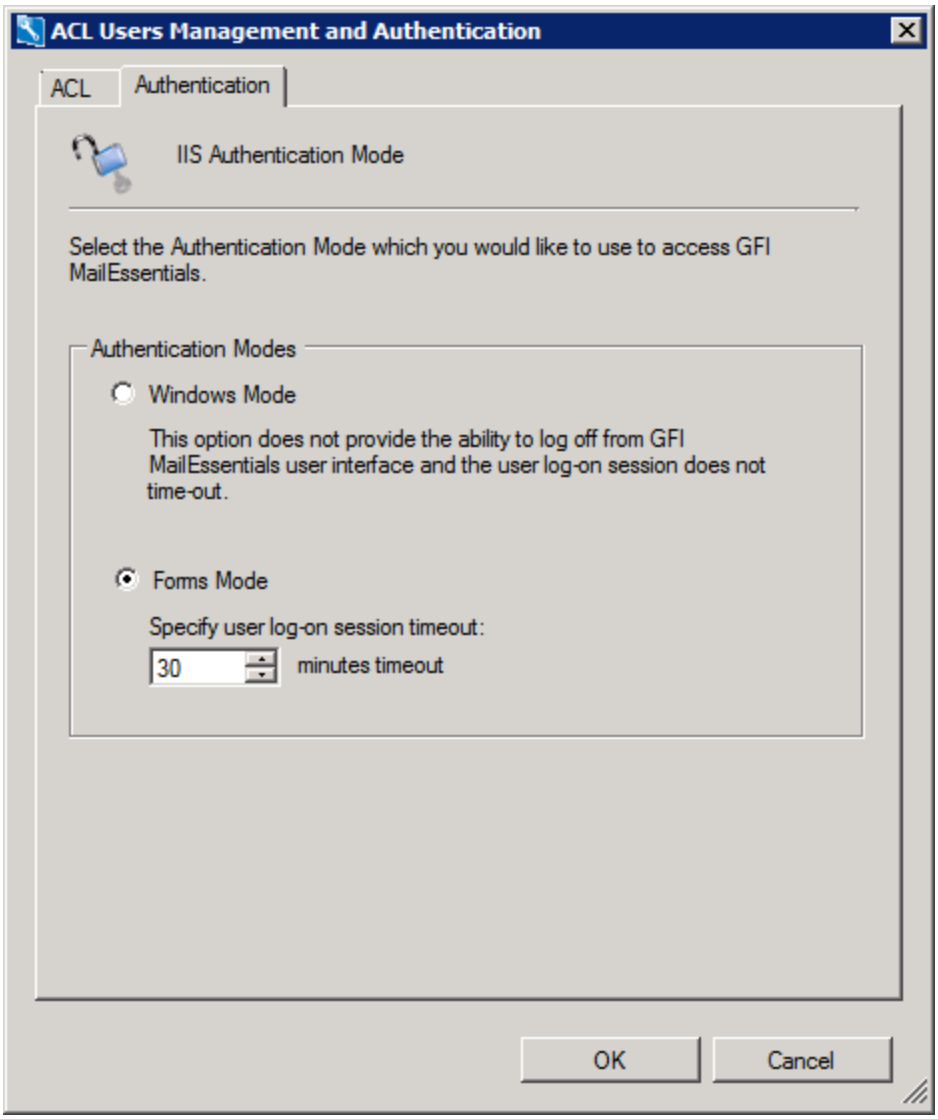
Modo de autenticação IIS

O Modo de autenticação do IIS permite que você escolha o método de autenticação a ser usado ao acessar o GFI MailEssentials.

1. Para carregar o Menu de controle, clique em **Iniciar > Programas > GFI MailEssentials > Switchboard**.

2. Selecione a guia **UI Mode**. Clique em **IIS Mode** e selecione **Security**.

3. Selecione a guia **Authentication**.



Screenshot 137: IIS Security - Guia Authentication

4. Selecione uma das opções disponíveis:

Opção	Descrição
Windows Mode	A autenticação do Windows ativa o GFI MailEssentials para usar as credenciais do usuário atualmente conectado e não fornece log-off e o tempo limite da sessão de interface do usuário.
Forms Mode	(Padrão) A autenticação de formulários permite que os usuários façam log-off. Ela também permite que você configure um tempo limite automático para a sessão de interface do usuário. Isso é recomendado se os usuários finais estiverem acessando o console do usuário do GFI MailEssentials, especialmente em computadores públicos.

5. Clique em **OK** para salvar as configurações.

11.4 Emails com falha

Em alguns casos, a segurança de email ou os filtros de conteúdo do GFI MailEssentials não poderão verificar um email, por exemplo, emails contendo informações de cabeçalho corrompidas. Nesse caso, o GFI MailEssentials bloqueia o email, pois ele pode ter conteúdo mal-intencionado, e move-o para a seguinte pasta:

<GFI MailEssentials caminho instalação>\EmailSecurity\failedmails

11.4.1 Reprocessando de emails legítimos com falha

É recomendável entrar em contato com o suporte da GFI quando vários emails forem movidos para a pasta **failedmails**. Quando o problema for resolvido, os emails podem ser verificados novamente pelo GFI MailEssentials para determinar se são seguros para serem entregues.

> **OBS.**
> Arquivos com a extensão .PROP na pasta **failedmails** são usados para solucionar problemas. Ao reprocessar emails com falha, esses arquivos poderão ser excluídos.

GFI MailEssentials instalado no Microsoft® Exchange Server 2007/2010

1. Na pasta **failedmails**, altere a extensão dos arquivos .TXT para .EML.

> **OBS.**
> Para mudar automaticamente a extensão de todos os arquivos .TXT na pasta **failedmails** para .EML, no prompt de comando, mude o diretório para a pasta **failedmails** e execute o seguinte comando:
> `ren *.txt *.eml`

2. Mova os arquivos renomeados para a seguinte pasta:

<unidade>\Arquivos de Programas\Microsoft\Exchange Server\TransportRoles\Replay

GFI MailEssentials instalado no Microsoft® Exchange Server 2003

Mova os emails (no formato .txt) da pasta **failedmails** para a seguinte pasta:

<Caminho de instalação do Microsoft Exchange>\Exchsrvr\Mailroot\vsi 1\PickUp

GFI MailEssentials instalado no servidor de Gateway

Mova os emails (no formato .txt) da pasta **failedmails** para a seguinte pasta:

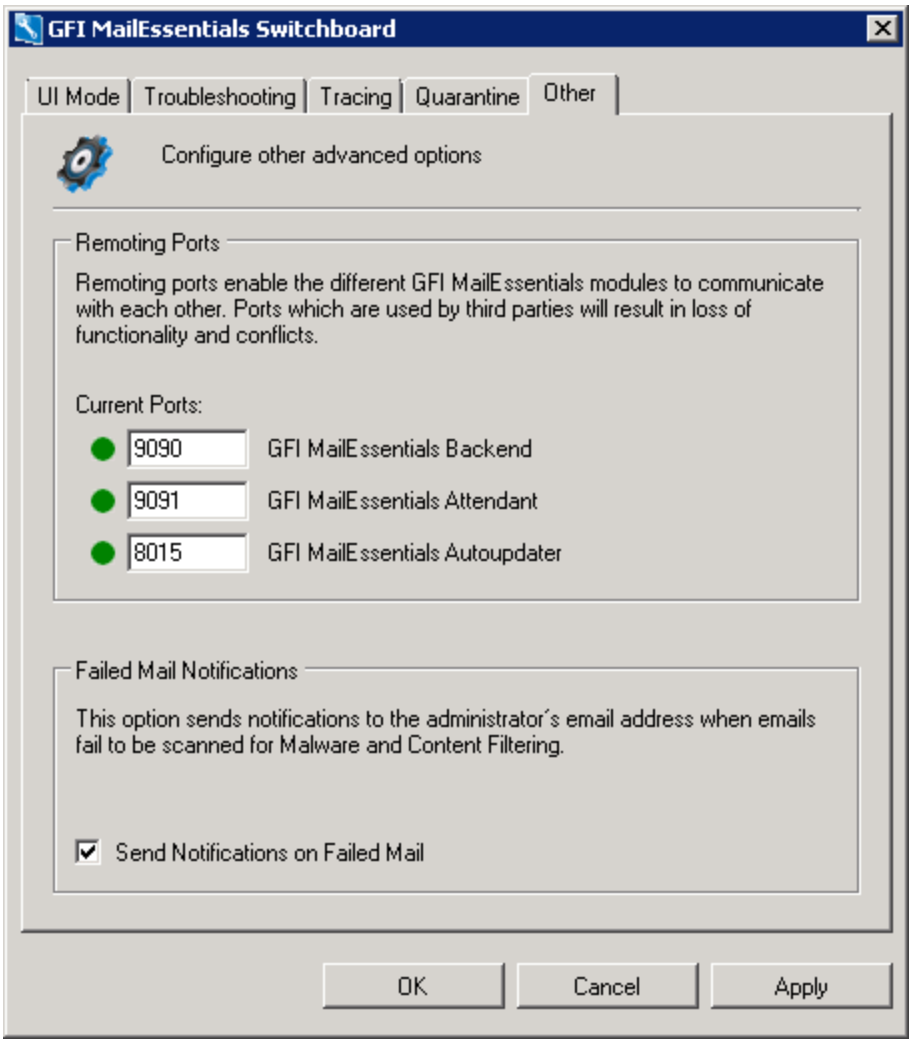
<drive>\Inetpub\mailroot\Pickup

11.4.2 Notificações de emails com falha

O GFI MailEssentials pode ser configurado para notificar o administrador quando ocorrer falha no processamento de um email.

O endereço de email do administrador pode ser configurado no nó General Settings do GFI MailEssentials. Para obter mais informações, consulte Endereço de email do administrador (página 240).

1. Inicie o GFI MailEssentials Switchboard em **Iniciar > Programas > GFI MailEssentials > Switchboard** e selecione a guia **Other**.



Screenshot 138: Ativar a notificação emails com falha

2. Selecione **Send Notifications on Failed Mail**.

3. Clique em **Apply**.

> **OBS.**
> Alguns serviços são temporariamente interrompidos quando esta operação é executada. Isso pode afetar o fluxo de emails e/ou a verificação de emails.

4. Clique em **Yes** para reiniciar os serviços exibidos.

5. Clique em **OK**.

11.5 Rastreamento

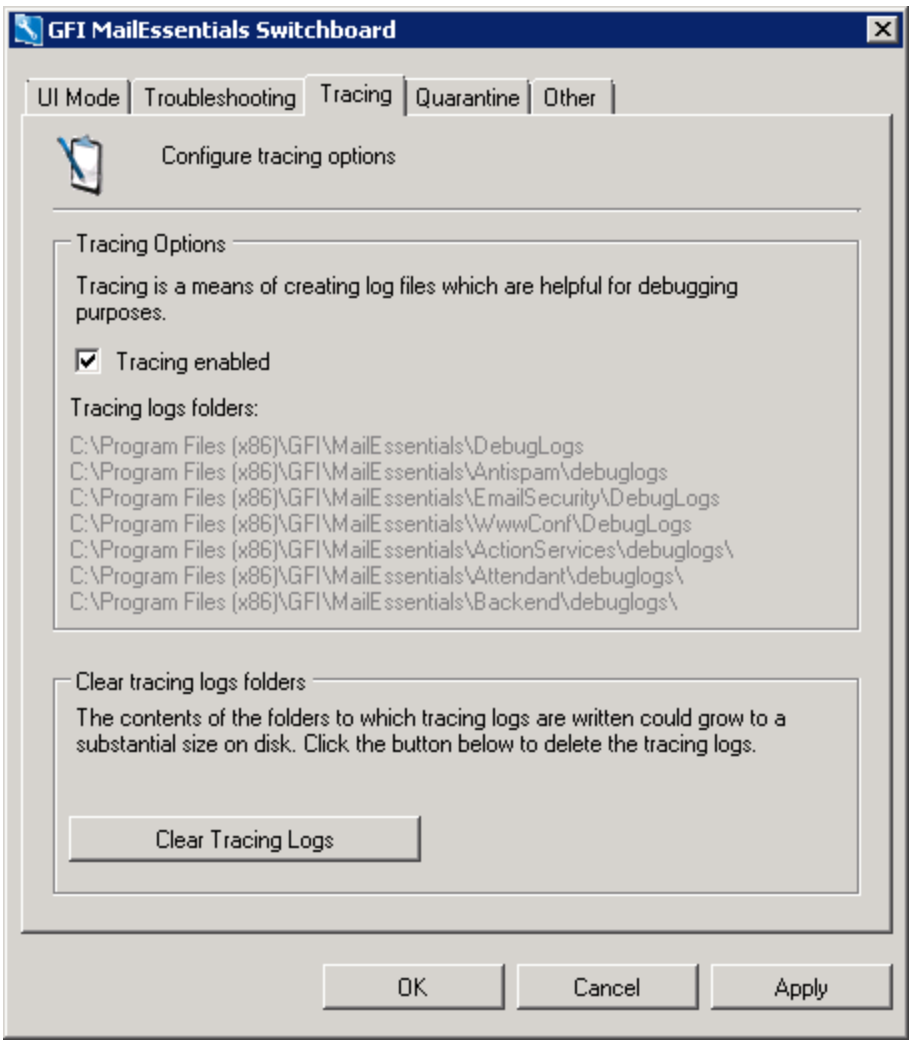
O GFI MailEssentials oferece a capacidade de criar arquivos de registro para fins de depuração. Use o rastreamento para solucionar problemas ou quando entrar em contato com o suporte da GFI. Desative o rastreamento se houver problemas de desempenho no GFI MailEssentials.

Quando ativado, o GFI MailEssentials armazena vários arquivos de registro nas seguintes pastas:

- <*GFI MailEssentials installation path*>*GFI**MailEssentials*\DebugLogs\
- <*GFI MailEssentials installation path*>*GFI**MailEssentials*\Antispam\DebugLogs\
- <*GFI MailEssentials installation path*>*GFI**MailEssentials*\EmailSecurity\DebugLogs\
- <*GFI MailEssentials installation path*>*GFI**MailEssentials*\WwwConf\DebugLogs\
- <*GFI MailEssentials installation path*>*GFI**MailEssentials*\ActionServices\DebugLogs\
- <*GFI MailEssentials installation path*>*GFI**MailEssentials*\Attendant\DebugLogs\
- <*GFI MailEssentials installation path*>*GFI**MailEssentials*\Backend\DebugLogs\

Para ativar ou desativar o rastreamento:

1. Inicie o GFI MailEssentials Switchboard em **Iniciar > Programas > GFI MailEssentials > Switchboard** e selecione a guia **Tracing**.



Screenshot 139: Configurar as opções de rastreamento

2. Selecione ou desmarque **Tracing enabled** para ativar ou desativar o registro, respectivamente.

> **OBS.**
> Alguns serviços são temporariamente interrompidos quando esta operação é executada. Isso pode afetar o fluxo de emails e/ou a verificação de emails.

3. Clique em **Yes** para reiniciar os serviços exibidos.

4. Clique em **OK**.

Limpar os registros de rastreamento

Para excluir todos os registros de rastreamento:

1. Inicie o GFI MailEssentials Switchboard em **Iniciar > Programas > GFI MailEssentials > Switchboard** e selecione a guia **Tracing**.

> **OBS.**
> Alguns serviços são temporariamente interrompidos quando esta operação é executada. Isso pode afetar o fluxo de emails e/ou a verificação de emails.

2. Clique em **Clear Tracing Logs** e clique em **Yes** para reiniciar os serviços exibidos.

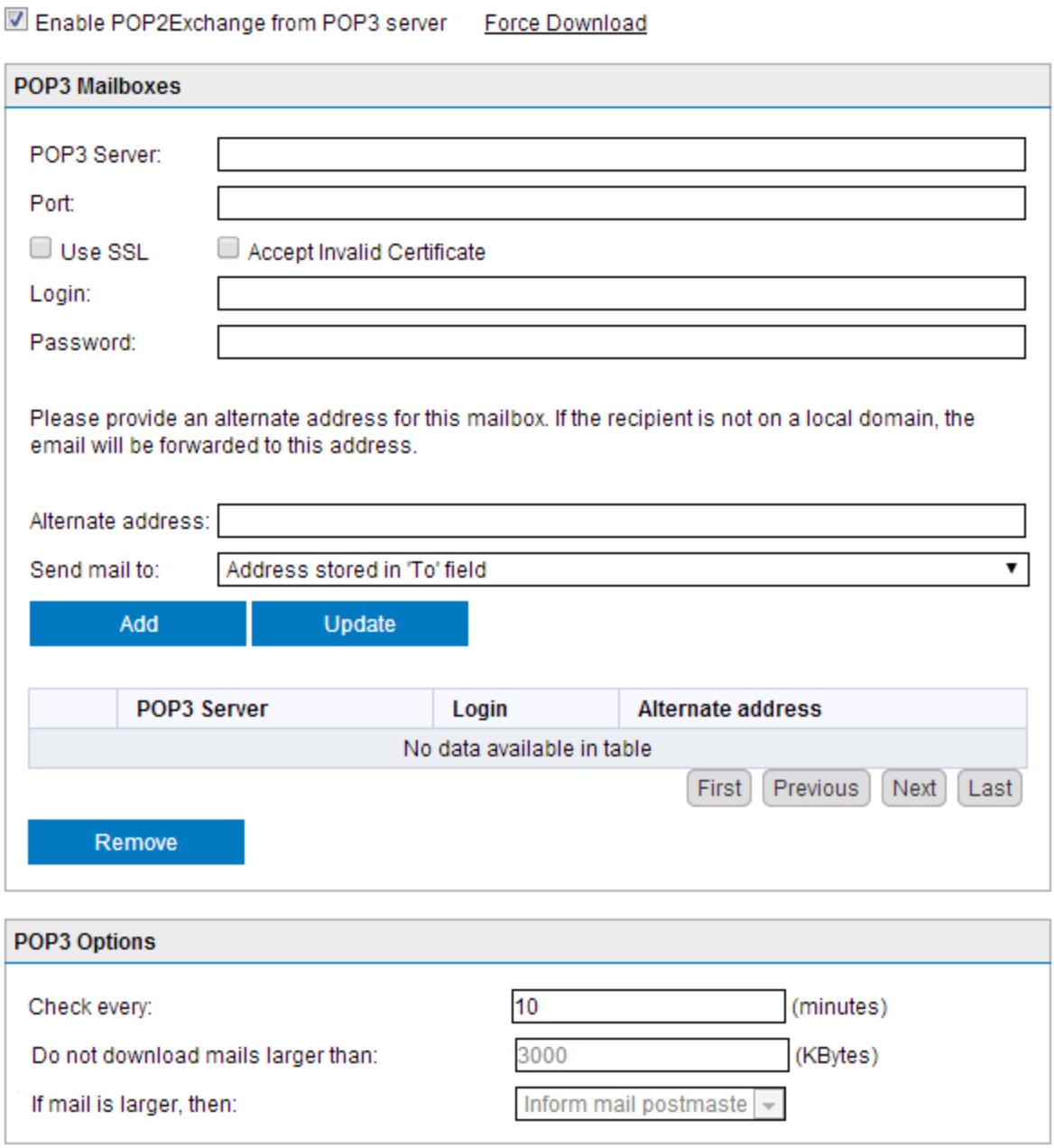
3. Clique em **OK** quando concluir.

11.6 POP2Exchange - Download de emails do servidor POP3

O Pop2Exchange faz o download de emails de um servidor POP3, processa esses emails e os envia para o servidor de email local. A recomendação para o GFI MailEssentials é, se possível, evitar o uso do POP3 e usar SMTP, pois o POP3 foi desenvolvido para clientes de email, não para servidores de email. Apesar desse fato e levando em conta situações nas quais um endereço IP estático exigido pelo SMTP não esteja disponível, o GFI MailEssentials poderá usar POP3 para recuperar emails.

11.6.1 Configurar o POP3 downloader

1. Acesse o nó **POP2Exchange**.



Screenshot 140: O GFI MailEssentials POP3 Downloader

2. Na guia **POP3**, selecione **Enable POP2Exchange from POP3 server** para ativar odPOP3 Downloader.

3. Na caixa **POP3 Mailboxes**, especifique os detalhes dos servidores POP3 para fazer o download de emails de:

Opção	Descrição
POP3 Server	Digite o endereço IP do servidor POP3 do qual fazer o download de emails.
Port	Digite o número da porta do POP3. Por padrão, o POP3 usa a porta 110 ou a porta 995 com uma conexão segura.
Use SSL	Selecione se o servidor POP3 exige uma conexão segura.

Opção	Descrição
Accept Invalid Certificate	Selecione esta opção se você quiser ignorar certificados não verificados do servidor POP3. É recomendável desmarcar essa opção para garantir que todos os certificados sejam validados.
Login & Password	Especifique as credenciais para fazer login na caixa de correio do POP3.
Alternate address	Se os emails na caixa de correio forem endereçados a um destinatário que não está em um dos domínios locais do GFI MailEssentials domínios locais, os emails serão enviados para esse endereço. Certifique-se de que esse é um endereço local, configurado no servidor de emails e protegido pelo GFI MailEssentials.
Send mail to:	Selecione: » **Address stored in 'To' field**: GFI MailEssentials analisa o cabeçalho do email e direciona os emails de acordo com a necessidade. Se a análise de emails falhar, o email será enviado para o endereço de email especificado no campo **Alternate address**. » **Alternate address**: GFI MailEssentials não analisa os cabeçalhos de email e todos os emails nessa caixa de correio são encaminhados para o endereço de email configurado em **Alternate address**.

4. Clique em **Add** para adicionar os detalhes do servidor POP3. Selecione um POP3 Server adicionado e clique em **Update** para substituí-lo pelas configurações digitadas.

5. Repita as etapas acima para adicionar vários servidores POP3.

6. Em **POP3 Options**, configure:

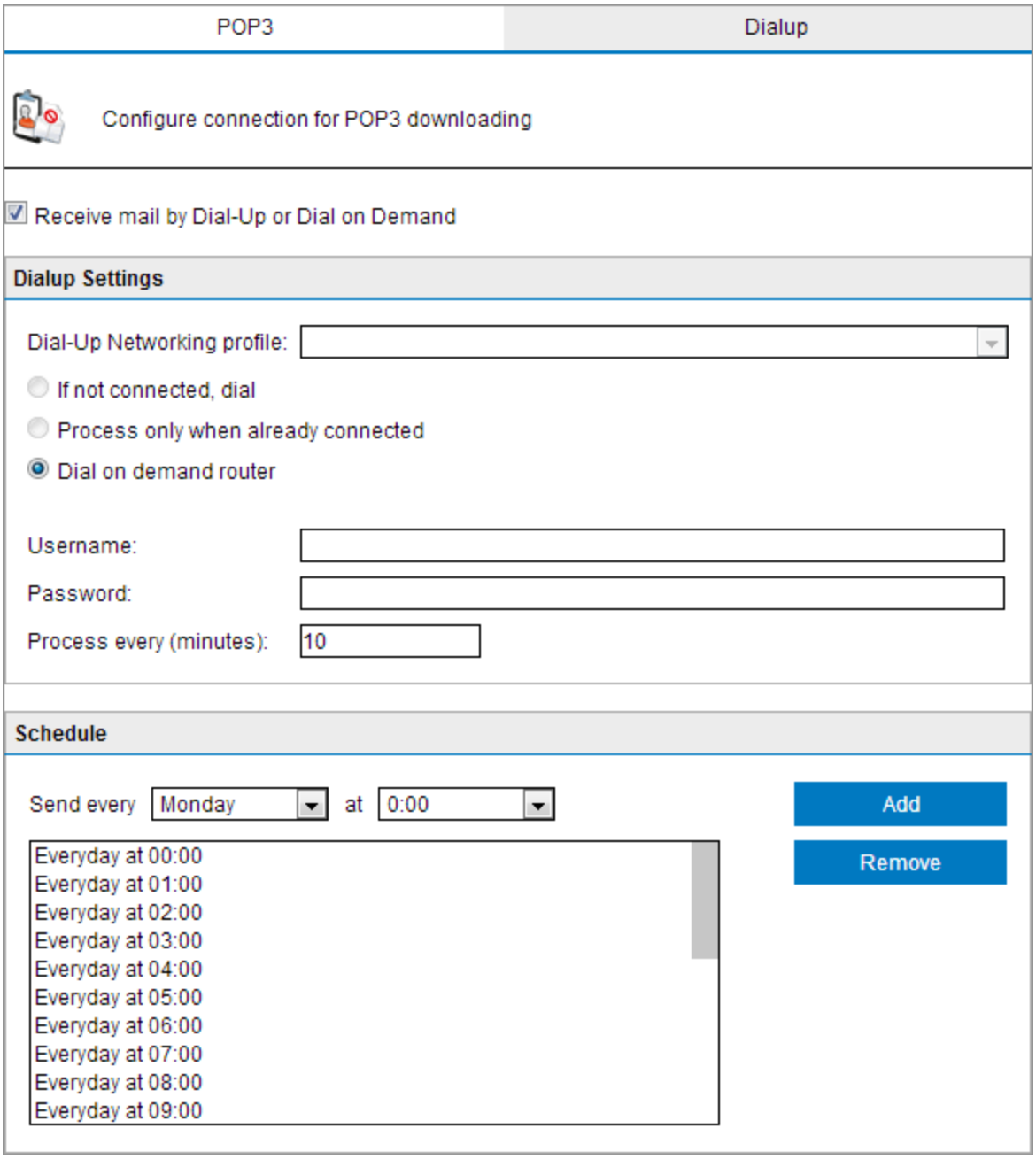
Opção	Descrição
Check every (minutes)	Especifique o intervalo do download em minutos.
Do not download mails larger than	Especifique um tamanho máximo de download em KB. Se o email ultrapassar esse tamanho, ele não será transferido por download.
If mail is larger, then:	Opte por excluir emails com tamanho maior que o máximo permitido ou envie uma mensagem para o postmaster.

8. Clique em **Apply**.

11.6.2 Configurar as opções de conexão discada

1. Acesse o nó **POP2Exchange** e selecione a guia **Dialup**.

2. Selecione **Receive mails by Dial-Up or Dial on Demand**.



Screenshot 141: Opções de discagem

3. Selecione um perfil de rede dial-up e configure um nome de usuário e senha. As seguintes opções estão disponíveis:

Opção	Descrição
Use this Dial-Up Networking profile	Escolha o perfil de rede discada a ser usado.
If not connected, dial	O GFI MailEssentials só discará se não houver conexão.
Process only when already connected	O GFI MailEssentials só processará o email se já existir uma conexão.

Opção	Descrição
Dial on demand router:	No caso de uma conexão com a Internet estabelecida automaticamente (como roteador de discagem sob demanda), selecione esta opção. GFI MailEssentials coletará emails no intervalo especificado sem acionar uma conexão discada.
Username & Password	Insira as credenciais utilizadas para fazer logon em seu Provedor de Serviços de Internet.
Process every (minutes)	Digite o intervalo em minutos.

4. Na área **Schedule**, especifique as horas nas quais o GFI MailEssentials deverá discar para coletar emails.

5. Clique em **Apply**.

11.7 Transferir email de spam para as pastas da caixa de correio do usuário

Quando o GFI MailEssentials estiver instalado no Microsoft® Exchange Server, emails de spam podem ser salvos em um pasta de correio do usuário. Para obter mais informações, consulte Ações de spam - O que fazer com emails de spam (página 148).

Se o GFI MailEssentials**NÃO** estiver instalado no Microsoft® Exchange Server, os emails de spam não podem ser direcionados para a pasta da caixa de correio de um usuário específico por meio das Spam Actions. No entanto, os emails podem continuar sendo encaminhados para a caixa de correio do usuário, como descrito abaixo.

11.7.1 Microsoft® Exchange 2007/2010

Para configurar o Microsoft® Exchange 2007/2010 para encaminhar emails marcados para a pasta Lixo Eletrônico da caixa de email, uma Regra de Transporte deverá ser criada.

> **IMPORTANTE**
> Em Spam Actions do GFI MailEssentials, selecione a ação Marcar o email com texto específico apenas. Se você selecionar qualquer outra ação, as mensagens detectadas como spam não chegarão à caixa de correio do usuário e, portanto, as regras de transporte configuradas não serão aplicáveis.

Para criar uma Regra de Transporte no Exchange 2007/2010:

1. Inicie o Console de Gerenciamento do Microsoft® Exchange.

2. Acesse **Microsoft Exchange > Organization Configuration > Hub Transport** e selecione o nó **Transport Rules**.

3. Clique em **New Transport Rule**.

4. Digite um nome para a nova regra (por exemplo, GFI MailEssentials `SPAM`) e clique em **Next**.

5. Na área **Conditions**, selecione **When the Subject field contains specific words**.

6. Na área **Edit rule**, clique em **Specific Words** para inserir as palavras usadas para marcar. Digite a marca especificada nas ações de spam de cada filtro de spam (por exemplo, `[SPAM]`) e clique em **Adicionar**. Clique em **OK** quando todas as palavras forem adicionadas e clique em **Next**.

7. Na área **Actions**, selecione **Set the spam confidence level to value**.

8. Na área **Edit rule**, clique em **0** e defina o nível de confiança para **9**. Clique em **OK** e em **Next**.

9. (Opcional) Configure as exceções a essa regra de transporte e clique em **Next**.

10. Clique em **New** para criar a nova Regra de Transporte.

> **OBS.**
> Certifique-se de que a pasta Lixo Eletrônico esteja ativada para as caixas de correio dos usuários.

A regra de transporte criada encaminhará todos os emails que contêm a marca GFI MailEssentials para a pasta Lixo Eletrônico dos usuários.

11.7.2 Microsoft® Exchange Server 2003

O GFI MailEssentials inclui um utilitário Rules Manager que envia automaticamente emails marcados como spam para a caixa de correio de usuários.

> **IMPORTANTE**
> Usar o Rules Manager, em Spam Actions selecione a opção **Tag the email with specific text** e especifique uma tag.

Instale o Gerenciador de Regras no Microsoft® Exchange Server

1. Na máquina do GFI MailEssentials, acesse:

<*GFI MailEssentials installation path*>\GFI\MailEssentials\Antispam\

2. Copie os seguintes arquivos para uma pasta no Microsoft® Exchange Server:

- rulemgmtres.dll
- rulemgmt.exe
- rule.dll
- gfi_log.dll

3. No Microsoft® Exchange Server, abra um prompt de comando e altere o diretório para o local onde os arquivos do Gerenciador de Regras foram copiados.

4. No prompt de comando, digite `regsvr32 rule.dll`

5. Na confirmação, clique em **OK**.

Inicie o Gerenciador de Regras

1. No Microsoft® Exchange Server, acesse o local no qual os arquivos do Gerenciador de Regras foram copiados e abra **rulemgmt.exe**.

2. Selecione um perfil do Microsoftt® Outlook (perfil MAPI) ou crie um novo perfil de login (quando usar o Gerenciador de Regras pela primeira vez).

3. Clique em **OK** para iniciar o Gerenciador de Regras.

4. A janela principal do Gerenciador de Regras mostra todas as caixas de correio habilitadas no Microsoft® Exchange Server. A cor das caixas de correio indica o status da caixa de correio:

» Azul - caixa de correio que tem regras configuradas

» Preto - caixa de correio que não tem regras configuradas.

Configurar novas regras

1. Marque as caixas de correio para definir uma regra e clique em **Configure…**.

> **OBS.**
> 1. Novas regras podem ser adicionadas às caixas de correio que já contém regras.
> 2. Selecione várias caixas de correio para configurar a mesma regra aplicável a todas as caixas de correio.

2. Na caixa de texto **Rule Condition**, digite a tag do email de mensagem de spam nas ações de spam GFI MailEssentials ações de spam.

3. Especifique a **Rule action**:

» Selecione **Delete** para excluir um email que possui um assunto que contém a regra condição

» Selecione **Move to:** para transferir emails de spam para uma pasta na caixa de correio. Digite o caminho da pasta na qual salvar o email de spam. Se você especificar Inbox\Spam, uma pasta spam será criada na pasta Inbox. Se você especificar apenas Spam, a pasta será criada no nível superior (mesmo nível da caixa de entrada).

4. Clique em **Apply** para salvar o conjunto de regras.

Gerenciar várias regras

Mais de uma regra pode ser definida na mesma caixa de correio.

Exemplo: Exclua emails marcados com `[Phishing]` e mova emails marcados com `[SPAM]` para a pasta Inbox\Spam.

1. Clique duas vezes em uma caixa de correio para abrir o diálogo Rules.

2. Uma lista de regras aplicáveis para a caixa de correio selecionada é exibida.

» Clique em **Add rule** para adicionar uma nova regra

» Selecione uma regra e clique em **Edit rule** para alterar as configurações da regra selecionada

» Selecione uma regra e clique em **Delete rule** para excluir a regra selecionada.

3. Clique em **Apply** para salvar as alterações.

11.8 Transferir spam para a pasta do Exchange 2010

Quando o GFI MailEssentials for instalado em um servidor Microsoft® Exchange 2010, um usuário dedicado deverá ser criado para usar a ação anti-spam **Deliver email to mailbox - In Exchange mailbox sub-folder**. Configure o usuário dedicado no GFI MailEssentials Switchboard.

OBS.
Se um usuário não estiver configurado, o spam não poderá ser movido para uma subpasta da caixa de correio.

Para configurar um usuário dedicado:

1. Inicie o GFI MailEssentialsSwitchboard a partir de **Iniciar > Programas > GFI MailEssentials > Switchboard**.

2. Selecione a guia **Move to Exchange**

OBS.
Essa guia só será exibida quando o GFI MailEssentials está instalado no servidor Microsoft® Exchange 2010.

3. Clique em **Specify user account...** para especificar o usuário dedicado.

4. Selecione uma das seguintes opções:

Opção	Descrição
Move spam using an automatically created user	Permite que o GFI MailEssentials crie um usuário automaticamente com todos os direitos necessários.
Move spam using the following user account	Use um usuário criado manualmente. Especifique as credenciais (**Domain\username** e **Password**) de um usuário dedicado e clique em **Set access rights** para atribuir as permissões necessárias ao usuário especificado.

OBS.
As credenciais de usuário especificadas manualmente devem ser dedicadas somente a este recurso. Nome de usuário, senha e outras propriedades não devem ser alteradas no Microsoft® Exchange ou no Active Directory. Caso contrário, o recurso não funcionará.

5. Clique em **Finish** para aplicar as configurações.

6. Clique em **OK**.

11.9 Sincronizar dados de configuração

Quando o GFI MailEssentials estiver instalado em diversos servidores, é importante manter os dados de configuração sincronizados entre servidores.

O GFI MailEssentials permite esse processo através de dois recursos que mantêm várias instalações doGFI MailEssentialssincronizadas:

» Agente de sincronização anti-spam – Este serviço automatiza o processo de manutenção da sincronia das configurações anti-spam entre instalações separadas usando o serviço Microsoft® BITS.

» Configuration Export/Import Tool - Este aplicativo permite a exportação manual das definições de configuração doGFI MailEssentials e a importação para outras instalações.

11.9.1 Agente de sincronização anti-spam

Como funciona

O Anti-Spam Synchronization Agent funciona da seguinte forma:

1. Uma máquina de servidor que hospeda o GFI MailEssentials é configurada como o servidor mestre.

2. As outras máquinas de servidor nas quais o GFI MailEssentials está instalado, são configuradas como servidores secundários.

3. Os servidores secundários carregam um arquivo contendo configurações para uma pasta virtual IIS hospedada no servidor mestre por meio do serviço Microsoft® BITS.

4. Quando o servidor mestre coleta todos os dados dos servidores secundários, os dados são extraídos de arquivos individuais e mesclados em um único arquivo central.

5. Os servidores secundários baixam esse arquivo central, o extraem e atualizam a instalação local do GFI MailEssentials para utilizar as novas configurações.

> **OBS.**
>
> 1. Os servidores que colaboram na sincronização de configurações devem usar a mesma versão do GFI MailEssentials.
>
> 2. Os arquivos carregados e obtidos por download pelo agente de sincronização são compactados para limitar o tráfego na rede.
>
> 3. Quando a sincronização falha por 3 vezes consecutivas, o GFI MailEssentials notifica o administrador através de um email.
>
> 4. Configurações para a segurança de email e mecanismos de filtragem de conteúdo não são sincronizados pelo agente.

Etapa 1: Configurar o diretório virtual do agente de sincronização no servidor mestre

Observações importantes

1. Apenas um servidor pode ser configurado como servidor mestre de cada vez.

2. Um diretório virtual IIS deve ser criado apenas no servidor mestre.

3. Para configurar um servidor mestre, ele deve atender a uma das seguintes configurações do sistema:

Sistema operacional	IIS	Serviço de transferência inteligente de plano de fundo (BITS)
Microsoft®Windows Server 2012	Obrigatório	Obrigatório Habilita o serviço de transferência inteligente de plano de fundo (BITS) do assistente **Add Roles and Features** do gerenciador de servidor.
Microsoft®Windows Server 2008 com SP1 ou posterior	Obrigatório	Obrigatório Para mais informações sobre como instalar o BITS consulte http://go.gfi.com/?pageid=ME_InstallBITS2008
Microsoft®Windows Server 2003 com SP1 ou posterior	Obrigatório	Obrigatório Para mais informações sobre como instalar o BITS consulte http://go.gfi.com/?pageid=ME_InstallBITS2003

Configuração do diretório virtual

No Gerenciador dos Serviços de Informações da Internet (IIS), configure um diretório virtual compartilhado no site padrão do servidor mestre, como descrito abaixo.

IIS 7.0

a. Carregue o console **Internet Information Services (IIS) Manager**, clique com o botão direito do mouse no site padrão e selecione **Add Virtual Directory**.

b. No diálogo **Add Virtual Directory**, digite `MESynchAgent` como um alias do diretório virtual.

c. Especifique um caminho no qual armazenar o conteúdo desse diretório virtual e clique em **OK** para adicionar o diretório virtual.

> **OBS.**
> Anote o caminho configurado para referência.

d. Selecione o diretório virtual **MESynchAgent** e na visualização Features, clique duas vezes em **SSL Settings**.

e. Desative a caixa de texto **Require SSL** e clique em **Apply**.

f. Retorne para a visualização Features do diretório virtual adicionado e clique duas vezes em **Authentication**.

g. Certifique-se de que somente a opção **Basic Authentication** esteja ativada.

h. Clique com o botão direito do mouse em **Basic Authentication** e clique em **Edit...** para especificar o **Default Domain** e **Realm** do nome do usuário e da senha usados para autenticação pelas máquinas escravas. Clique em **OK** e em **Apply**.

i. Retorne para a visualização Features do diretório virtual **MESynchAgent** e clique duas vezes em **BITS Uploads**.

j. Selecione **Allow clients to upload files** e selecione **Use default settings from parent**. Clique em **Apply**.

IIS 6.0

a. No console **Internet Information Services (IIS) Manager**, clique com o botão direito do mouse no site padrão e selecione **New > Virtual Directory**.

b. No **Virtual Directory Creation Wizard**, digite `MESynchAgent` como um alias do diretório virtual e clique em **Next**.

c. Especifique um caminho no qual armazenar o conteúdo desse diretório virtual e clique em **Next**.

> **OBS.**
> Anote o caminho configurado para referência.

d. Selecione as caixas de texto **Read** e **Write** e desmarque todas as outras caixas de texto. Clique em **Next** e **Finish**.

e. Clique com o botão direito do mouse no diretório virtual **MESynchAgent** e selecione **Properties**.

f. Selecione a guia **Directory Security** e no grupo **Authentication and access control** clique em **Edit**.

g. No grupo **Authenticated access**, marque **Basic Authentication** e especifique **Default domain** e **Realm** do nome de usuário e da senha usados para a autenticação pelas máquinas escravas.

OBS.
Certifique-se de que todas as outras caixas de texto estejam desmarcadas.

h. Clique em **OK**.

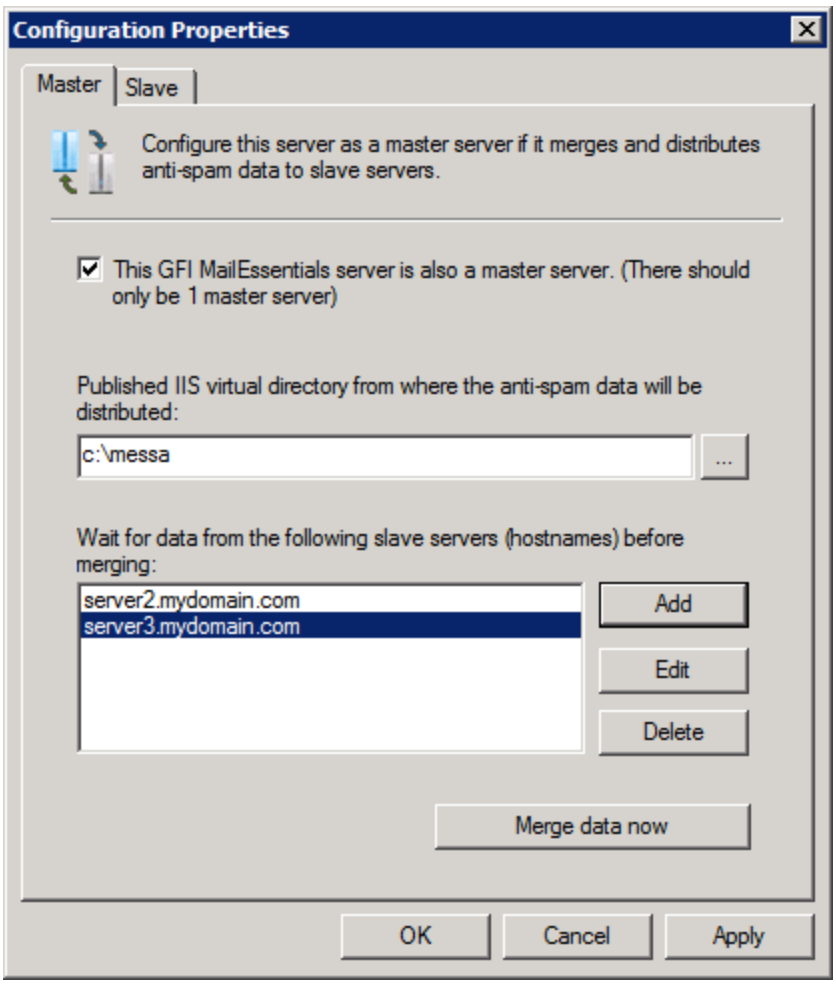
i. Selecione a guia **BITS Server Extension** e selecione **Allow clients to transfer data to this virtual directory**.

j. Clique em **OK** para fechar as propriedades do diálogo do diretório virtual.

Etapa 2: Configurar o servidor mestre doGFI MailEssentials

1. No servidor mestre, acesse <*GFI MailEssentials installation path*>\GFI\MailEssentials\`AntiSpam\` e abra **mesentcfg.msc**.

2. Clique com o botão direito do mouse em **Synchronization Agent > Configuration** e selecione **Properties**.



Screenshot 142: Configurar um servidor mestre

3. Na guia **Master**, selecione **This GFI MailEssentials Configuration server is also a master server** e digite o caminho completo da pasta configurada para armazenar o conteúdo do diretório virtual **MESynchAgent**.

4. Clique em **Add** e digite o nome de host do servidor escravo. Clique em **OK** para adicioná-lo à lista. Repita esta etapa e adicione todos os outros servidores escravos.

OBS.
Certifique-se de configurar todas as máquinas nesta lista como servidores escravos. Caso contrário, o agente de sincronização no servidor mestre não mesclará os dados.

OBS.
Um servidor mestre também pode ser um servidor escravo. Nesse caso, o servidor mesclará seus próprios dados aos dados carregados por outros servidores escravos. Para isso funcionar, também é necessário adicionar o nome de host do servidor mestre à lista de servidores escravos.

5. Se necessário, selecione um servidor escravo na lista e clique em **Edit** ou **Delete** para editá-lo ou excluí-lo.

6. Clique em **OK**.

Etapa 3: Configurar servidores escravos

Observações importantes

1. Para configurar um servidor como escravo, ele deve atender a uma das seguintes especificações do sistema:

» Microsoft® Windows Server 2008

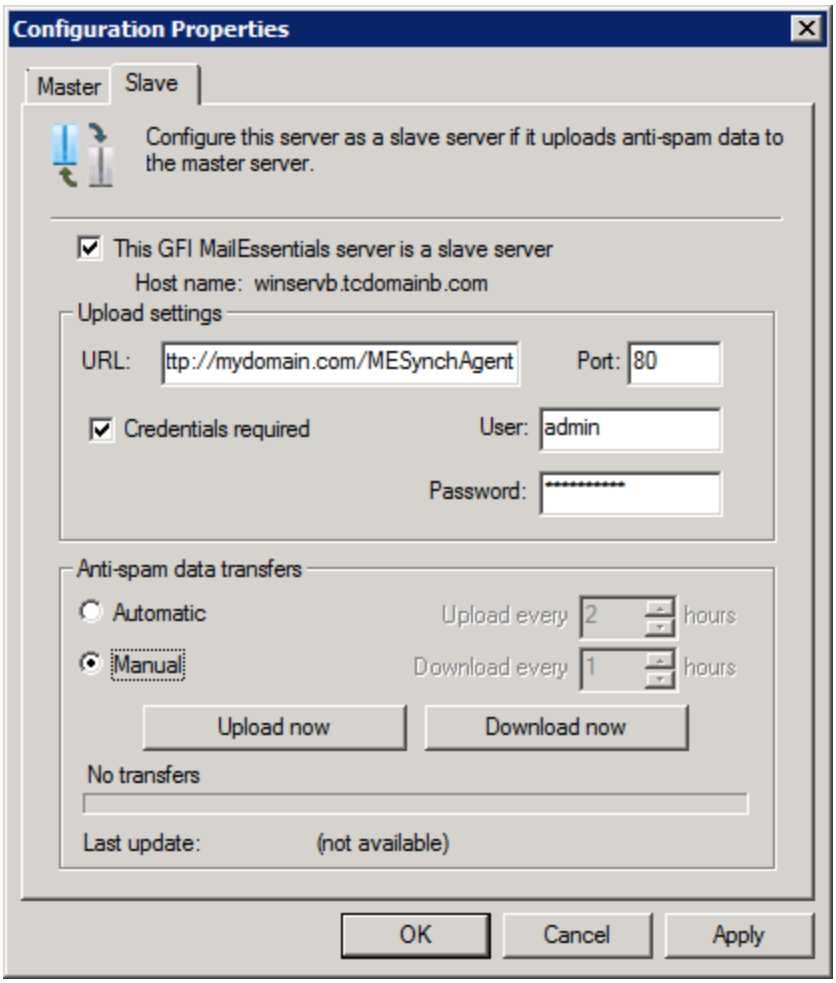
» Microsoft® Windows Server 2003 – É recomendável que você faça o download da atualização do cliente BITS 2.0 a partir de: http://go.gfi.com/?pageid=ME_BITS2003Update

2. Os servidores escravos carregam automaticamente um arquivo compactado que contém configurações do diretório virtual do IIS no servidor mestre. Portanto, nenhum diretório virtual deverá ser criado em servidores escravos.

Configuração do servidor escravo

1. No servidor secundário, acesse *<GFI MailEssentials installation path>*\GFI\MailEssentials\AntiSpam\ e abra **mesentcfg.msc**.

2. Clique com o botão direito do mouse no nó **Anti-Spam Synchronization Agent > Configuration** e selecione **Properties**.



Screenshot 143: Configurar o servidor escravo

3. Na guia **Slave**, selecione **This GFI MailEssentials server is a slave server**.

4. No campo URL, especifique o URL completo do diretório virtual hospedado no servidor mestre no seguinte formato:

`http://<master server domain name>/MESynchAgent`

» Exemplo: `http://mydomain.com/MESynchAgent`

5. No campo **Port**, especifique a porta usada pelo servidor mestre para aceitar comunicações HTTP.

> **OBS.**
> Por padrão, o valor da porta é **80**, que é a porta padrão usada pelo HTTP.

6. Selecione **Credentials required** e digite as credenciais utilizadas para a autenticação em um servidor mestre.

7. Selecione:

Opção	Descrição
Automático	A sincronização ocorre automaticamente em um determinado intervalo. No campo **Upload every**, especifique o intervalo de carregamento em horas que determina com que frequência o servidor escravo carregará as configurações no servidor mestre. No campo **Download every**, especifique o intervalo de download em horas que determina com que frequência o servidor escravo verifica atualizações no servidor mestre e faz o download dessas atualizações. Observações importantes sobre a configuração do intervalo: » O intervalo de hora em hora para carregamento e download não pode ser definido para o mesmo valor. » O intervalo de hora em hora poderá ser definido com um valor entre 1 e 240 horas. » É recomendado que o intervalo de download seja configurado para um valor menor que o do intervalo de carregamento. » Também é recomendado usar o mesmo intervalo para todos os servidores escravos. Exemplo: Defina o intervalo de download para 3 horas e o intervalo de carregamento para 4 horas. Dessa forma, os downloads são mais frequentes que os carregamentos.
Manual	Carregue e faça o download do arquivo compactado de configurações manualmente. Para carregar as configurações do servidor escravo no servidor mestre, clique em **Upload now**. Para fazer o download das configurações mescladas atualizadas do servidor mestre, clique em **Download now**.

8. Clique em **OK**.

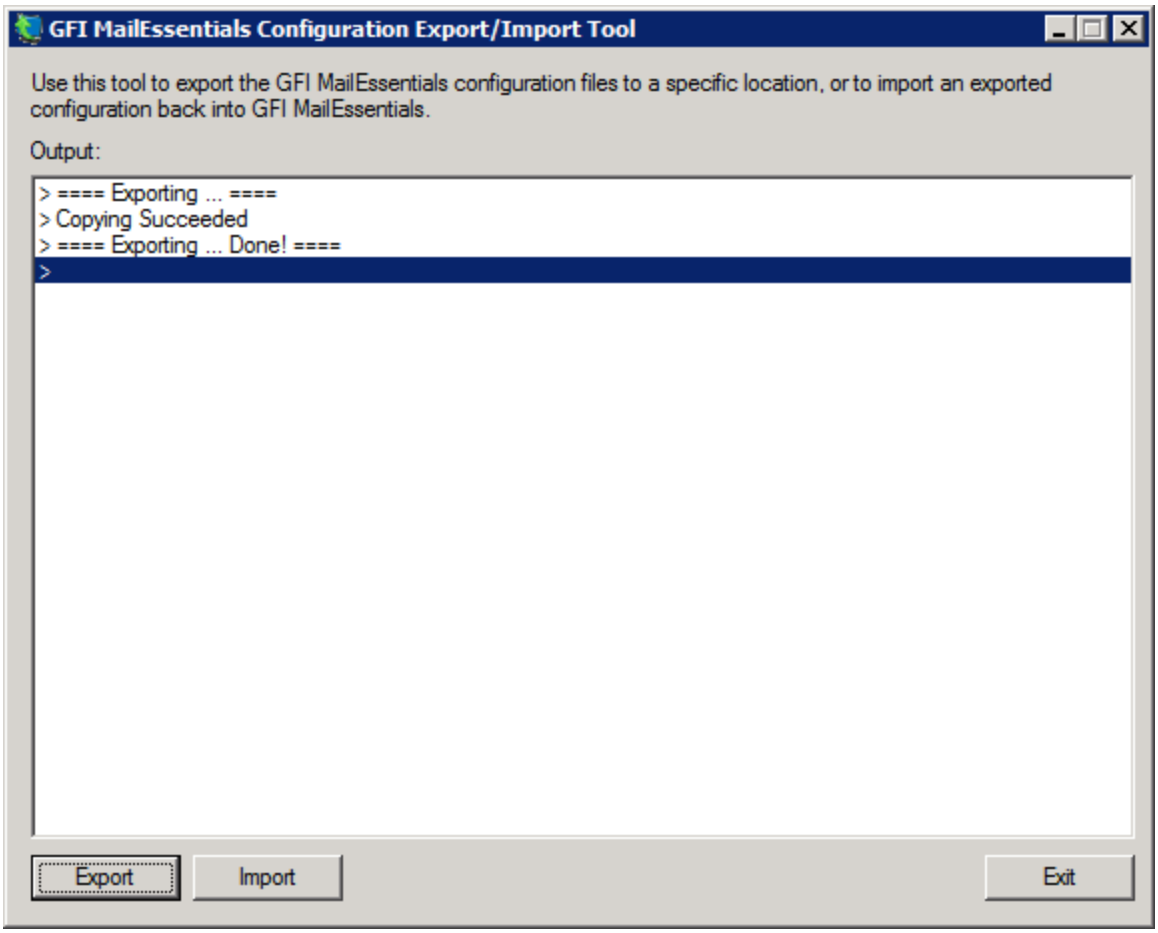
11.9.2 Exportar e importar configurações manualmente

O GFI MailEssentials inclui uma ferramenta Configuration Export/Import para exportar configurações de uma instalação e importá-los em outra instalação.

> **OBS.**
> As configurações podem também ser importadas e/ou exportadas da linha de comando. Para obter mais informações, consulte Exportar/importar configurações via linha de comando (página 274).

Etapa 1: Exportar configurações existentes

1. Acesse *<GFI MailEssentials installation path>*\GFI\MailEssentials\ e inicie **meconfigmgr.exe**.



Screenshot 144: Ferramenta Exportar/importar configuração

> **OBS.**
> A duração dos processos de exportação depende dos tamanhos dos bancos de dados.

4. Clique em **Export**.

5. No diálogo **Browse for Folder**, escolha uma pasta para onde exportar as configurações e clique em **OK**.

6. Quando terminar, clique em **Exit**.

Etapa 2: Copiar as configurações exportadas

1. Copie manualmente a pasta de onde as definições de configuração foram exportadas.

2. Cole a pasta nas máquinas para onde importar as configurações.

Etapa 3: Importar configurações para uma nova instalação

> **IMPORTANTE**
> Ao importar configurações, os arquivos importados substituem as configurações existentes (por exemplo, as configurações do Source DNS) e podem exigir a reconfiguração de determinadas configurações de rede e ações de spam.

OBS.
Alguns serviços são temporariamente interrompidos quando esta operação é executada. Isso pode afetar o fluxo de emails e/ou a verificação de emails.

1. Interrompa os seguintes serviços:

- GFI List Server
- GFI MailEssentials AS Scan Engine
- GFI MailEssentials Attendant
- GFI MailEssentials Autoupdater
- GFI MailEssentials AV Scan Engine
- GFI MailEssentials Backend
- GFI MailEssentials Enterprise Transfer
- GFI MailEssentials Legacy Attendant
- GFI MailEssentials Quarantine Action Services
- GFI POP2Exchange
- IIS Admin service

2. Acesse *<GFI MailEssentials installation path>*\GFI\MailEssentials\ e inicie **meconfigmgr.exe**.

OBS.
A duração do processo de importação depende do tamanho dos bancos de dados a serem importados.

4. Clique em **Importar**, escolha a pasta que contém os dados a serem importados e clique em **OK**.

AVISO
O processo de importação substitui os arquivos de configuração pelos arquivos encontrados nesta pasta.

OBS.

Algumas configurações importadas podem não ser apropriadas para a instalação do GFI MailEssentials e talvez precisem ser redefinidas. Por exemplo, a configuração do DNS, da lista de domínios e dos servidores de perímetro pode ser diferente do servidor do qual as configurações foram exportadas. Clique em **Yes** para iniciar o Post-Installation wizard do GFI MailEssentials para redefinir configurações importantes.

Para obter mais informações, consulte Assistente pós-instalação (página 45).

Também é recomendável verificar as configurações a seguir, que não são definidas durante a execução do Post-Installation wizard.

» **Directory Harvesting**: deve ser verificada durante a importação para um servidor que se conecte a um Active Directory diferente ou um Active Directory localizado em um servidor diferente. Para obter mais informações, consulte Coleta de diretório (página 115).

» **Spam Actions**: algumas ações de spam estão disponíveis apenas para os ambientes Microsoft® Exchange. Se você importar configurações para um ambiente diferente (por exemplo, um Servidor IIS), as ações não funcionarão. Para obter mais informações, consulte Ações de spam - O que fazer com emails de spam (página 148).

OBS.

Para obter mais informações sobre as configurações a serem verificadas após a importação, consulte:

http://go.gfi.com/?pageid=ME_CheckImportSettings

6. Quando terminar, clique em **Sair**.

7. GFI MailEssentials tente iniciar automaticamente os serviços que foram interrompidos na etapa 1.

IMPORTANTE

Outros serviços poderão ser interrompidos ao interromper o **IIS Admin service**, como o serviço **SMTP (Simple Mail Transfer Protocol)**. Reinicie esses serviços manualmente no miniaplicativo Services.

11.9.3 Exportar/importar configurações via linha de comando

Exportar configurações via linha de comando

1. No prompt de comando, altere o diretório para a pasta-raiz de instalação do GFI MailEssentials.

2. Chave:

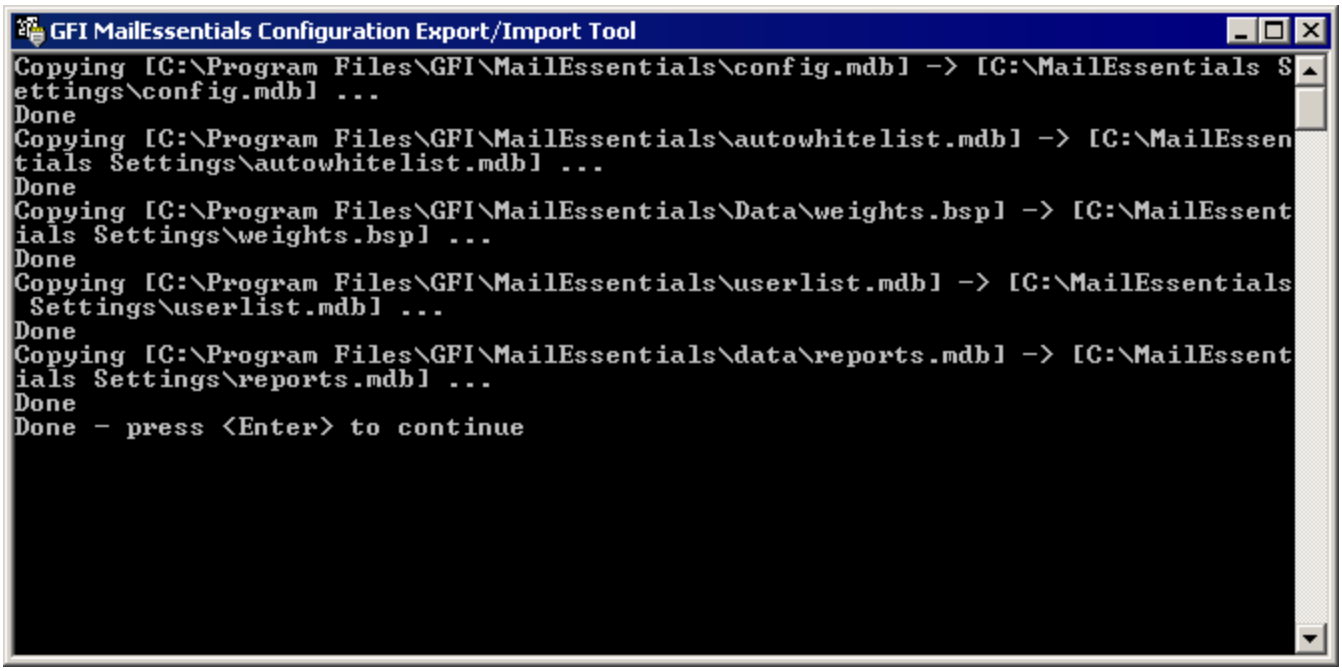
```
meconfigmgr /export:”c:\MailEssentials Settings” /verbose /replace
```

Onde:

» `"C:\MailEssentials Settings"` - o local para onde exportar os arquivos. Substitua pelo caminho de destino desejado.

» `/verbose` - instrui a ferramenta a exibir o progresso ao copiar arquivos.

» `/replace` - instrui a ferramenta a substituir os arquivos existentes na pasta de destino.



Screenshot 145: Exportar configurações via linha de comando

3. Reinicie os serviços interrompidos na etapa 1.

Importar configurações via linha de comando

1. Interrompa os seguintes serviços:

- GFI List Server
- GFI MailEssentials AS Scan Engine
- GFI MailEssentials Attendant
- GFI MailEssentials Autoupdater
- GFI MailEssentials AV Scan Engine
- GFI MailEssentials Backend
- GFI MailEssentials Enterprise Transfer
- GFI MailEssentials Legacy Attendant
- GFI MailEssentials Quarantine Action Services
- GFI POP2Exchange
- IIS Admin service

2. No prompt de comando, altere o diretório para a pasta-raiz de instalação GFI MailEssentials.

3. Digite:

```
meconfigmgr /import:”c:\MailEssentials Settings” /verbose /replace
```

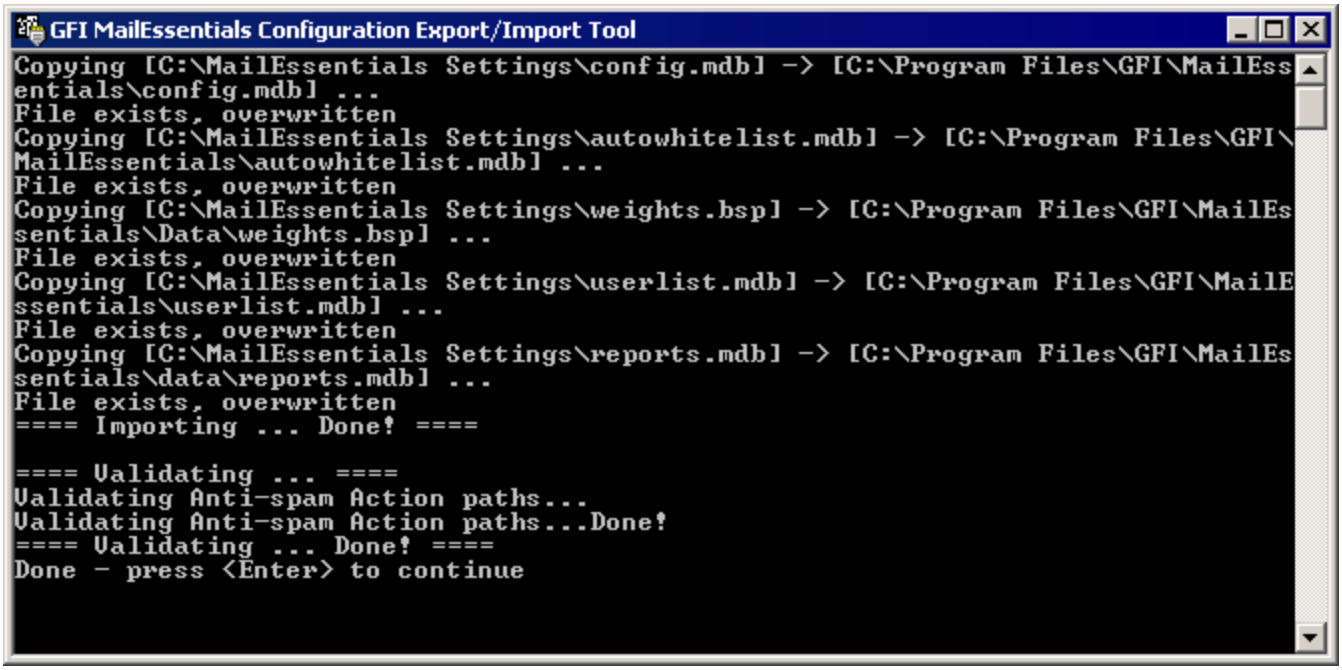
Onde:

- `"C:\MailEssentials Settings"` - local onde os arquivos a serem importados estão localizados. Substitua pelo caminho onde os arquivos a serem importadas estão localizados.

» `/verbose` - instrui a ferramenta a exibir o progresso ao copiar arquivos.

» `/replace` - instrui a ferramenta a substituir os arquivos existentes na pasta de destino.

AVISO
O processo de importação substitui os arquivos de configuração pelos arquivos encontrados nesta pasta.



Screenshot 146: Importar configurações via linha de comando

4. Reinicie os serviços interrompidos na etapa 1.

OBS.
Algumas configurações importadas podem não ser apropriadas para a instalação do GFI MailEssentials e talvez precisem ser redefinidas. Por exemplo, a configuração do DNS, da lista de domínios e dos servidores de perímetro pode ser diferente do servidor do qual as configurações foram exportadas. Clique em **Yes** para iniciar o Post-Installation wizard do GFI MailEssentials para redefinir configurações importantes.

Para obter mais informações, consulte Assistente pós-instalação (página 45).

Também é recomendável verificar as configurações a seguir, que não são definidas durante a execução do Post-Installation wizard.

» **Directory Harvesting**: deve ser verificada durante a importação para um servidor que se conecte a um Active Directory diferente ou um Active Directory localizado em um servidor diferente. Para obter mais informações, consulte Coleta de diretório (página 115).

» **Spam Actions**: algumas ações de spam estão disponíveis apenas para os ambientes Microsoft® Exchange. Se você importar configurações para um ambiente diferente (por exemplo, um Servidor IIS), as ações não funcionarão. Para obter mais informações, consulte Ações de spam - O que fazer com emails de spam (página 148).

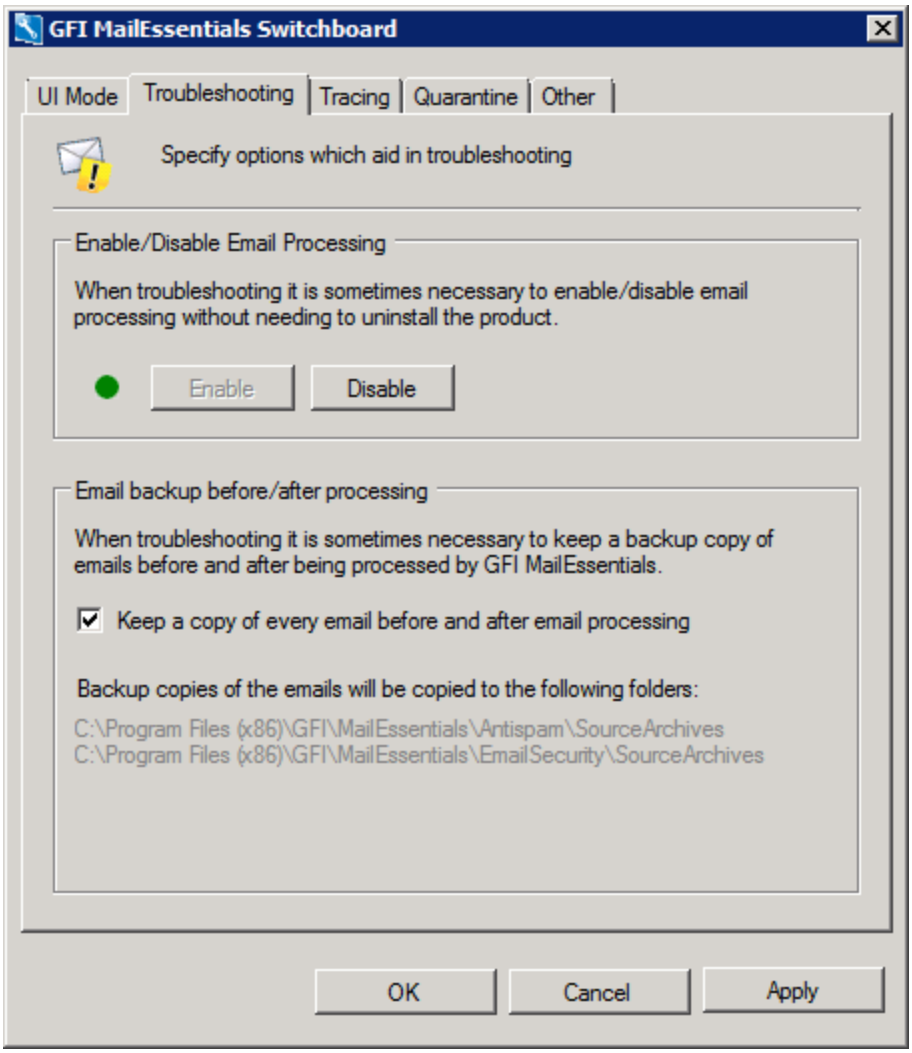
OBS.
Para obter mais informações sobre as configurações para verificar após a importação, consulte: http://go.gfi.com/?pageid=ME_CheckImportSettings

11.10 Desabilitar o processamento de email

O desativamento do processamento de email desativa todas as proteções oferecidas pelo GFI MailEssentials e permite que todos os emails (incluindo spam e emails mal-intencionados) acessem as caixas de correio do usuário. Geralmente, o processamento de email só é desabilitado para solucionar problemas.

Para ativar/desativar o processamento de emails no GFI MailEssentials:

1. Inicie o GFI MailEssentials Switchboard em **Iniciar > Programas > GFI MailEssentials > Switchboard** e selecione a guia **Troubleshooting**.



Screenshot 147: O GFI MailEssentials Switchboard: Solução de problemas

2. Clique em **Enable** ou **Disabled** para habilitar ou desabilitar o processamento de email

OBS.
Alguns serviços são temporariamente interrompidos quando esta operação é executada. Isso pode afetar o fluxo de emails e/ou a verificação de emails.

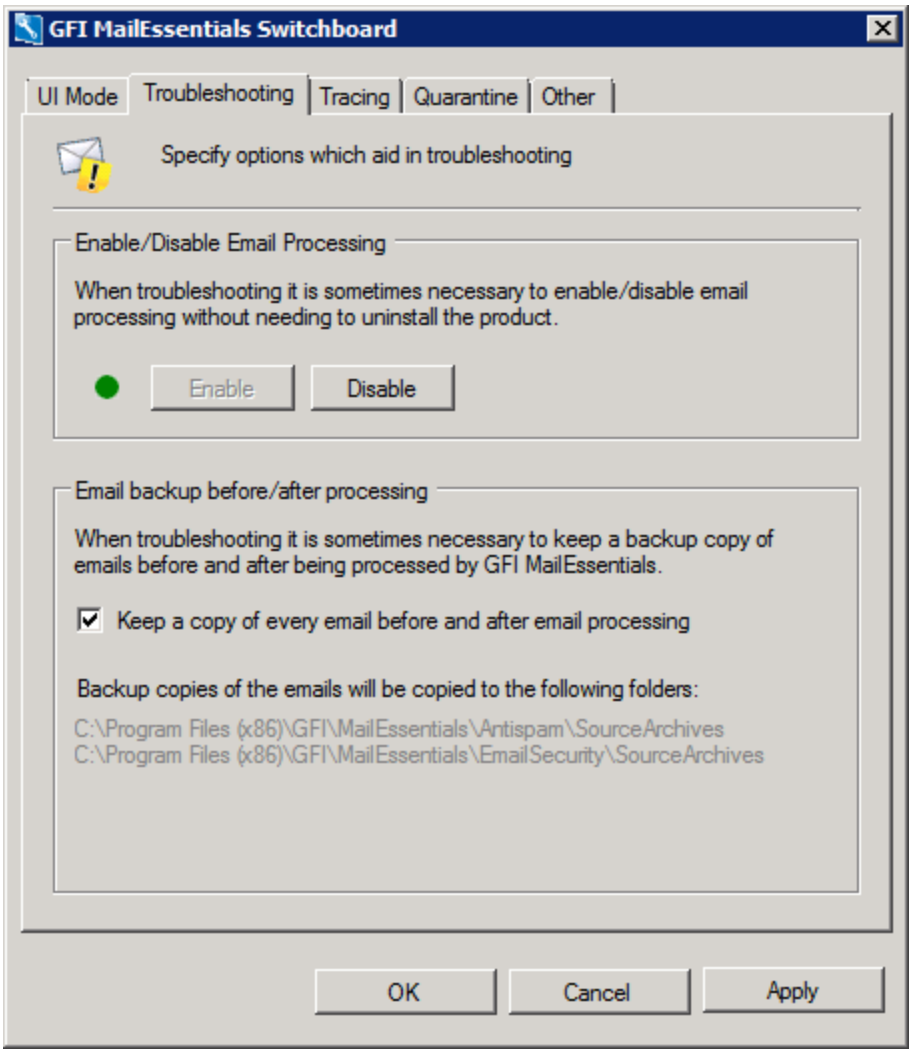
3. No diálogo **Service Restart Required**, clique em **Yes** para reiniciar os serviços.

4. Clique em **OK**.

11.11 Backup de email antes e depois do processamento

IMPORTANTE
Use esta opção somente para solucionar problemas.

1. Inicie o GFI MailEssentials Switchboardem **Iniciar > Programas > GFI MailEssentials > Switchboard** e selecione a guia **Solução de problemas** .



Screenshot 148: O GFI MailEssentials Switchboard: Solução de problemas

2. Marque/desmarque a caixa de seleção **Keep a copy of every email before and after email processing** para armazenar uma cópia de cada email processado.

Todos os emails são armazenados nos seguintes locais:

» *<GFI MailEssentials installation path>*\GFI\MailEssentials\AntiSpam\SourceArchives\

» *<GFI MailEssentials installation path>*\GFI\MailEssentials\EmailSecurity\SourceArchives\

> **OBS.**
> Alguns serviços são temporariamente interrompidos quando esta operação é executada. Isso pode afetar o fluxo de emails e/ou a verificação de emails.

3. Clique em **OK**.

4. No diálogo **Service Restart Required**, clique em **Yes** para reiniciar os serviços.

5. Clique em **OK**.

11.12 Portas remotas

Portas remotas permitem que módulos no GFI MailEssentials se comuniquem uns com os outros. Por padrão, o GFI MailEssentials usa as portas:

» **9090** – usado pelo serviço de back-end do GFI MailEssentials

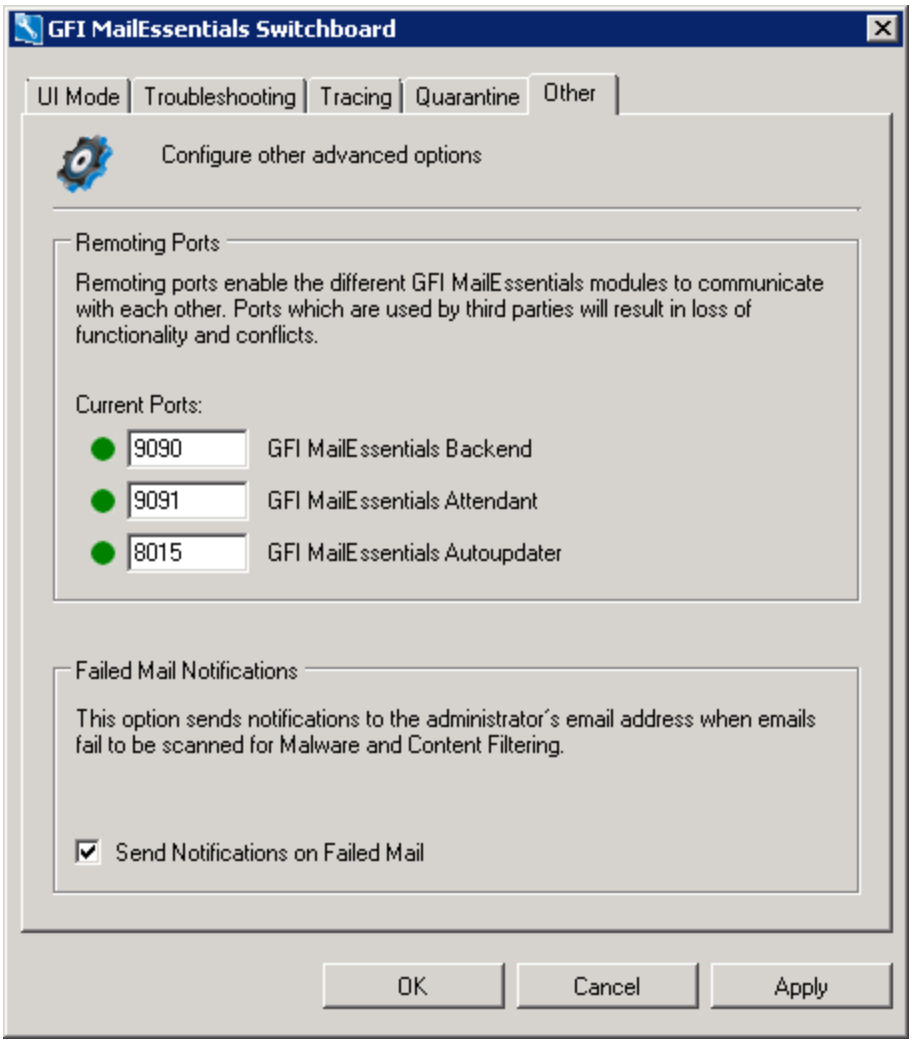
» **9091** – usado pelo serviço de atendedor do GFI MailEssentials

» **9091** – usado pelo serviço AutoUpdater do GFI MailEssentials

Verifique se não há outros aplicativos (exceto GFI MailEssentials) escutando nessas portas. Se essas portas forem usadas por outro aplicativo, altere o número dessas portas para portas que não são usadas por outros aplicativos.

Para alterar as portas remotas:

1. Inicie o GFI MailEssentials Switchboardem **Iniciar > Programas > GFI MailEssentials > Switchboard** e selecione a guia **Outros**.



Screenshot 149: Alterar as portas remotas

2. Na área **Remoting Ports**, altere o número da porta remota que uma porta que não seja usada por outros aplicativos.

3. Clique em **Apply**.

> **OBS.**
> Alguns serviços são temporariamente interrompidos quando esta operação é executada. Isso pode afetar o fluxo de emails e/ou a verificação de emails.

4. Clique em **Yes** para reiniciar os serviços exibidos.

5. Clique em **OK**.

11.13 Monitorar a API de verificação de vírus

Quando o GFI MailEssentials estiver instalado em uma máquina com o Microsoft® Exchange, você poderá monitorar API de Verificação de Vírus usando o MMC do Monitor de Desempenho.

OBS.
O Information Store Protection (VSAPI) não é compatível com o Microsoft® Exchange Server 2013 porque o VSAPI foi removido do Microsoft® Exchange Server 2013.

11.13.1 Contador de desempenho no Windows 2003 Server

Para adicionar e exibir o contador do monitor de desempenho do Windows 2003 Server, siga estas etapas:

1. Acesse **Iniciar > Painel de Controle**.

2. Na janela Painel de Controle, clique duas vezes em **Ferramentas Administrativas**.

3. Clique duas vezes em **Desempenho** para iniciar o MMC do **Monitor de Desempenho**.

4. No painel de visualização **Monitor do sistema**, clique em **Adicionar** para carregar o diálogo **Adicionar Contador**.

5. Na lista suspensa **Objeto de desempenho**, selecione **MSExchangeIS**.

6. Clique em **Selecione contadores da lista**.

7. Selecione qualquer contador **Virus Scan** que você precise adicionar. Para obter mais informações, consulte Contadores do Monitor de Desempenho (página 283).

8. Clique em **Add**.

9. Repita as etapas 7 e 8 para adicionar todos os contadores de desempenho necessários.

10. Clique em **Close**.

Os contadores de processos adicionados agora são exibidos no Monitor de desempenho.

11.13.2 Contador de desempenho no Windows 2008 Server

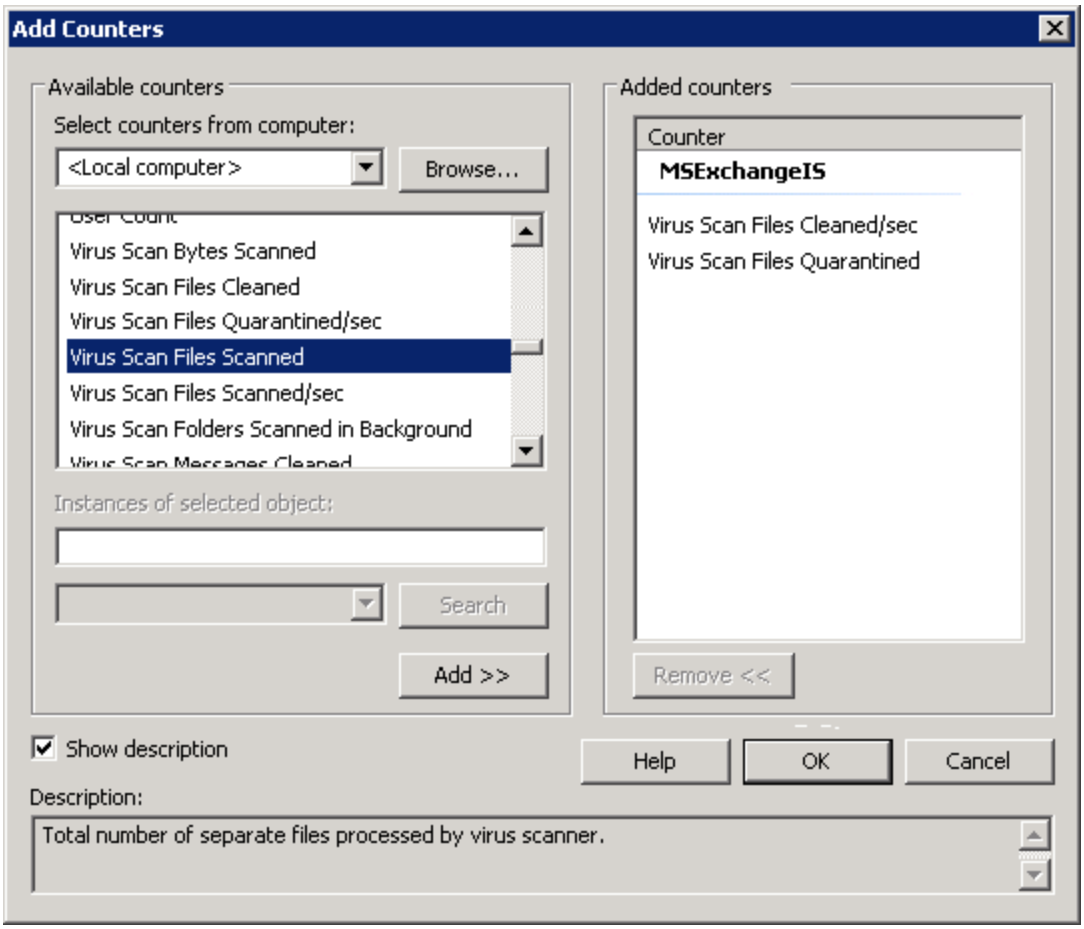
OBS.
Em um ambiente do Microsoft® Exchange Server 2007/2010, os contadores do monitor de desempenho VSAPO estão disponíveis apenas em máquinas com função de servidor Caixa de Correio instalada.

Para adicionar e exibir o contador do monitor de desempenho do Windows 2008 Server, siga estas etapas:

1. Acesse **Iniciar > Painel de Controle > Ferramentas Administrativas > Monitor de Confiabilidade e desempenho**.

2. No diálogo do monitor, expanda **Ferramentas de Monitoramento** e selecione **Monitor de Desempenho**.

3. No painel de visualização, clique em **Adicionar** para carregar a caixa de diálogo **Adicionar contadores**.



Screenshot 150: Adicionar contadores do monitor de desempenho VSAPI no Windows 2008 Server

4. Na lista suspensa **Select counters from computer**, selecione o computador a ser monitorado.

5. Na lista de contadores disponíveis, expanda **MSExchangeIS**.

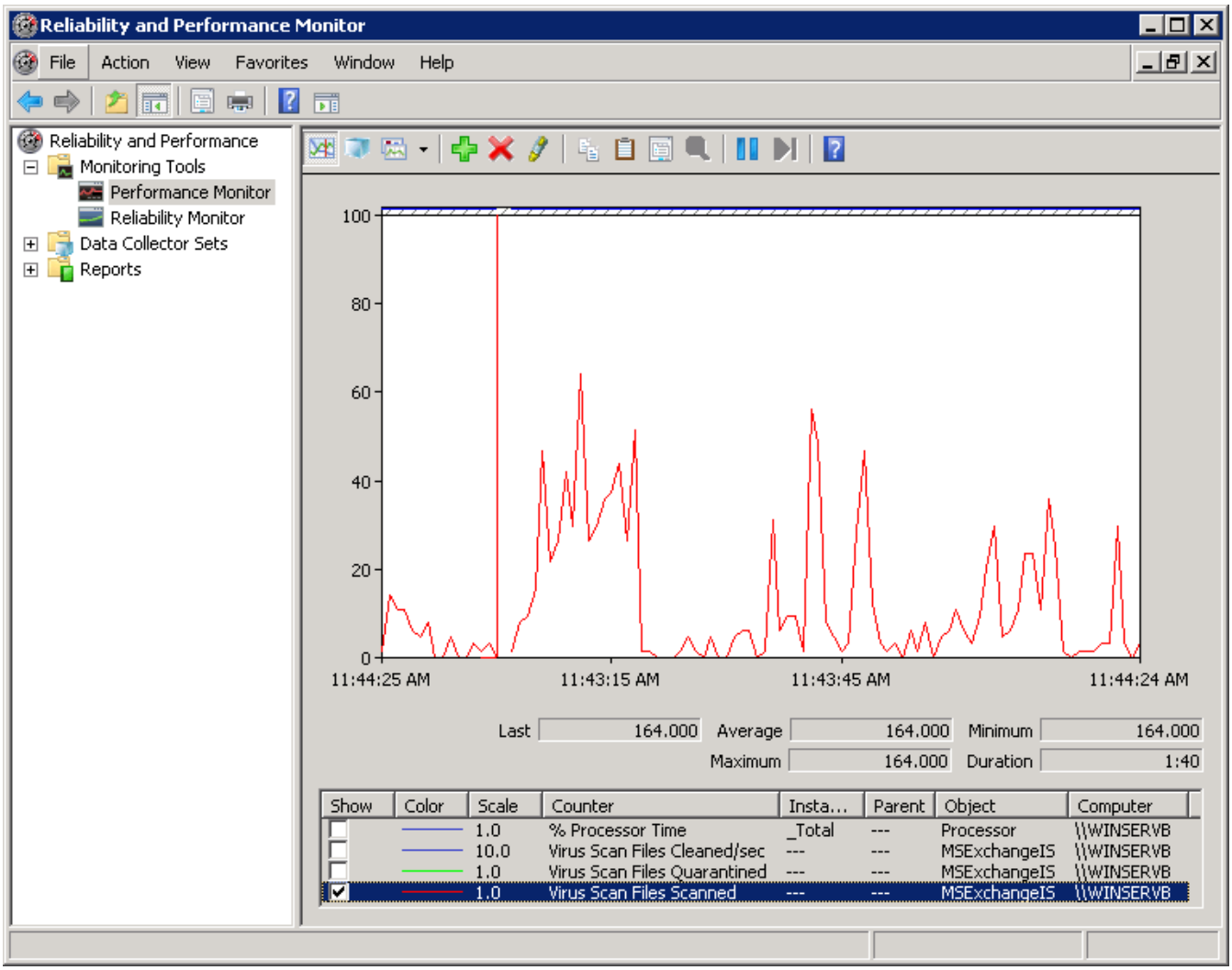
6. Selecione qualquer contador **Virus Scan** que você precise adicionar. Para obter mais informações, consulte Contadores do Monitor de Desempenho (página 283).

7. Clique em **Add**.

8. Repita as etapas 6 e 7 para cada processo a ser monitorado.

9. Clique em **OK** para aplicar as alterações.

Os contadores de processos adicionados agora são exibidos no Monitor de desempenho.



Screenshot 151: Monitorar arquivos de verificação de vírus verificados no Monitor de Desempenho do Windows Server 2008

11.13.3 Contadores do Monitor de Desempenho

Os seguintes contadores do Monitor de desempenho VSAPI estão disponíveis:

Contador de Desempenho	Descrição
Mensagens de Verificação de Vírus Processadas	Um valor acumulativo do número total de mensagens de nível superior processadas pelo verificador de vírus.
Mensagens de Verificação de Vírus Processadas/s	Representa a velocidade na qual mensagens de nível superior são processadas pelo verificador de vírus.
Mensagens de Verificação de Vírus Eliminadas	Número total de mensagens de nível superior eliminadas pelo verificador de vírus.
Mensagens de Verificação de Vírus Eliminadas/s	Velocidade na qual mensagens de nível superior são eliminadas pelo verificador de vírus.
Mensagens de Verificação de Vírus em Quarentena	Número total de mensagens de nível superior colocadas em quarentena pelo verificador de vírus.
Mensagens de Verificação de Vírus em Quarentena/s	Velocidade na qual mensagens de nível superior são colocadas em quarentena pelo verificador de vírus.
Arquivos de Verificação de Vírus Verificados	Número total de arquivos separados processados pelo verificador de vírus.

Contador de Desempenho	Descrição
Arquivos de Verificação de Vírus Verificados/s	Velocidade na qual arquivos separados são processados pelo verificador de vírus.
Arquivos de Verificação de Vírus Eliminados	Número total de arquivos separados eliminados pelo verificador de vírus.
Arquivos de Verificação de Vírus Eliminados/s	Velocidade na qual arquivos separados são eliminados pelo mecanismo verificador de vírus.
Arquivos de Verificação de Vírus em Quarentena	Número total de arquivos separados colocados em quarentena pelo verificador de vírus.
Arquivos de Verificação de Vírus em Quarentena/s	Velocidade na qual os arquivos separados são colocados em quarentena pelo verificador de vírus.
Bytes de Verificação de Vírus Verificados	Número total de bytes em todos os arquivos processados pelo verificador de vírus.
Comprimento da Fila de Verificação de Vírus	Número atual de solicitações pendentes na fila para verificação de vírus.
Pastas de Verificação de Vírus Verificadas no Plano de Fundo	Número total de pastas processadas pela verificação em segundo plano.
Mensagens de Verificação de Vírus Verificadas no Plano de Fundo	O número total de mensagens processadas pela verificação em segundo plano.

12 Solução de problemas e suporte

12.1 Introdução

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

- Este manual - a maioria dos problemas pode ser solucionada com as informações nesta seção.
- Artigos do banco de dados de conhecimento da GFI
- Fórum da Web
- Suporte técnico da GFI

12.2 Problemas comuns

Problema encontrado	Solução
O Painel mostra que nenhum e-mail está sendo processado; ou Somente emails de entrada e de saída são processados	1. Certifique-se de que a verificação de emails não esteja desabilitada no GFI MailEssentials. Para obter mais informações, consulte Desabilitar o processamento de email (página 277). 2. Verifique vários servidores virtuais SMTP do Microsoft® IIS e certifique-se de que o GFI MailEssentials esteja conectado ao servidor virtual correto. Para obter mais informações, consulte Associações do servidor virtual SMTP (página 245). 3. O registro MX do domínio não está configurado corretamente. Certifique-se de que o registro MX aponte para o endereço IP do servidor que executa o GFI MailEssentials. 4. Se os emails de entrada estiverem passando por outro gateway, certifique-se de que o servidor de email executado no outro gateway encaminhe os emails de entrada por meio do GFI MailEssentials. 5. Certifique-se de que os emails de saída estejam configuradas para serem roteados por meio do GFI MailEssentials. Para obter mais informações, consulte Instalar em um gateway de email ou servidor de retransmissão/perímetro (página 27). 6. Verifique se o servidor virtual SMTP usado pelo Microsoft® Exchange Server para emails de saída é o mesmo servidor SMTP ao qual o GFI MailEssentials está conectado. Para obter mais informações sobre como resolver esse problema, consulte: http://go.gfi.com/?pageid=ME_MonitorProcessing
Após a instalação do GFI MailEssentials, alguns emails mostram um corpo de mensagem distorcido quando visualizados no Microsoft® Outlook	Esse problema ocorre nos emails que usam um conjunto de caracteres no cabeçalho da mensagem e um conjunto de caracteres diferente no corpo da mensagem. Quando esses emails são processados pelo Microsoft® Exchange 2003, eles aparecem distorcidos no Microsoft® Outlook. A Microsoft® lançou um hotfix para solucionar esse problema. Para obter mais informações, consulte: http://go.gfi.com/?pageid=ME_OutlookCharacters e http://go.gfi.com/?pageid=ME_MessageGarbled

Problema encontrado	Solução
O GFI MailEssentials está configurado para transferir mensagens bloqueadas como SPAM para uma subpasta da caixa de correio dos usuários. Clientes conectados ao Microsoft® Exchange via POP3 não podem exibir mensagens bloqueadas como SPAM.	Conecte-se ao Microsoft® Exchange usando IMAP. Para obter mais informações, consulte: http://go.gfi.com/?pageid=ME_POP3ViewSpam
Atualizações automáticas falham, no entanto, o download manual via GFI MailEssentials configuration funciona	Certifique-se de que conexões não autenticadas sejam permitidas na máquina do GFI MailEssentials para o http://update.gfi.com na porta 80. Para obter mais informações, consulte: http://go.gfi.com/?pageid=ME_AutoUpdatesFail Verifique também o servidor proxy, se aplicável.
Dados de configuração não podem ser importados.	Certifique-se de que a versão e a compilação do GFI MailEssentials sejam idênticas nas instalações de origem e de destino. Para obter mais informações sobre como resolver esse problema, consulte: http://go.gfi.com/?pageid=ME_ExpImpBuild
Comandos remotos não funcionam	Consulte: http://go.gfi.com/?pageid=ME_RemoteCommands
O processamento de emails está muito lento	Isso pode ocorrer quando houver problemas de DNS na rede. Se o DNS não estiver funcionando corretamente, as pesquisas de DNS feitas por alguns filtros anti-spam no GFI MailEssentials expirarão. Para obter mais informações, consulte: http://go.gfi.com/?pageid=ME_ProcessingSlow
Dados antigos não estão disponíveis no banco de dados ao usar o Microsoft® Access.	Quando o banco de dados **reports.mdb** exceder 1.7 GB, o banco de dados será automaticamente renomeado para **reports_<data>.mdb** e um novo banco de dados **reports.mdb** será criado. Para obter mais informações sobre como resolver esse problema, consulte: http://go.gfi.com/?pageid=ME_ReportDB
A interface de quarentena mostra o erro D10:**Cannot access the Quarantine Store database. Use uma ferramenta de reparo de banco de dados (como esentutl.exe) para reparar o banco de dados.**	Consulte o http://go.gfi.com/?pageid=ME_esentutl para obter mais informações sobre como usar esentutl.exe para reparar o banco de dados do armazenamento de quarentena.
Erro ao receber emails: **Body type not supported by Remote Host**	Este erro ocorre quando emails são retransmitidos do servidor SMTP do IIS para o servidor Microsoft® Exchange. Isso ocorre porque as versões 4.0, 5.0 e 5.5 do Microsoft® Exchange Server não são compatíveis com mensagens MIME de 8 bits. Para obter instruções sobre como desativar 8BITMIME no Windows Server 2003, consulte: http://go.gfi.com/?pageid=ME_TurnOff8bitMIME.

Problema encontrado	Solução
Emails legítimos são movidos para a pasta **failedmails**	**Causa** Quando o GFI MailEssentials não puder verificar emails de entrada, esses emails não são entregues aos destinatários, pois podem ter conteúdo mal-intencionado.GFI MailEssentials move esses emails para a seguinte pasta: <*GFI MailEssentials installation path*>\GFI\MailEssentials\EmailSecurity\failedmails\ **Solução** Se emails legítimos forem movidos para a pasta failedmails, eles poderão ser manualmente reprocessados para a entrega. Para obter mais informações, consulte Emails com falha (página 255). Para obter mais informações sobre emails com falha, consulte: http://go.gfi.com/?pageid=ME_FailedMails
Preciso atualizar minha chave de licença ao atualizar para uma nova versão?	Informações sobre licenciamento estão disponíveis em: http://go.gfi.com/?pageid=ME_adminManualEN
Onde acessar a versão on-line deste manual?	A versão on-line deste manual está disponível em: http://go.gfi.com/?pageid=GFI_Manuals

12.3 Mecanismos de verificação e filtros

Problema encontrado	Solução
Spam é enviado para a caixa de correio dos usuários	Siga a lista de verificação a seguir para resolver o problema. 1. Verifique se a verificação de emails está desabilitada no GFI MailEssentials. Para obter mais informações, consulte Desabilitar o processamento de email (página 277). 2. Verifique se todos os filtros obrigatórios estão habilitados. Para obter mais informações, consulte Filtros anti-spam (página 109). 3. Verifique se os domínios locais estão configurados corretamente. Para obter mais informações, consulte Domínio local (página 243). 4. Verifique se os emails estão passando pelo GFI MailEssentials ou se o GFI MailEssentials está conectado ao servidor virtual SMTP do IIS correto. 5. Verifique se a localização '%TEMP%' (que, por padrão, é a pasta 'C:\Windows\Temp') contém uma grande quantidade de arquivos. 6. Verifique se o número de usuários usando GFI MailEssentials excede o número de licenças adquiridas. 7. Verifique se a lista de permissão está configurada corretamente. Para obter mais informações, consulte Lista de permissão (página 141). 8. Verifique se as ações estão configuradas corretamente. Para obter mais informações, consulte Ações de spam - O que fazer com emails de spam (página 148). 9. Verifique se o filtro da análise bayesiana está configurado corretamente. Para obter mais informações, consulte Análise bayesiana (página 138). Para obter mais informações sobre como resolver esse problema, consulte: http://go.gfi.com/?pageid=ME_SpamChecklist
As páginas Email Blocklist, Whitelist e/ou Content Filtering demoram muito para carregar ou parecem travadas	Limite o número de entradas na lista a 10.000.

Problema encontrado	Solução
O SpamRazer não faz o download de atualizações	1. Certifique-se de que sua chave de licença é válida. 2. Certifique-se de que a portas necessárias estão abertas e que seu firewall está configurado para permitir conexões com o servidor do GFI MailEssentials. Para obter mais informações, consulte Configurações da porta do firewall (página 26). 3. Certifique-se de que, se for o caso, as configurações do servidor proxy para conexão com a Internet estejam corretas.
Emails não estão sendo incluídos na lista de exclusão temporária	Para verificar o funcionamento do filtro Lista de exclusão temporária: **Etapa 1: Confirme se o filtro Lista de exclusão temporária está habilitado** Nas propriedades do filtro Lista de exclusão temporária, certifique-se de que a opção Enable Greylist esteja selecionada. **Etapa 2: Verificar endereços excluídos** Nas exclusões de IP e email nas propriedades da Lista de exclusão temporária, certifique-se de que não há exclusões incorretas (como *@*.com). **Etapa 3: Use esentutl.exe para garantir que o banco de dados da Lista de exclusão temporária não esteja corrompido.** Para obter mais informações, consulte: http://go.gfi.com/?pageid=ME_esentutl
Estou recebendo emails com spam de meu domínio.	Alguns emails com spam contêm um falso endereço de email "SMTP FROM" contendo o mesmo domínio do destinatário. Pode parecer que o email é proveniente de um usuário local. 1. Habilite a Estrutura de políticas do remetente no filtro anti-spam do SpamRazer para bloquear emails originados de endereços falsos. Para obter mais informações, consulte SpamRazer (página 110). 2. Crie um registro SPF para o seu domínio. Para obter mais informações, consulte http://go.gfi.com/?pageid=ME_CreateSPFRecord. 3. Certifique-se de que o SpamRazer está configurado para ser executado com uma prioridade maior que o módulo Whitelist. Para obter mais informações, consulte Classificar filtros anti-spam por prioridade (página 151).
Os emails enviados de remetentes na lista de permissão são bloqueados.	1. Emails na lista de permissão podem ser bloqueados se tiverem conteúdo ou anexos que violem as regras anti-malware, pois essas regras têm ordem de prioridade maior que a lista de permissão. Certifique-se de que os emails bloqueados não violem as regras anti-malware. 2. Certifique-se de que as prioridades do filtro estejam definidas para que a lista esteja acima de qualquer tipo de filtro que esteja bloqueando email legítimos. Para obter mais informações, consulte: http://go.gfi.com/?pageid=ME_BlockedWhitelistedSenders
Spam não entregue a subpasta Microsoft® Exchange ou spam que não está sendo enviado para a subpasta determinada no Outlook em um ambiente do Microsoft® Exchange Server 2010	1. Confirme se esse recurso está configurado corretamente. Para obter mais informações, consulte Transferir spam para a pasta do Exchange 2010 (página 264). 2. Consulte http://go.gfi.com/?pageid=ME_AutodiscoverIssues para obter informações detalhadas sobre como resolver esse problema.

12.4 Gerenciamento de email

Problema encontrado	Solução
Nenhum aviso de isenção de responsabilidade é adicionado a emails de saída	Avisos de isenção de responsabilidade só serão adicionados a emails de saída provenientes de domínios protegido pelo GFI MailEssentials. Avisos de isenção de responsabilidade não serão adicionados quando: » Emails forem enviados de domínios que não estiverem especificados na lista de domínios locais. » Emails forem enviados para os domínios que estejam na lista de domínios locais, pois eles serão considerados emails internos. Certifique-se de que todos os domínios locais estejam especificados no diálogo Inbound email domains. Para obter mais informações, consulte Domínio local (página 243).
Alguns caracteres no texto do aviso de isenção de responsabilidade não são exibidos corretamente	Configure o Microsoft® Outlook para não usar a codificação automática e forçar o GPO a usar a codificação correta. Para obter mais informações sobre como resolver esse problema, consulte: http://go.gfi.com/?pageid=ME_Outlook2003Encoding
Os emails enviados para o servidor da lista são convertidos para texto simples	Os emails enviados para o Servidor de lista são convertidos em mensagens de texto simples apenas quando o formato original do email for RTF. Envie emails em formato HTML para manter o formato original
Usuários internos receberão um relatório de não entrega ao enviar o email para o list server quando o GFI MailEssentials for instalado em uma máquina de gateway	Para obter mais informações sobre como usar o recurso List Server se o GFI MailEssentials estiver instalado em um gateway, consulte: http://go.gfi.com/?pageid=ME_ListServerGateway
Emails enviados por determinados usuários ou enviados para determinados usuários não são monitorados.	Regras de monitoramento de email não monitorar emails enviados do e para o administrador do GFI MailEssentials e o endereço de email ao qual os emails monitorados são enviados. Regras de monitoramento de email também não se aplicam aos emails enviados entre usuários internos com o mesmo armazenamento de informações.

12.5 GFI SkyNet

A GFI mantém um repositório de banco 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/.

12.6 Fórum da Web

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

12.7 Solicitar suporte técnico

Se os recursos aqui mencionados não ajudarem você a resolver seus problemas, contate a equipe de suporte técnico da 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 nesta 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 da GFI em: http://customers.gfi.com.

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

12.8 Documentação

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

13 Apêndice - Filtragem bayesiana

O filtro Bayesian é uma tecnologia anti-spam usada no GFI MailEssentials. É uma técnica adaptativa baseada em algoritmos de inteligência artificial, reforçados para resistir a mais ampla variedade de técnicas de spam disponíveis hoje em dia.

Este capítulo explica como funciona a filtragem bayesiana e como ela pode ser configurada e treinada.

> **OBS.**
> 1. O filtro anti-spam Bayesian fica desativado por padrão. É altamente recomendado que você treine o filtro Bayesiano antes de habilitá-lo.
> 2. GFI MailEssentials deve funcionar por pelo menos uma semana para que o filtro Bayesiano atinja o desempenho ideal. Isso é necessário porque o filtro Bayesiano adquire a taxa de detecção mais alta quando se adapta aos padrões do seu email.

Como o filtro de spam Bayesiano funciona?

A filtragem Bayesiana é baseada no princípio de que a maioria dos eventos é dependente e que a probabilidade que um evento ocorra no futuro pode ser inferida com base nas últimas ocorrências do evento.

> **OBS.**
> Consulte os links abaixo para obter mais informações sobre a base matemática da filtragem bayesiana:
> http://go.gfi.com/?pageid=ME_BayesianParameterEstimation

Esta mesma técnica foi adaptada pelo GFI MailEssentials para identificar e classificar as mensagens de spam. Se um snippet de texto geralmente ocorre em emails de spam, mas não em emails legítimos, seria razoável assumir que o email é spam.

Criar um banco de dados de palavras bayesiano personalizado

Antes que a filtragem bayesiana seja usada, um banco de dados com palavras e itens (por exemplo, um sinal de $, endereços IP e domínios, etc) deve ser criado. Isso pode ser obtido a partir de uma amostra de email de spam e um email válido (denominados "não spam").

A probabilidade de o valor ser atribuído a cada palavra ou dispositivo é baseado em cálculos que levam em consideração a frequência com que essa palavra ocorre em spam em vez de não spam. Isso é feito ao analisar os emails de saída dos usuários e spam conhecidos: Todas as palavras e itens em ambos os conjuntos de email são analisados para gerar a probabilidade de que uma determinada palavra aponte para o email que é spam.

Essa probabilidade é calculada como o seguinte exemplo:

Se a palavra "hipoteca" ocorrer em 400 dos 3.000 emails de spam e em cinco dos 300 emails legítimos, a probabilidade de spam será de 0,8889 (por exemplo, [400/3000] / [5/300 +400/3000]).

Criar um banco de dados de emails não spam personalizado

A análise do email não spam é feita no email da empresa e, portanto, é adequada a uma determinada empresa.

» **Exemplo**: Uma instituição financeira pode usar a palavra "hipoteca" muitas vezes e obter um número excessivo de falsos positivos se estiver usando um conjunto de regras anti-spam gerais. Por outro lado, a filtragem bayesiana, se for adequada à sua empresa por meio de um período de treinamento inicial, leva em consideração emails de saída válidos da empresa e reconhece os emails enviados (e reconhece "hipoteca" como sendo usada em mensagens legítimas), poderá ter uma melhor detecção de spam e uma taxa muito baixa de falsos positivos.

Criar um banco de dados de spam bayesiano

Além de email não spam, o filtro bayesiano também contém um arquivo de dados de spam. Esse arquivo de dados de spam deve incluir um grande número de amostras de spam. Além disso, ele também deve ser constantemente atualizado com os mais recentes spams pelo software anti-spam. Isso garante que o filtro bayesiano reconheça tendências de spam mais recentes, o que resulta em uma alta taxa de detecção de spam.

Como a filtragem bayesiana é feita?

Uma vez que os bancos de dados de não spam e spam foram criados, as probabilidades de palavras podem ser calculadas e o filtro está pronto para o uso.

Na chegada, os novos emails são divididos em palavras e as palavras mais relevantes (aquelas que são mais significativas para identificar se o email é spam ou não) são identificadas. Usando essas palavras, o filtro bayesiano calcula a probabilidade de a mensagem ser um spam. Se a probabilidade for maior que o limite, a mensagem será classificada como spam.

> **OBS.**
> Para obter mais informações sobre a filtragem bayesiana e suas vantagens, consulte:
> http://go.gfi.com/?pageid=ME_Bayesian

Treinar o filtro de análise bayesiana

> **OBS.**
> O filtro de análise bayesiana também pode ser treinado usando pastas públicas. Para obter mais informações, consulte Configurar o filtro bayesiano (página 139).

É recomendável que o filtro de análise bayesiana seja treinado com base no fluxo de email da empresa por um período de tempo. Também é possível que a análise bayesiana seja treinada com base em emails enviados e recebidos, antes que o GFI MailEssentials seja instalado usando o assistente de análise bayesiana. Isso permite que a análise bayesiana seja habilitada imediatamente.

Este assistente analisa fontes de:

» emails legítimos: por exemplo, uma pasta de itens enviados da caixa de correio

» mensagens de spam: por exemplo, uma pasta da caixa de correio dedicada a emails de spam.

Etapa 1: Instalar o assistente de análise bayesiana

O assistente de análise bayesiana pode ser instalado em:

» Uma máquina que se comunica com o Microsoft® Exchange, para analisar os emails em uma caixa de correio

» Uma máquina com o Microsoft Outlook instalado, para analisar os emails no Microsoft Outlook

Para instalar o assistente de análise bayesiana:

1. Copie o arquivo de instalação do **Bayesian Analysis Wizard.exe** para a máquina selecionada. Ele está localizado em: GFI MailEssentials *caminho de instalação\AntiSpam\BSW*

2. Abrir o **Bayesian Analysis Wizard.exe**.

3. Na tela inicial, escolha o idioma e revise o Contrato de licença do usuário final. Clique em **Next**.

4. Selecione a pasta de instalação e clique em **Next**.

5. Clique em **Install** para iniciar a instalação.

6. Clique em **Finish** quando a instalação for concluída.

Etapa 2: Analisar emails legítimos e emails com spam

Para iniciar a análise de emails usando o Assistente de Análise bayesiana:

1. Carregue o assistente de análise bayesiana em **Start > Programs >GFI MailEssentials >GFI MailEssentialsBayesian Analysis Wizard**.

2. Clique em **Next** na tela de boas-vindas.

3. Escolha se deseja:

» Criar um novo arquivo de Perfil de spam bayesiano (.bsp) ou atualizar um arquivo existente. Especifique o caminho onde deseja armazenar o arquivo e o nome do arquivo.

» Atualize o perfil de spam bayesiano usado pelo filtro de análise bayesiana diretamente quando instalá-lo na mesma máquina do GFI MailEssentials.

Clique em **Next** para prosseguir.

4. Selecione como o assistente acessará os emails legítimos. Selecione:

» **Use Microsoft Outlook profile configured on this machine**: obtém emails de uma pasta de emails no Microsoft Outlook. O Microsoft Outlook deve estar em execução para usar esta opção.

» **Connect to a Microsoft® Exchange Server mailbox store**: recupera emails de uma caixa de correio do Microsoft® Exchange. Especifique as credenciais de logon na próxima tela.

» **Do not update legitimate mail (ham) in the Bayesian Spam profile**: ignore a recuperação de emails legítimos. Pule para a etapa 6.

Clique em **Next** para continuar.

5. Depois que o assistente se conectar à origem, selecione a pasta que contém a lista de emails legítimos (por exemplo, a pasta de itens enviados) e clique em **Next**.

6. Selecione como o assistente acessará a fonte de emails com spam. Selecione:

» **Download latest Spam profile from GFI website**: faz o download de um arquivo de perfil de spam que seja atualizado regularmente coletando mensagem dos principais sites de spam. Uma conexão com a Internet é necessária.

» **Use Microsoft Outlook profile configured on this machine**: recupera spam a partir de uma pasta de emails no Microsoft Outlook. O Microsoft Outlook deve estar em execução para usar esta opção.

» **Connect to a Microsoft® Exchange Server mailbox store**: recupera spam de uma caixa de correio do Microsoft® Exchange. Especifique as credenciais de logon na próxima tela.

» **Do not update Spam in the Bayesian Spam profile**: ignora a recuperação de emails com spam. Pule para a etapa 8.

Clique em **Next** para continuar.

7. Depois que o assistente se conectar à origem, selecione a pasta que contém a lista de emails com spam e clique em **Next**.

8. Clique em **Next** para iniciar a recuperação das fontes especificadas. Esse processo pode levar vários minutos para ser concluído.

9. Clique em **Finish** para fechar o assistente.

Etapa 3: Importar o perfil de spam bayesiano

Quando o assistente não for executado no servidor do GFI MailEssentials, importe o arquivo do Perfil de spam bayesiano (.bsp) para o GFI MailEssentials.

1. Mova o arquivo para a pasta **Data** no caminho de instalação doGFI MailEssentials.

2. Reinicie o **GFI MailEssentials AS Scan Engine** e os serviços do **GFI MailEssentials Legacy Attendant**.

14 Glossário

A

Ações de spam

Ações executadas nos emails com spam recebidos, como excluir email ou enviar para a pasta e Lixo eletrônico.

Active Directory

Uma tecnologia que proporciona diversos serviços de rede, incluindo serviços do diretório LDAP.

AD

Consulte Active Directory

Armazenamento de quarentena

Um repositório central do GFI MailSecurity onde todos os emails bloqueados são mantidos até que sejam analisados por um administrador.

Arquivamento recursivo

Sistema de arquivamento que contém vários níveis de subarquivos (ou seja, arquivos dentro de arquivos). Também conhecidos como arquivos aninhados.

Aviso de isenção de responsabilidade

Uma instrução para identificar ou limitar o intervalo de direitos e obrigações de destinatários de emails

B

BITS

Consulte Serviço de transferência inteligente de plano de fundo

Botnet

Uma rede de computadores infectados que funcionam de forma autônoma e são controlados por um hacker/cracker.

C

Cabeçalhos de email

Informações que precedem o texto do email (corpo) em uma mensagem de email. Essas informações incluem remetente, destinatário, assunto, data e hora de envio e recebimento, etc.

Cavalo de Troia

Software mal-intencionado que compromete um computador fazendo-se passar por um software legítimo.

CIDR

Consulte Roteamento entre Domínios sem Classificação

Coleta de diretório

Ataques a emails nos quais endereços de emails conhecidos são usados como um modelo para criar outros endereços de email.

Comandos remotos

Instruções que facilitam a possibilidade de executar tarefas remotamente.

Componente de Acesso a Dados da Microsoft

Uma tecnologia da Microsoft que oferece aos desenvolvedores uma forma homogênea e consistente de desenvolvimento de software que possa acessar praticamente qualquer armazenamento de dados.

Criptografia PGP

Um sistema criptográfico de chave pública muito usado para criptografar emails.

D

DMZ

Consulte Zona desmilitarizada

DNS

Consulte Sistema de Nomes de Domínio

DNS MX

Consulte Troca de emails

E

Exploração

Um método de ataque que utiliza vulnerabilidades conhecidas dos aplicativos ou sistemas operacionais para comprometer a segurança de um sistema.

F

Falsos negativos

Emails com spam que não são detectados como spam.

Falsos positivos

Emails legítimos que são identificados incorretamente como spam.

Feeds RSS

Um protocolo utilizado por sites para distribuir conteúdo (feeds) que é frequentemente alterado (por exemplo, notícias) para assinantes.

Filtragem bayesiana

Uma técnica anti-spam na qual um índice de probabilidades estatísticas baseado em treinamento de usuários é usado para identificar spam.

Filtro da lista de exclusão temporária

Um filtro anti-spam que bloqueia emails enviados por spammers para não reenviar uma mensagem quando uma nova mensagem for recebida.

G

Gateway

O computador (servidor) em uma LAN que está diretamente conectado a uma rede externa. No GFI MailSecurity, gateway se refere a servidores de email da empresa que recebe email de domínios externos.

H

Ham

Email legítimo

HTTP

Hypertext Transfer Protocol - Protocolo usado para transferir dados de hipertexto entre servidores e navegadores da Internet.

I

IIS

Consulte Serviços de Informações da Internet

IMAP

Consulte Protocolo IMAP

L

LDAP

Consulte Protocolo LDAP

Lista de bloqueio

Uma lista de endereços ou domínios de email dos quais emails devem ser rejeitados pelos usuários.

Lista de bloqueio em tempo real

Bancos de dados online de endereços IP de spam. Os emails recebidos são comparados com essas listas para determinar se foram enviados por usuários bloqueados.

Lista de permissão

Uma lista de endereços de email e domínios dos quais os emails são sempre recebidos

Lista de servidores

Um servidor que distribui emails enviados para listas de discussão e boletins informativos e gerencia solicitações de assinatura.

M

Malware

Todos os tipos de software maliciosos que são projetados para comprometer a segurança de computadores e que normalmente se espalham através de métodos mal-intencionados.

MAPI

Consulte MAPI

MDAC

Consulte o Componente de Acesso a Dados da Microsoft

Mecanismo de descompactação

Um módulo de verificação que descompacta e analisa arquivos compactados (por exemplo, arquivos .zip ou .rar) anexados a um email.

Mecanismo de verificação de vírus

Uma tecnologia de detecção de vírus implementada em softwares antivírus que é responsável pela detecção de vírus.

MIME

Consulte MIME

MSMQ

Consulte Serviços de Enfileiramento de Mensagens da Microsoft

N

NDR

Consulte Notificação de falha na entrega

Notificação de falha na entrega

Uma mensagem de email enviada para o remetente sobre um problema de entrega de email.

P

Pasta pública

Uma pasta comum que permite que o usuário do Microsoft Exchange compartilhe informações.

Phishing

O processo de aquisição de informações pessoais confidenciais com o objetivo de fraudar indivíduos, normalmente através do uso de comunicações falsas

POP2Exchange

Um sistema que coleta mensagens de email de caixas de correio POP3 e as roteia para o servidor de email.

POP3

Consulte Protocolo POP ver.3

Protocolo IMAP

Um dos dois protocolos padrão da Internet mais usados para a recuperação de emails. O outro é o POP3.

Protocolo LDAP

Um protocolo de aplicativo usado para consultar e modificar serviços de diretório executados em TCP/IP.

Protocolo POP ver.3

Um protocolo de cliente/servidor para armazenar emails para que os clientes possam estabelecer uma conexão com o servidor POP3 a qualquer momento e ler o email. Um cliente de email estabelece uma conexão TCP/IP com o servidor e, por meio da troca de uma série de comandos, permite que os usuários leiam o email.

Protocolo SMTP

Um padrão de Internet usado para a transmissão de emails através de redes IP.

Protocolo SSL

Um protocolo para garantir uma comunicação integral e segura entre redes.

Q

Quarentena

Um banco de dados de emails no qual emails detectados como spam e/ou malware são armazenados em um ambiente controlado. Os emails em quarentena não são uma ameaça ao ambiente de rede.

R

RBL

Consulte a Lista de bloqueio em tempo real

Recuperador de HTML

Um módulo de filtragem do GFI MailSecurity que verifica e remove código de scripts HTML de emails.

Regras de monitoramento de email

Regras que permitem a replicação de emails entre endereços de email.

Respostas automáticas

Uma resposta de email enviada automaticamente quando emails são recebidos.

Roteamento entre Domínios sem Classificação

Uma notação de endereçamento IP que define um intervalo de endereços IP.

S

Serviço de transferência inteligente de plano de fundo

Um componente dos sistemas operacionais Microsoft Windows que facilita a transferência de arquivos entre sistemas usando a largura de banda de rede inativa.

Serviços de Enfileiramento de Mensagens da Microsoft

Uma implementação de fila de mensagens para os sistemas operacionais Windows Server.

Serviços de Informações da Internet

Conjunto de serviços baseados na Internet criado pela Microsoft Corporation para servidores de Internet.

Servidor/gateway de perímetro

O host em uma LAN que está diretamente conectado a uma rede externa. No GFI MailEssentials, gateway de perímetro se refere aos servidores de email da empresa que recebem emails de domínios externos.

Sistema de nomes de domínio

Um banco de dados usado por redes TCP/IP que permite a tradução de nomes de host em endereços IP e fornece outras informações relacionadas ao domínio.

SMTP

Consulte Protocolo SMTP

Software antivírus

Software que detecta malware, como Cavalos de Troia, em emails, arquivos e aplicativos.

SSL

Consulte Protocolo SSL

T

Troca de emails

O registro DNS utilizado para identificar os endereços IP dos servidores de email do domínio.

W

WebDAV

Uma extensão do HTTP que permite aos usuários gerenciar arquivos remotamente e de modo interativo. Usado para gerenciar email na caixa de correio e na pasta pública do Microsoft Exchange.

Z

Zona desmilitarizada

Uma seção com acesso à Internet de uma rede que não faz parte da rede interna. Normalmente, funciona como gateway entre as redes internas e a Internet.

Zumbi

Um computador infectado que faz parte de uma Botnet através de malware.

15 Índice

N

P

Q

R

S

V

W

EUA, CANADÁ E AMÉRICA DO SUL E CENTRAL

4309 Emperor Blvd, Suite 400, Durham, NC 27703, USA

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, UK

Telefone: +44 (0) 870 770 5370

Fax: +44 (0) 870 770 5377

sales@gfi.co.uk

EUROPA, ORIENTE MÉDIO E ÁFRICA

GFI House, Territorials Street, Mriehel BKR 3000, Malta

Telefone: +356 2205 2000

Fax: +356 2138 2419

sales@gfi.com

AUSTRÁLIA E NOVA ZELÂNDIA

83 King William Road, Unley 5061, South Australia

Telefone: +61 8 8273 3000

Fax: +61 8 8273 3099

sales@gfiap.com