AVG Email Server Edition 2013

Manual do Usuário

Revisão do documento 2013.01 (20.11.2012)

Conteúdo

1. Introdução

Este manual do usuário fornece uma documentação completa para o **AVG Email Server Edition 2013**.

Parabéns pela aquisição do AVG Email Server Edition 2013!

O **AVG Email Server Edition 2013** é um dos vários produtos premiados da AVG, criados para proporcionar paz de espírito e total segurança a seu servidor. Como ocorre com todos os produtos AVG, o **AVG Email Server Edition 2013** foi totalmente reformulado para oferecer proteção de segurança certificada e renomada, de uma nova forma mais eficiente e amigável.

O AVG foi projetado e desenvolvido para proteger seu computador e sua atividade de rede. Aproveite a experiência da proteção completa com o AVG.

Observação: *esta documentação contém a descrição de recursos específicos do Email Server Edition. Caso necessite de informações sobre os recursos do AVG, consulte o guia de usuário para Internet Security Edition que contém todos os detalhes necessários. Você pode fazer download do arquivo em http://www.avg.com.*

2. Requisitos de instalação do AVG

2.1. Sistemas operacionais suportados

O **AVG Email Server Edition 2013** destina-se a proteger servidores de email executados nos seguintes sistemas opcionais:

- Windows 2008 Server Edition (x86 e x64)
- Windows 2003 Server (x86, x64) SP1

2.2. Servidores de e-mail suportados

Os seguintes servidores de arquivos são suportados:

- Versão do MS Exchange 2003 Server
- Versão do MS Exchange 2007 Server
- Versão do MS Exchange 2010 Server
- Kerio MailServer – versão 6.7.2 e superior

2.3. Requisitos de hardware

Os requisitos mínimos de hardware para o **AVG Email Server Edition 2013** são:

- CPU Intel Pentium 1.5 GHz
- 500 MB de espaço livre em disco rígido (para fins de instalação)
- 512 MB de memória RAM

Os requisitos de hardware recomendados para o **AVG Email Server Edition 2013** são:

- CPU Intel Pentium 1.8 GHz
- 600 MB de espaço livre em disco rígido (para fins de instalação)
- 512 MB de memória RAM

2.4. Desinstalar versões anteriores

Se você tiver uma versão mais antiga do AVG Email Server instalada, deverá desinstalá-la manualmente antes de instalar o **AVG Email Server Edition 2013**. Você deve executar a desinstalação da versão anterior manualmente, utilizando a funcionalidade do Windows.

- No menu iniciar ***Iniciar/Configurações/Painel de Controle/Adicionar ou Remover Programas***, selecione o programa correto da lista de softwares instalados (ou é possível fazê-lo ainda mais

facilmente através do menu ***Iniciar/Todos os Programas/AVG/Desinstalar o AVG***).

- Se você usou anteriormente o AVG 8.x ou versão mais antiga, não se esqueça de desinstalar também plug-ins de servidor individual.

  Observação: *será necessário reiniciar o serviço de armazenamento durante o processo de desinstalação.*

  Trocar plug-in – execute setupes.exe com o parâmetro /uninstall na pasta em que o plug-in estava instalado.

  por exemplo: C:\AVG4ES2K\setupes.exe /uninstall

  Lotus Domino/Notes plug-in – execute setupln.exe com o parâmetro /uninstall na pasta em que o plug-in estava instalado:

  por exemplo: C:\AVG4LN\setupln.exe /uninstall

2.5. MS Exchange Service Packs

Nenhum service pack é necessário para o MS Exchange 2003 Server; entretanto, é recomendável manter o sistema o mais atualizado possível com os service packs e hotfixes mais recentes para obter o máximo de segurança disponível.

Service Pack para MS Exchange 2003 Server (opcional):

http://www.microsoft.com/en-us/download/details.aspx?id=9664

No início da instalação, todas as versões de biblioteca do sistema serão examinadas. Se for necessário instalar bibliotecas mais novas, o instalador renomeará as antigas com uma extensão .delete. Elas serão excluídas após a reinicialização do sistema.

Service Pack para MS Exchange 2007 Server (opcional):

http://www.microsoft.com/downloads/details.aspx?FamilyID=44c66ad6-f185-4a1d-a9ab-473c1188954c&displaylang=en

Service Pack para MS Exchange 2010 Server (opcional):

http://www.microsoft.com/en-us/download/details.aspx?id=28190

3. Processo de instalação do AVG

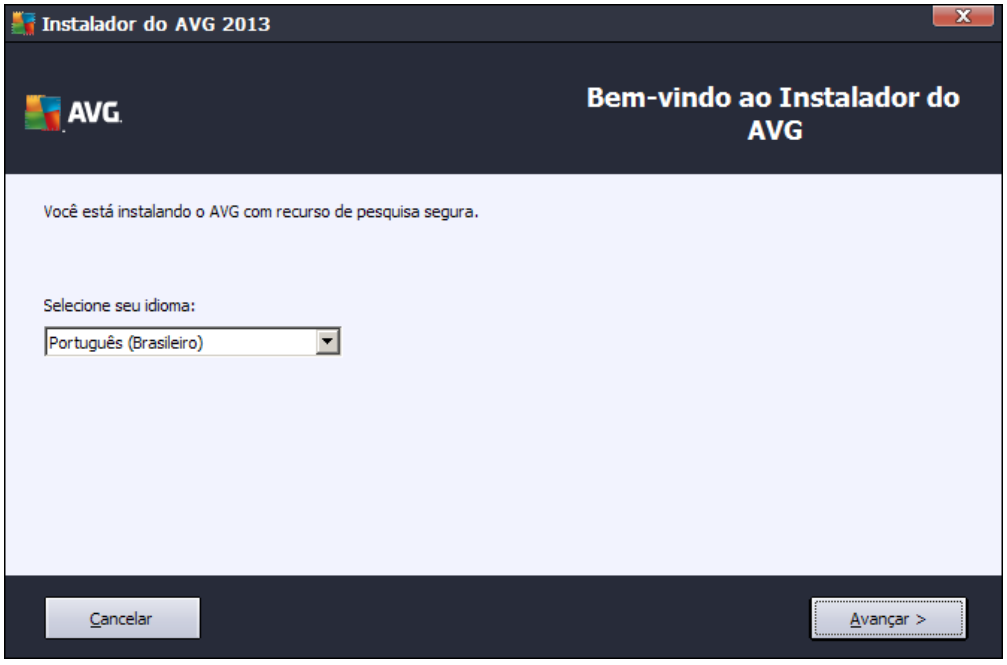
Para instalar o AVG no computador, é necessário obter o arquivo de instalação mais recente. Você pode usar o arquivo de instalação do CD que é parte da edição, mas o arquivo pode estar desatualizado. Dessa forma, é recomendável obter a versão mais recente do arquivo de instalação on-line. Você pode fazer download do arquivo no site da AVG (em http://www.avg.com/download?prd=msw).

Há dois pacotes de instalação disponíveis para o seu produto – para sistemas operacionais de 32 bits (marcado como x86) e para sistemas operacionais de 64 bits (marcado como x64). Use o pacote de instalação correto para o seu sistema operacional específico.

Durante o processo de instalação será solicitado o seu número de licença. Certifique-se de tê-lo disponível antes de iniciar a instalação. O número pode ser encontrado na embalagem do CD. Se você adquiriu a sua cópia do AVG on-line, o número da licença foi enviado para você por email.

Após fazer download e salvar o arquivo de instalação na unidade de disco rígido, você poderá iniciar o processo de instalação. A instalação é uma sequência de janelas de caixa de diálogo com uma descrição resumida do que fazer em cada etapa. A seguir, oferecemos uma explicação de cada janela da caixa de diálogo:

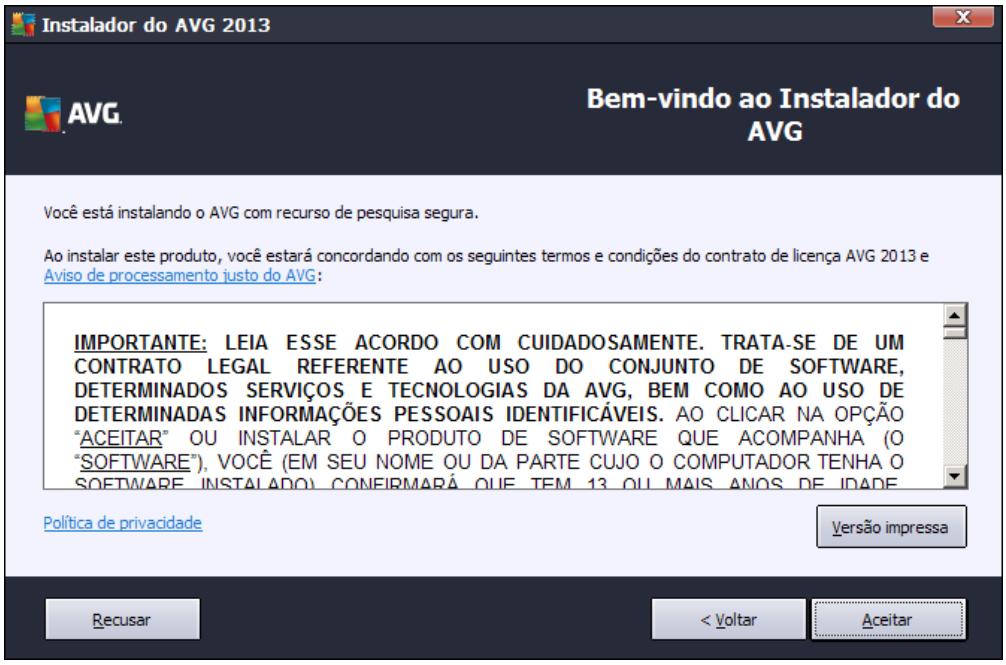
3.1. Início da instalação



O processo de instalação é iniciado com a janela de ***boas-vindas***. Nela você seleciona o idioma usado para o processo de instalação e pressiona o botão ***Avançar***.

Você poderá escolher também idiomas adicionais para a interface de aplicativo posteriormente, durante o processo de instalação.

3.2. Contrato de licença

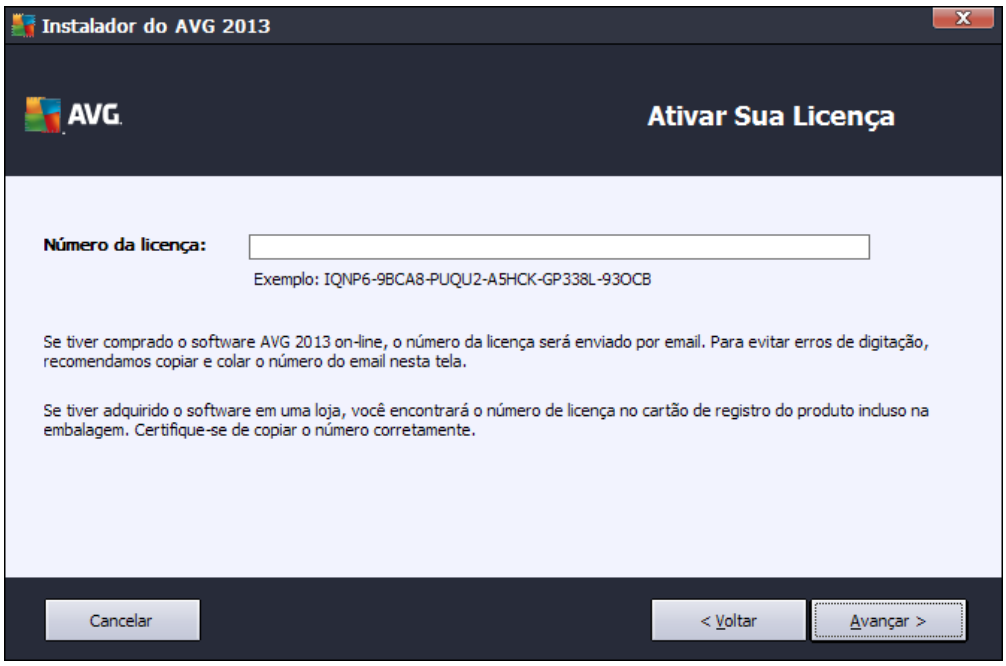


Esta caixa de diálogo permite que você leia as condições da licença. Use o botão ***Versão impressa*** para abrir o texto da licença em uma nova janela. Pressione o botão ***Aceitar*** para confirmar e passar para a próxima caixa de diálogo.

3.3. Ativar Sua Licença

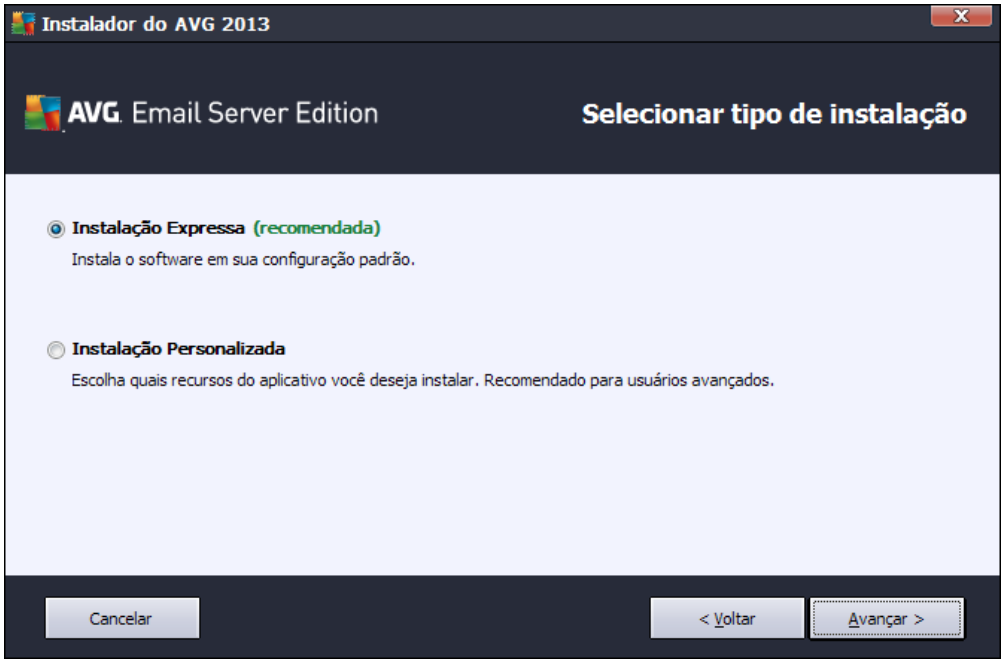
Na caixa de diálogo ***Ativar licença*** você precisa preencher os seus dados de registro.

Digite seu número de licença no campo de texto ***Número da Licença***. O número da licença está no email de confirmação recebido depois da compra do AVG on-line. Digite o número exatamente como mostrado. Se o formulário digital do número de licença estiver disponível (no email), é recomendável usar o método de copiar e colar para inseri-lo.



Pressione o botão ***Avançar*** para continuar o processo de instalação.

3.4. Selecionar o tipo de instalação



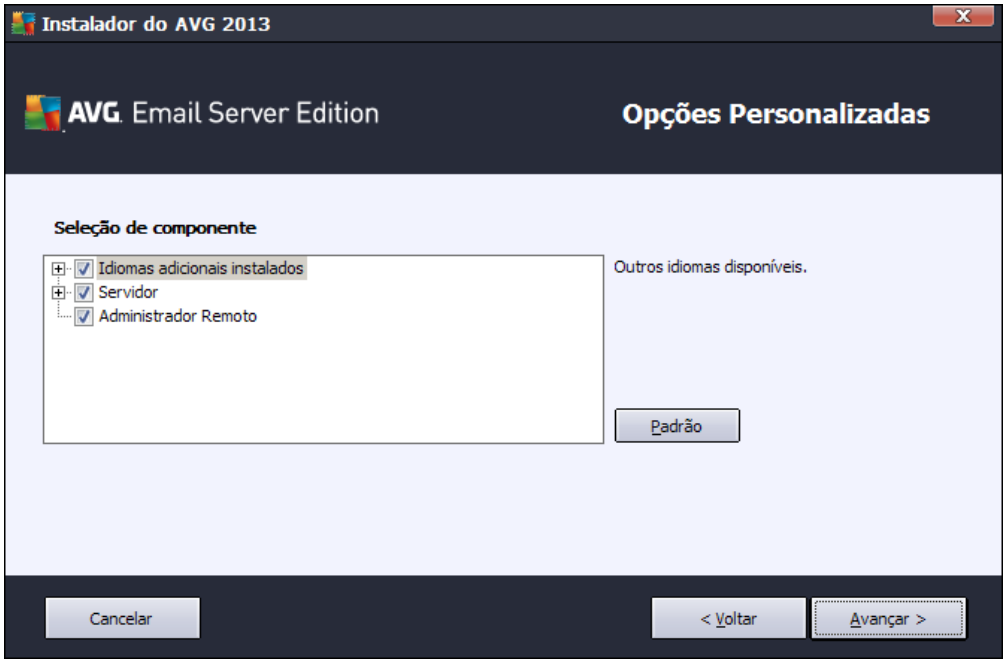
A caixa de diálogo ***Selecionar tipo de instalação*** oferece duas opções de instalação: ***Instalação Expressa*** e ***Instalação Personalizada***.

Para a maioria dos usuários, é altamente recomendável manter a ***Instalação Expressa***, que instala o AVG no modo totalmente automático, com configurações predefinidas pelo fornecedor do programa. Essa configuração fornece o máximo de segurança combinado com o uso ideal dos recursos. No futuro, se houver necessidade de alterar a configuração, você sempre terá a possibilidade de fazer isso diretamente no aplicativo AVG.

A Instalação Personalizada só deve ser usada por usuários experientes que tenham um motivo válido para instalar o AVG com configurações diferentes das padrão, ou seja, para se ajustar aos requisitos específicos do sistema.

Ao selecionar Instalação Personalizada, a seção ***Pasta de destino*** é exibida na parte inferior da caixa de diálogo. Ela permite especificar o local onde o AVG será instalado. Como padrão, o AVG será instalado na pasta Arquivos de programas da unidade C:. Se você desejar alterar esse local, use o botão ***Procurar*** para exibir a estrutura da unidade e selecionar a respectiva pasta.

3.5. Instalação personalizada – Opções personalizadas



A seção ***Seleção do Componente*** exibe uma visão geral de todos os componentes do AVG que podem ser instalados. Se as configurações padrão não forem adequadas a você, será possível remover/adicionar componentes específicos.

Entretanto, só é possível selecionar os componentes incluídos na edição do AVG que você adquiriu. Somente esses componentes serão oferecidos para a instalação na caixa de diálogo Seleção do componente.

- ***Administração Remota*** – se você pretende conectar o AVG a um AVG DataCenter (Edições de rede do AVG), será necessário selecionar esta opção.

- ***Idiomas adicionais instalados*** – você pode definir em que idioma(s) o AVG deverá ser instalado. Marque o item ***Idiomas adicionais instalados*** e selecione os idiomas desejados no respectivo menu.

Visão geral básica de componentes individuais de servidor (no ramo ***Servidor***):

- ***Servidor Anti-Spam para MS Exchange***

  Verifica todas as mensagens de email recebidas e marca os emails indesejáveis como SPAM. Usa diversos métodos de análise para processar cada mensagem de email, oferecendo o máximo de proteção possível contra mensagens de email indesejáveis.

- ***Verificador de Email para MS Exchange (Agente de Transporte de roteamento)***

  Verifica todas as mensagens de email internas, recebidas e enviadas através da função HUB do MS Exchange.

- ***Verificador de Email para MS Exchange (SMTP Agente de Transporte)***

  Verifica todas as mensagens de email que chegam através da interface SMTP do MS Exchange (pode ser instalado em funções EDGE e HUB).

- ***Verificador de Email para MS Exchange (VSAPI)***

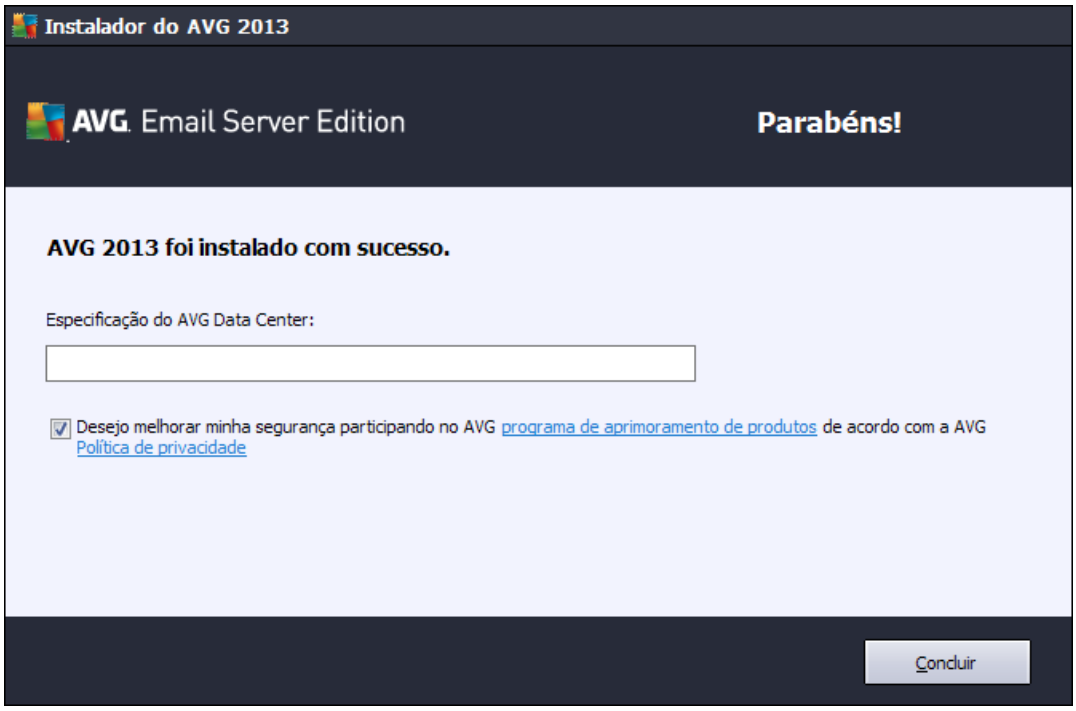
  Verifica todas as mensagens de email armazenadas nas caixas de correio dos usuários. Se algum vírus for detectado, será movido para a Quarentena de vírus, ou removido completamente.

Para os usuários do Exchange 2003 apenas os componentes Anti-Spam e Verificador de Email (VSAPI) estão disponíveis.

Continue pressionando o botão ***Avançar***.

3.6. Conclusão da instalação

Se você tiver selecionado o módulo de ***Administração remota*** durante a seleção de módulo, na tela final você poderá definir a string de conexão para conectar ao seu AVG DataCenter.



Esta caixa de diálogo permite que você decida se deseja participar no Programa de Aprimoramento de Produto que coleta informações anônimas sobre as ameças detectadas, para aumentar o nível de segurança geral na Internet. Se você concorda com esta declaração, mantenha a opção ***Desejo aprimorar minha segurança participando do Programa de Aprimoramento de Produto da AVG de acordo com a Política de Privacidade da AVG*** marcada *(como padrão, a opção está confirmada)*.

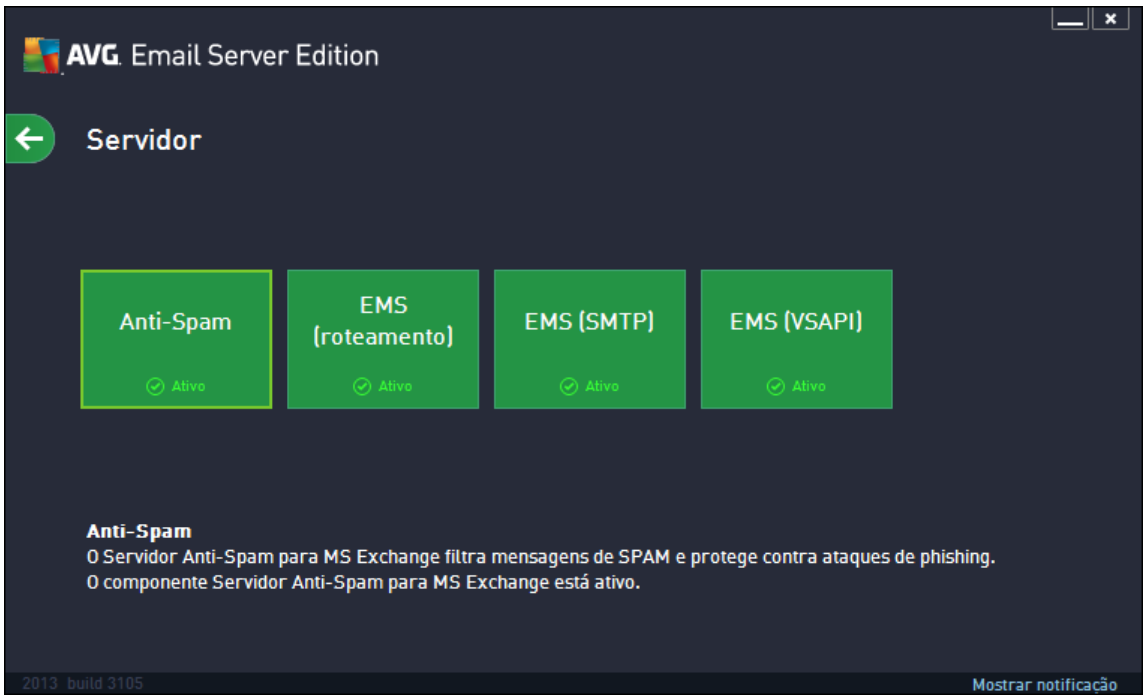
Confirme suas escolhas clicando no botão **Concluir**.

Agora o AVG está instalado no computador e funcionando perfeitamente. O programa está sendo executado em segundo plano, em modo totalmente automático.

4. Após a Instalação

Imediatamente após a instalação ser concluída, a tela principal do ***AVG Email Server Edition 2013*** é exibida:

Este manual trata apenas dos recursos específicos do ***AVG Email Server Edition 2013***; todos os outros componentes e configurações são descritos no manual do AVG Destktop. Para acessar a caixa de diálogo principal de componentes do servidor, clique no botão ***Servidor***. A seguinte tela será exibida:



Observe que todos os componentes estarão disponíveis (a menos que você escolha não instalar alguns deles durante o processo de instalação, claro) apenas se você estiver usando MS Exchange 2007 ou superior. O MS Exchange 2003 suporta apenas os componentes Anti-Spam e Verificador de Email (VSAPI).

Para configurar individualmente a proteção do seu servidor de email, siga o capítulo apropriado:

- ***Verificadores de Email MS Exchange***
- ***Servidor Anti-Spam para MS Exchange***
- ***AVG para Kerio MailServer***

5. Verificadores de e-mail para MS Exchange

5.1. Visão geral

Visão geral básica dos componentes individuais de servidor do Verificador de Email:

- ***EMS (roteamento) – Verificador de Email para MS Exchange (Agente de Transporte de roteamento)***

  Verifica todas as mensagens de email internas, recebidas e enviadas através da função HUB do MS Exchange.

  Disponível para MS Exchange 2007/2010 e pode ser instalado somente para a função HUB.

- ***EMS (SMTP) – Verificador de Email para MS Exchange (SMTP Agente de Transporte)***

  Verifica todas as mensagens de email recebidas através da interface SMTP do MS Exchange.

  Disponível para MS Exchange 2007/2010 e só pode ser instalado para as funções EDGE e HUB.

- ***EMS (VSAPI) – Verificador de Email para MS Exchange (VSAPI)***

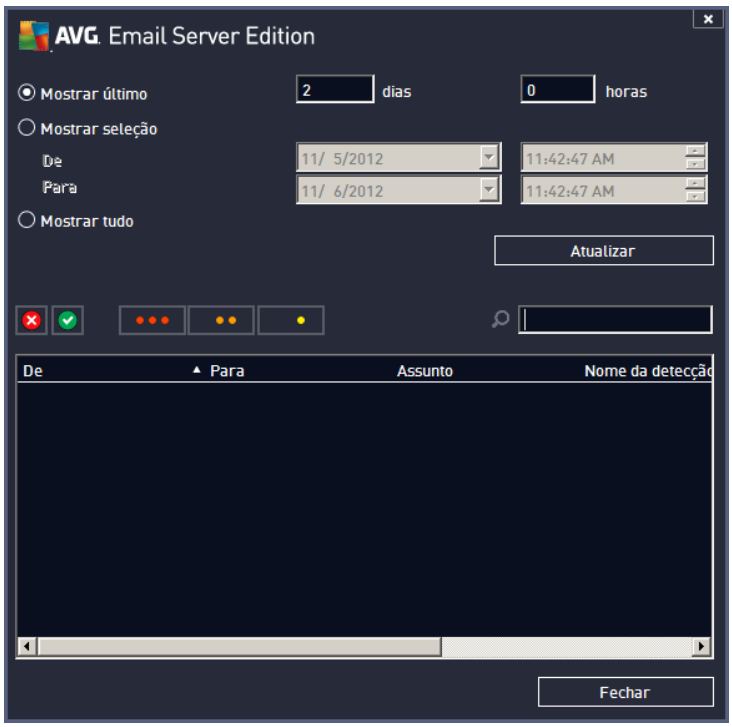
  Verifica todas as mensagens de email armazenadas nas caixas de correio dos usuários. Se algum vírus for detectado, será movido para a Quarentena de vírus, ou removido completamente.

Clique no ícone de um componente necessário para abrir sua interface. Todos os componentes compartilham os botões e links de controle comum a seguir:

- ***ATIVADO/DESATIVADO*** – clicar nesse botão ativa ou desativa o componente selecionado (se o componente estiver ligado, o botão e o texto são verdes, se estiver desligado, vermelhos).

- ***Resultados da verificação***

  Abre uma nova caixa de diálogo em que você pode revisar os resultados de verificação:



  Aqui você pode verificar as mensagens divididas em várias páginas de acordo com sua gravidade. Veja a configuração dos componentes individuais para alteração da gravidade e geração de relatórios.

  São exibidos por padrão somente os resultados para os últimos dois dias. Você pode alterar o período exibido, alterando as seguintes opções:

  - ***Mostrar último*** – insira dias e horas de preferência.
  - ***Mostrar seleção*** – selecione um intervalo de data e hora personalizado.
  - ***Mostrar tudo*** – exibe resultados para todo o período de tempo.

  Use botão ***Atualizar*** para recarregar os resultados.

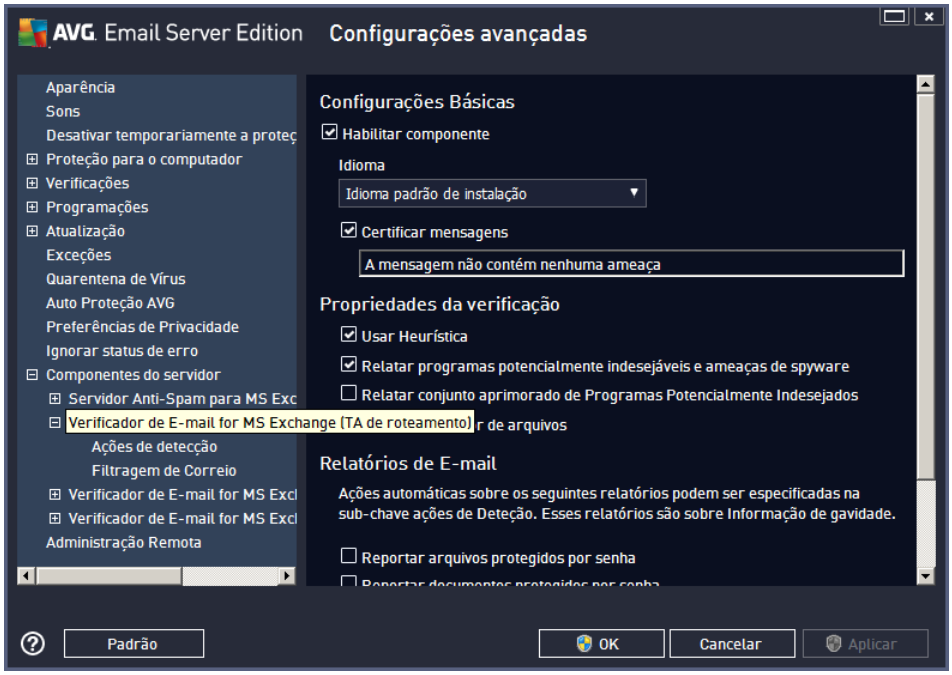
- ***Atualizar valores estatísticos*** – atualiza as estatísticas exibidas acima.

Clicar no botão de trabalho ***Configurações*** abre configurações avançadas para o componente selecionado (você encontrará mais informações sobre configurações adicionais de todos os componentes nos capítulos abaixo).

5.2. Verificador de E-mail para MS Exchange (TA de roteamento)

Para abrir as configurações do ***Verificador de Email para MS Exchange (agente de transporte de roteamento)***, selecione o botão ***Configurações*** na interface do componente.

A partir da lista ***Componentes do servidor***, selecione o item ***Verificador de Email para MS Exchange (TA de roteamento)***:



A seção ***Configurações básicas*** contém as seguintes opções:

- ***Ativar componente*** – desmarque para desativar todo o componente.
- ***Idioma*** – selecione o idioma de preferência do componente.
- ***Certificar mensagens*** – selecione esta opção para adicionar uma nota de certificação a todas as mensagens verificadas. Você pode personalizar a mensagem no campo seguinte.

A seção ***Propriedades de verificação***:

- ***Usar heurística*** – selecione esta caixa para ativar o método de análise heurística durante a verificação.
- ***Reportar ameaças de spyware e programas potencialmente indesejáveis*** – selecione esta opção para informar a presença de spyware e programas potencialmente indesejáveis.
- ***Informar conjunto avançado de programas potencialmente indesejáveis*** – marque essa caixa para detectar o pacote estendido de spyware: programas que estão perfeitamente ok e inofensivos quando adquiridos do fabricante diretamente, mas podem ser mal utilizados para finalidades mal intencionadas posteriormente, ou programas sempre inofensivos mas que podem ser indesejados (várias barras de ferramentas, etc.). Essa é uma medida adicional que aumenta ainda mais a segurança e o conforto do seu computador, no entanto possivelmente ela bloqueie programas legais; portanto, está desativada por padrão. Observação: este recurso de detecção é adicional para a opção anterior; por isso, se quiser

proteção contra os tipos básicos de spyware, sempre mantenha a caixa anterior selecionada.

- ***Verificar dentro de arquivos*** – selecione esta opção para permitir que o verificador procure dentro de arquivos de compactação (zip, rar, etc.).

A seção ***Informação de anexos de email*** permite que você escolha quais itens devem ser informados durante a verificação. Se marcada, cada email com este item conterá a tag [INFORMAÇÃO] no assunto da mensagem. Esta é a configuração padrão que pode ser facilmente alterada na seção ***Ações de detecção***, parte ***Informações*** (veja abaixo).

As seguintes opções estão disponíveis:

- ***Reportar arquivos protegidos por senha***
- ***Reportar documentos protegidos por senha***
- ***Reportar arquivos que contenham macro***
- ***Reportar extensões ocultas***

Há também estes subitens disponíveis na seguinte estrutura de árvore:

- ***Ações de detecção***
- ***Filtragem de correio***

5.3. Verificador de E-mail para MS Exchange (SMTP TA)

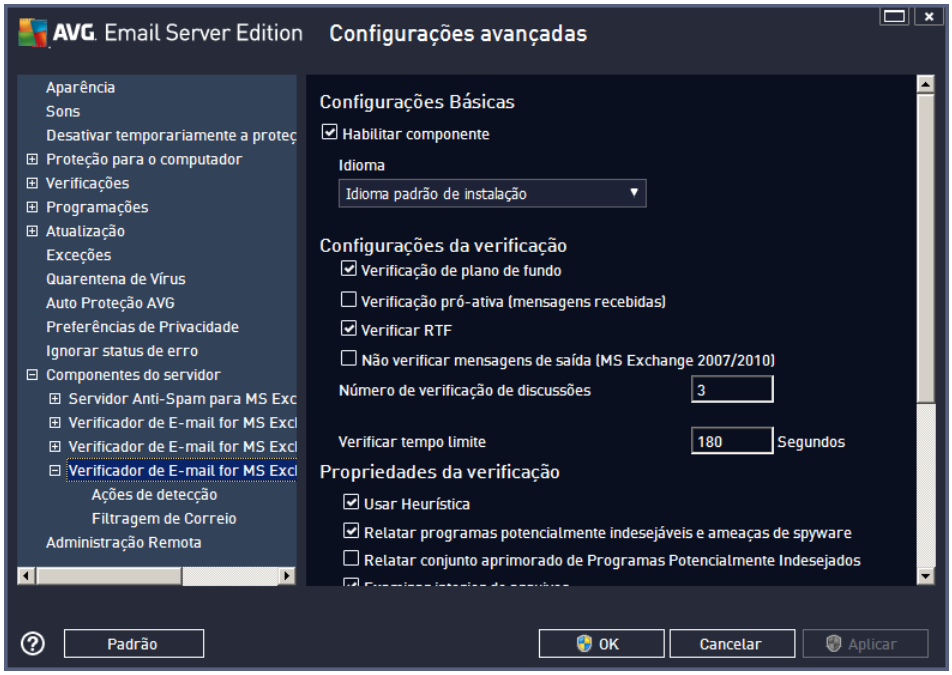
A configuração para o ***Verificador de Email para MS Exchange (agente de transporte do SMTP)*** é exatamente o mesmo como no caso do agente de transporte de roteamento. Para maiores informações, consulte o capítulo acima ***Verificador de Email para MS Exchange (roteamento TA)***.

Há também estes subitens disponíveis na seguinte estrutura de árvore:

- ***Ações de detecção***
- ***Filtragem de correio***

5.4. Verificador de E-mail para MS Exchange (VSAPI)

Este item contém as configurações do ***Verificador de Email para MS Exchange (VSAPI)***.



A seção ***Configurações básicas*** contém as seguintes opções:

- ***Ativar componente*** – desmarque para desativar todo o componente.
- ***Idioma*** – selecione o idioma de preferência do componente.

A seção ***Configurações da verificação***:

- ***Verificação em Segundo Plano*** – use esta caixa para ativar ou desativar a verificação em segundo plano. Essa verificação é um dos recursos da interface de aplicativo VSAPI 2.0/2.5. Ela oferece verificação encadeada dos bancos de dados de mensagens do Exchange. Sempre que um item que não tenha sido verificado antes com a atualização com base de vírus do AVG for encontrado nas pastas da caixa de correio dos usuários,ele será enviado ao AVG para Exchange Server para verificação. A verificação e a procura de objetos não examinados são executadas em paralelo.

  Um processo de baixa prioridade específico é utilizado para cada banco de dados, o que garante que outras tarefas (por exemplo, armazenamento de mensagens de email no banco de dados do Microsoft Exchange) sejam sempre executadas com preferência.

- ***Verificação pró-ativa (mensagens recebidas)***

  Você pode ativar ou desativar a função de verificação pró-ativa do VSAPI 2.0/2.5 aqui. Esta verificação ocorre quando um item for entregue para uma pasta, mas uma solicitação não tenha sido feita por um cliente.

  Assim que as mensagens são enviadas para o armazenamento no Exchange, entram na fila global de verificação como prioridade baixa (máximo de 30 itens). Eles são verificados com base na primeira

entrada, primeira saída (FIFO). Se um item for acessado quando ainda estiver na fila, é alterado para alta prioridade.

O excesso de mensagens continuará para a loja não autorizada.

Mesmo que você desative as opções ***Verificação em segundo plano*** e ***Verificação pró-ativa***, o verificador em acesso ainda estará ativo quando um usuário tentar baixar uma mensagem com o cliente MS Outlook.

- ***Verificar RTF*** – especifique aqui se o tipo de arquivo RTF deverá ser verificado ou não.
- ***Não verificar mensagens de saída (MS Exchange 2007/2010)*** – com ambos os componentes de servidores VSAPI e Agente de Transporte de Roteamento (TA de roteamento) instalados (seja em apenas um servidor ou em dois diferentes), os emails de saída podem ser verificados duas vezes. A primeira verificação é feita pelo verificador de acesso VSAPI, e a segunda pelo Agente de Transporte de Roteamento. Isso pode causar lentidão no servidor e atrasos moderados no envio de emails. Se tem certeza de que os componentes do servidor estão instalados e ativos, você pode optar por evitar esta verificação dupla de email de saída através da desativação do verificador de acesso VSAPI.
- ***Número de ameaças verificadas*** – o processo de verificação é encadeado por padrão para aumentar o desempenho geral da verificação em um certo nível de paralelismo. Altere a contagem de processos aqui.

  O número padrão de processos é calculado como 2 vezes o 'número_de_processadores + 1.

  O número mínimo de ameaças computadas são ('número de processos'+1) divididas por 2.

  O número mínimo de ameaças computadas como 'processos 'número de processadores' + 5) multiplicados por 5+1.

  Se o valor é o mínimo ou menor valor ou o valor máximo igual ou superior, o valor padrão é usado.
- ***Campo Tempo Limite de Verificação*** – o intervalo contínuo máximo (em segundos) para que um processo acesse a mensagem sendo verificada).

A seção ***Propriedades de verificação***:

- ***Usar heurística*** – selecione esta caixa para ativar o método de análise heurística durante a verificação.
- ***Reportar ameaças de spyware e programas potencialmente indesejáveis*** – selecione esta opção para informar a presença de spyware e programas potencialmente indesejáveis.
- ***Informar conjunto avançado de programas potencialmente indesejáveis*** – marque essa caixa para detectar o pacote estendido de spyware: programas que estão perfeitamente ok e inofensivos quando adquiridos do fabricante diretamente, mas podem ser mal utilizados para finalidades mal intencionadas posteriormente, ou programas sempre inofensivos mas que podem ser indesejados (várias barras de ferramentas, etc.). Essa é uma medida adicional que aumenta ainda mais a segurança e o conforto do seu computador, no entanto possivelmente ela bloqueie programas legais; portanto, está desativada por padrão. Observação: este recurso de detecção é adicional para a opção anterior; por isso, se quiser proteção contra os tipos básicos de spyware, sempre mantenha a caixa anterior selecionada.
- ***Verificar dentro de arquivos*** – selecione esta opção para permitir que o verificador procure dentro de

arquivos de compactação (zip, rar, etc.).

A seção ***Informação de anexos de email*** permite que você escolha quais itens devem ser informados durante a verificação. A configuração padrão pode ser facilmente alterada na seção ***Ações de detecção***, parte ***Informações*** (veja abaixo).

As seguintes opções estão disponíveis:

- ***Reportar arquivos protegidos por senha***
- ***Reportar documentos protegidos por senha***
- ***Reportar arquivos que contenham macro***
- ***Reportar extensões ocultas***

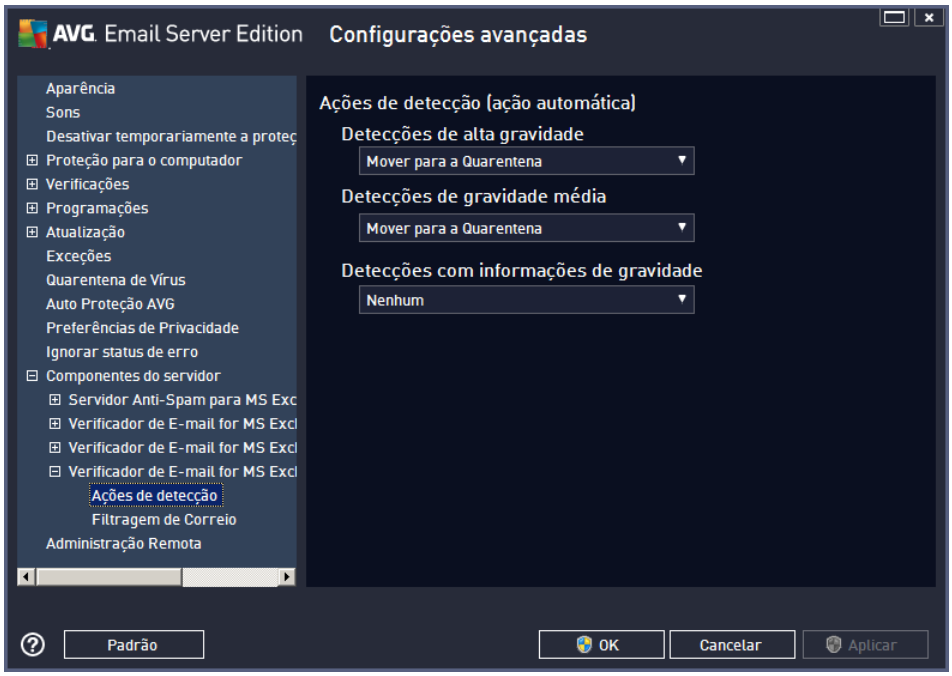
Geralmente alguns destes recursos são extensões de usuário dos serviços da interface de aplicativo Microsoft VSAPI 2.0/2.5. Para obter informações detalhadas sobre a VSAPI 2.0/2.5, consulte os seguintes links (e também os links acessíveis pelos indicados):

- http://support.microsoft.com/default.aspx?scid=kb;en-us;328841&Product=exch2k – para obter informações sobre o Exchange e a interação de software antivírus.
- http://support.microsoft.com/default.aspx?scid=kb;en-us;823166 – para obter informações sobre recursos adicionais da VSAPI 2.5 no aplicativo Exchange 2003 Server.

Há também estes subitens disponíveis na seguinte estrutura de árvore:

- ***Ações de detecção***
- ***Filtragem de correio***

5.5. Ações de detecção



No subitem ***Ações de detecção*** você pode escolher ações automáticas que devem ocorrer durante o processo de verificação.

As ações estão disponíveis para os seguintes itens:

- ***Detecções de alta gravidade*** – códigos maliciosos que copiam e espalham-se, passando muitas vezes despercebidos até que o estrago esteja feito.
- ***Detecções de gravidade média*** – em geral, esses programas variam de ameaças realmente sérias a apenas em potencial à sua privacidade.
- ***Detecções com informações de gravidade*** – inclui todas as possíveis ameaças detectadas que não possam ser classificadas em nenhuma das categorias acima.

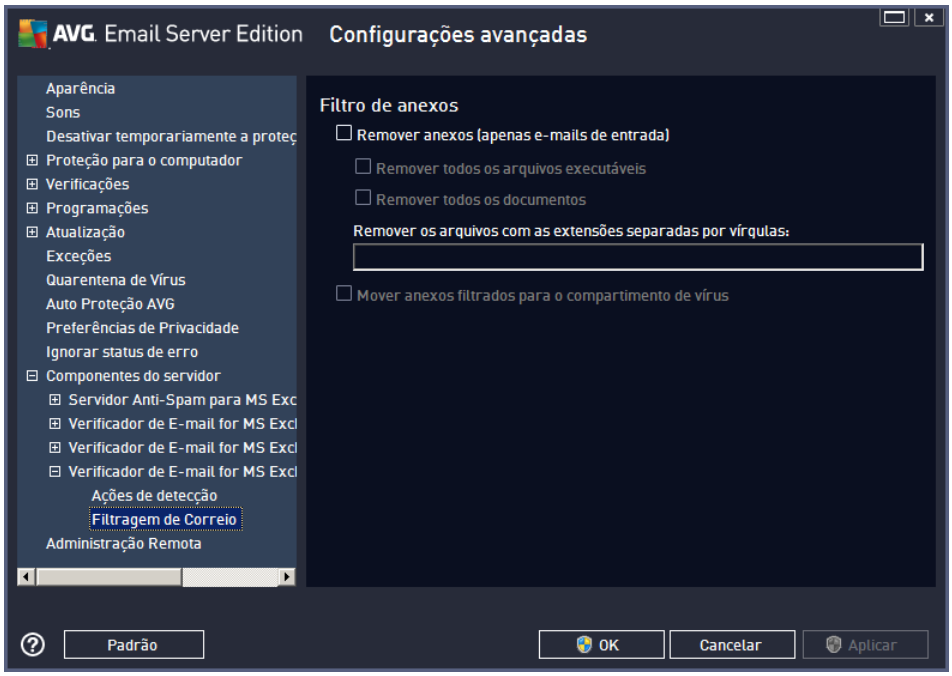
Use o menu suspenso para escolher uma ação para cada item:

- ***Nenhuma*** – nenhuma ação será realizada.
- ***Mover para Quarentena*** – a ameaça determinada será movida para a Quarentena de vírus.
- ***Remover*** – a ameaça determinada será removida.

Para selecionar um texto de assunto personalizado para mensagens que contenham item/ameaça determinadas, selecione e caixa ***Marcar assunto com...*** e preencha um valor preferido.

O último recurso mencionado não está disponível para o Verificador de email para VSAPI para MS Exchange.

5.6. Filtragem de correio



No subitem ***Filtragem de correio*** é possível escolher quais anexos devem ser automaticamente removidos, se houver. As seguintes opções estão disponíveis:

- ***Remover anexos*** – selecione esta caixa para ativar o recurso.
- ***Remover todos os arquivos executáveis*** – remove todos os executáveis.
- ***Remover todos os documentos*** – remove todos os arquivos de documentos.
- ***Remover arquivos com estas extensões separadas por vírgula*** – preencha a caixa com as extensões de arquivo que você deseja remover automaticamente. Separe as extensões com vírgulas.
- ***Mover anexos filtrados para a quarentena de vírus*** – marque essa opção se não desejar que os anexos filtrados sejam totalmente removidos. Com essa caixa selecionada, todos os anexos selecionados nesta caixa de diálogo serão movidos automaticamente para o ambiente da Quarentena de vírus. A quarentena é um lugar seguro para armazenar arquivos potencialmente perigosos. Eles podem ser exibidos e analisados sem qualquer tipo de risco para o sistema. A Quarentena de vírus pode ser acessada pelo menu superior da interface principal do **AVG Email Server Edition 2013**. Basta clicar com o botão esquerdo no item ***Opções*** e escolher ***Quarentena de Vírus*** no menu suspenso.

6. Servidor Anti-spam para MS Exchange

6.1. Princípios do Anti-Spam

Spam refere-se a email não solicitado, a maioria referente a propaganda de produto ou de serviço, enviada em grande quantidade para um grande número de endereços de email ao mesmo tempo, enchendo as caixas de correio. Spam não se refere a email comercial válido, cujo envio conta com o consentimento por parte dos clientes. O spam não é apenas inoportuno, mas também pode ser fonte de fraudes, vírus ou conteúdo ofensivo.

O ***Anti-Spam*** verifica todas as mensagens de email recebidas e marca os emails indesejáveis como SPAM. Usa diversos métodos de análise para processar cada mensagem de email, oferecendo o máximo de proteção possível contra mensagens de email indesejáveis.

6.2. Interface do Anti-Spam

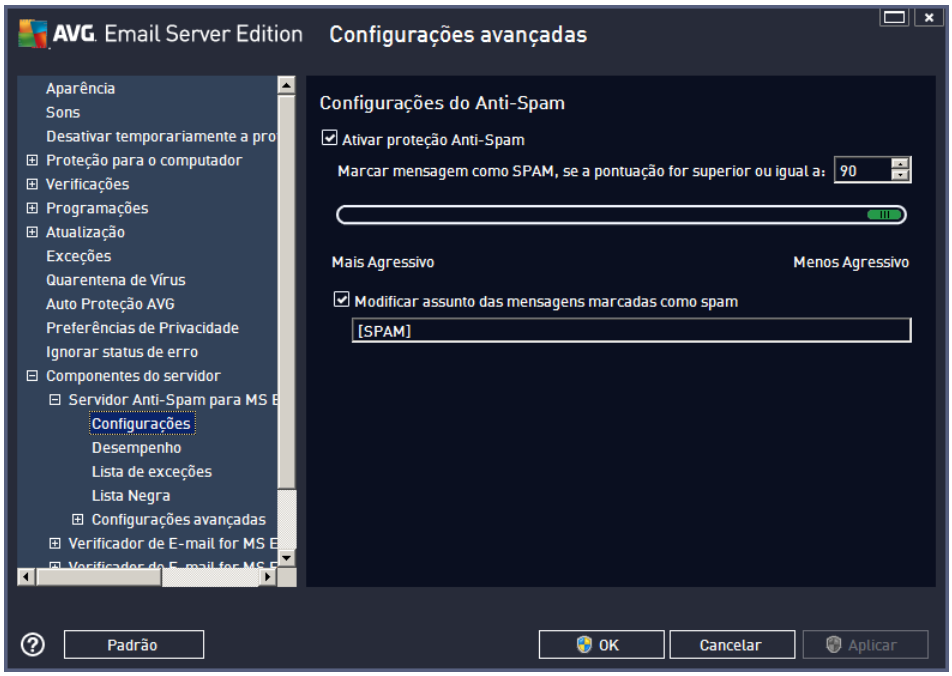
Esta caixa de diálogo contém uma breve informação sobre a funcionalidade do componente de servidor, informações sobre seu status atual (*Ativado/Desativado*), e algumas estatísticas.

Botões disponíveis e links:

- ***ATIVADO/DESATIVADO*** – clicar nesse botão ativa ou desativa o componente selecionado (se o componente estiver ligado, o botão e o texto são verdes, se estiver desligado, vermelhos).
- ***Atualizar valores estatísticos*** – atualiza as estatísticas exibidas acima.
- ***Configurações*** – use esse botão para abrir as Configurações avançadas do Anti-Spam.

6.3. Configurações Anti-Spam

6.3.1. Configurações



Nesta caixa de diálogo, você pode marcar a caixa de seleção ***Ativar proteção do Anti-Spam*** para permitir/ proibir a verificação anti-spam da comunicação por email.

Nessa caixa de diálogo, você pode selecionar medidas de pontuação mais ou menos agressivas. O ***filtro Anti-Spam*** atribui a cada mensagem uma pontuação (*ou seja, o nível de semelhança entre um SPAM e o conteúdo da mensagem*), com base em várias técnicas dinâmicas de verificação. É possível ajustar a configuração ***Marcar mensagem como spam se o resultado for superior ou igual a*** digitando o valor (*50 a 90*) ou movendo o controle deslizante para a esquerda ou para a direita.

Veja uma análise geral do limite de pontuação:

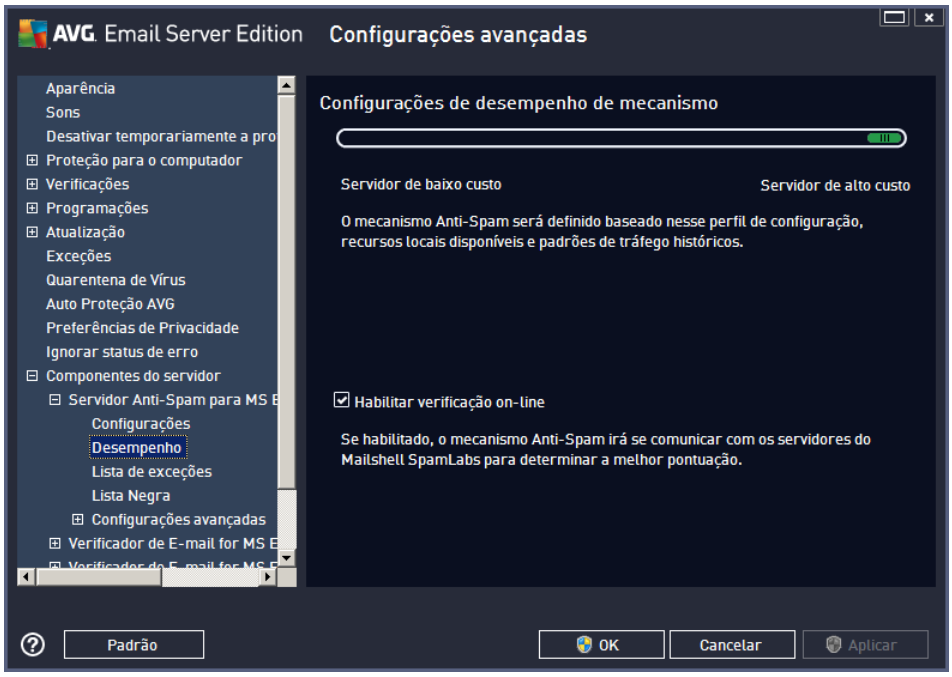
- ***Valor 90*** – a maioria das mensagens de email recebidas será entregue normalmente (sem ser marcada como spam. O spam mais facilmente identificado será filtrado, mas uma quantidade significativa de spam ainda não será bloqueada.
- ***Valor entre 80 e 89*** – as mensagens de email que parecem ser spam serão filtradas. Algumas mensagens que não são spam poderão ser bloqueadas incorretamente.
- ***Valor entre 60 e 79*** – uma configuração considerada bastante agressiva. As mensagens de email que provavelmente são spam serão filtradas. É provável que mensagens não spam também sejam bloqueadas
- ***Valor entre 50 e 59*** – Configuração muito agressiva. É provável que mensagens de email não spam sejam bloqueadas como verdadeiras mensagens spam. Esse intervalo limite não é recomendado para uso normal.

Você pode definir mais tarde como a mensagem de email com spam detectada deve ser tratada:

- ***Modificar assunto das mensagens marcadas como vírus*** – marque essa caixa de seleção se desejar que todas as mensagens detectadas como spam sejam marcadas com uma palavra ou um caractere específico no campo de assunto do email. O texto desejado pode ser digitado no campo de texto ativado.

- ***Perguntar antes de relatar detecção incorreta*** – caso, durante o processo de instalação, você tenha concordado em participar do Programa de Aprimoramento de Produto – esse programa nos ajuda a coletar informações atualizadas sobre as ameaças mais recentes de todos os participantes mundialmente e, em troca, podemos aprimorar a proteção para todos – ou seja, você permitiu o relato das ameaças detectadas à AVG. A geração de relatório é feita automaticamente. Entretanto, você pode marcar esta caixa de seleção para configurar que deseja que uma pergunta seja feita antes de relatar qualquer spam detectado à AVG, para ter certeza de que a mensagem deva realmente ser classificada como spam.

6.3.2. Desempenho



A caixa de diálogo ***Configurações de desempenho do mecanismo*** (*que pode ser acessada no link do item* ***Desempenho*** *do painel de navegação esquerdo*) oferece as configurações de desempenho do componente ***Anti-Spam***. Mova o controle deslizante para a esquerda ou para a direita para alterar o nível de intervalo de desempenho de verificação entre os modos ***Pouca memória***/***Alto desempenho***.

- ***Pouca memória*** – durante o processo de verificação para identificar spam, nenhuma regra será usada. Apenas os dados de treinamento serão usados para identificação. Esse modo não é recomendado para uso comum, a menos que o hardware do computador seja realmente fraco.

- ***Alto desempenho*** – este modo consumirá muita memória. Durante o processo de verificação para identificar um spam, os seguintes recursos serão usados: cache do banco de dados de regras e spam, regras básicas e avançadas, endereços IP de spam e

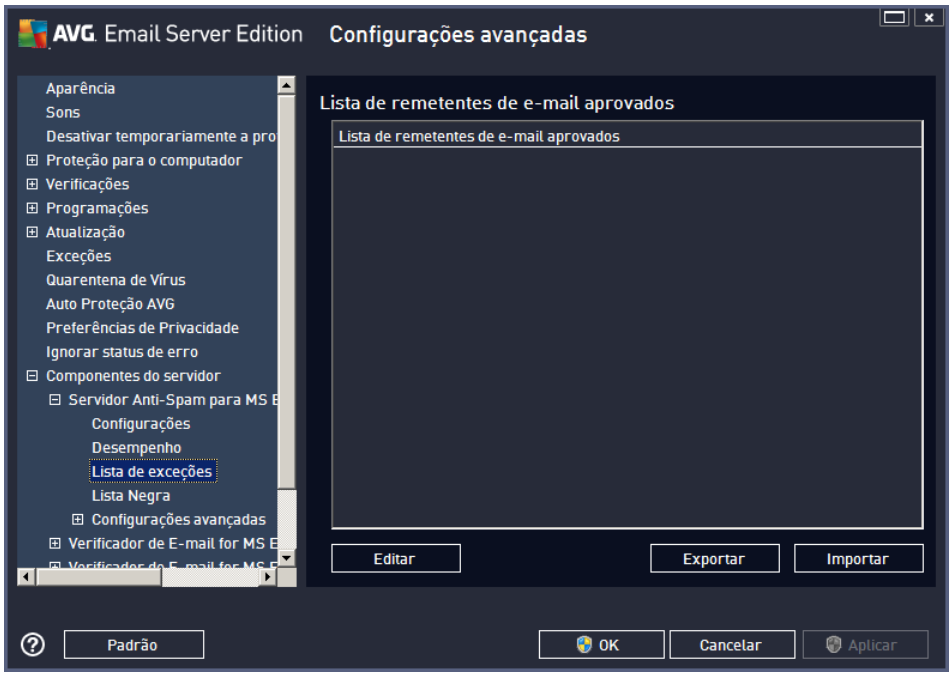
bancos de dados de spam.

O item ***Habilitar verificação online*** fica ativado por padrão. Isso resulta em uma detecção de spam mais precisa por meio da comunicação com os servidores Mailshell, ou seja, os dados verificados serão comparados com o banco de dados Mailshell on-line.

Geralmente é recomendável manter as configurações padrão e alterá-las somente se houver um motivo para isso. Alterações na configuração devem ser feitas somente por usuários experientes!

6.3.3. Lista de exceções

O item ***Lista de exceções*** abre uma caixa de diálogo com uma lista global de endereços de email e nomes de domínio de remetentes aprovados cujas mensagens nunca serão marcadas como spam.



Na interface de edição, você pode compilar uma lista dos remetentes sobre os quais tem certeza de que não enviarão mensagens indesejáveis (spam). Você pode também compilar uma lista de nomes de domínio completos (como *avg.com*) que você sabe que não gera mensagens de spam.

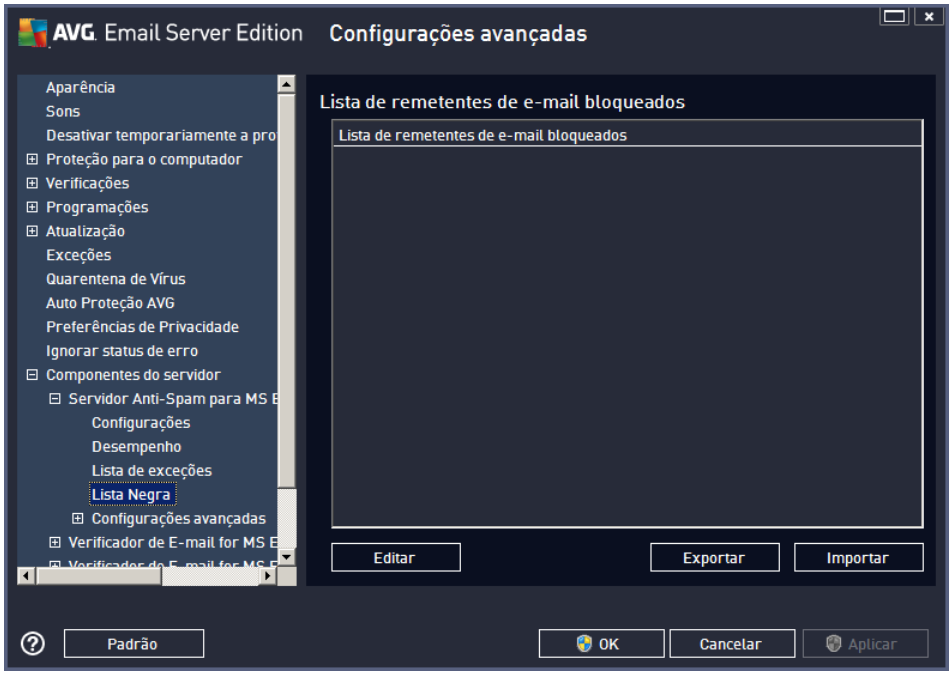
Depois de preparar essa lista de remetentes e/ou nomes de domínio, você poderá inseri-los digitando diretamente cada endereço de email ou importando toda a lista de endereços de uma vez. Os seguintes botões estão disponíveis:

- ***Editar*** – pressione este botão para abrir uma caixa de diálogo na qual é possível inserir manualmente uma lista de endereços (você pode usar *o método copiar/colar*). Insira um item (remetente, nome do domínio) por linha.
- ***Importar*** – você pode importar endereços de email existentes selecionando esse botão. O arquivo de entrada pode ser um arquivo de texto (em formato de texto simples e o conteúdo deve conter somente um item – endereço, nome de domínio – por linha), arquivo WAB ou a importação pode ser realizada a partir do Catálogo de endereços do Windows ou Microsoft Office Outlook.

- ***Exportar*** – se, por algum motivo, você decidir exportar os registros, será possível fazê-lo pressionando esse botão. Todos os registros serão salvos em um arquivo de texto simples.

6.3.4. Lista negra

O item ***Lista negra*** abre uma caixa de diálogo com uma lista global de endereços de email e nomes de domínio de remetentes bloqueados cujas mensagens sempre serão marcadas como spam.



Na interface de edição, você pode compilar uma lista dos remetentes que você espera que enviem mensagens indesejáveis (spam). Você pode também compilar uma lista de nomes de domínio completos (como *empresaqueenviaspam.com*), dos quais espera receber mensagens de spam. Todos os endereços de email/ domínios listados serão identificados como spam.

Depois de preparar essa lista de remetentes e/ou nomes de domínio, você poderá inseri-los digitando diretamente cada endereço de email ou importando toda a lista de endereços de uma vez. Os seguintes botões estão disponíveis:

- ***Editar*** – pressione este botão para abrir uma caixa de diálogo na qual é possível inserir manualmente uma lista de endereços (você pode usar *o método copiar/colar*). Insira um item (remetente, nome do domínio) por linha.

- ***Importar*** – você pode importar endereços de email existentes selecionando esse botão. O arquivo de entrada pode ser um arquivo de texto (em formato de texto simples e o conteúdo deve conter somente um item – endereço, nome de domínio – por linha), arquivo WAB ou a importação pode ser realizada a partir do Catálogo de endereços do Windows ou Microsoft Office Outlook.

- ***Exportar*** – se, por algum motivo, você decidir exportar os registros, será possível fazê-lo pressionando esse botão. Todos os registros serão salvos em um arquivo de texto simples.

6.3.5. Configurações Avançadas

Esta ramificação contém várias opções de configuração para o componente Anti-Spam. Essas configurações se destinam exclusivamente a usuários experientes, principalmente administradores de rede, que precisam configurar a proteção anti-spam em detalhes para melhor proteger os servidores de email. Por essa razão, não há ajuda adicional disponível para as caixas de diálogo individuais; entretanto, existe uma breve descrição de cada opção respectiva diretamente na interface do usuário.

É altamente recomendável não alterar as configurações, a menos que você esteja bastante familiarizado com todas as configurações avançadas do Spamcatcher (MailShell Inc.). Qualquer alteração inapropriada poderá resultar em mau desempenho ou no funcionamento incorreto do componente.

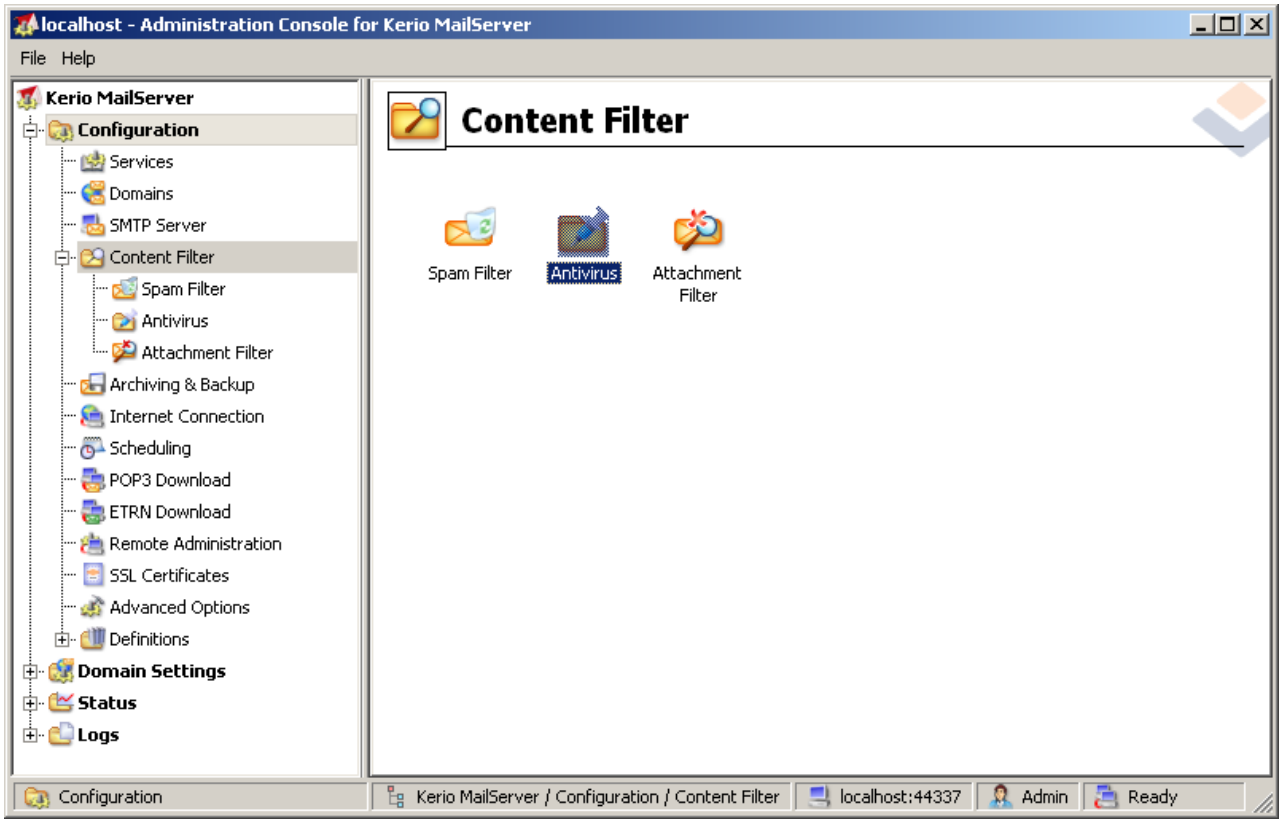
Se você ainda acredita que precisa alterar as configurações Anti-Spam no nível muito avançado, siga as instruções fornecidas diretamente na interface do usuário. Geralmente, em cada caixa de diálogo você encontrará um único recurso específico que poderá editar – sua descrição é sempre incluída na própria caixa.

- ***Filtragem*** – lista de idiomas, lista de países, IPs aprovados, IPs bloqueados, países bloqueados, conjunto de caracteres bloqueados, remetentes falsificados
- ***RBL*** – servidores RBL, vários acertos, limite, tempo limite, máximo de IPs
- ***Conexão com a Internet*** – tempo limite, servidor proxy, autenticação proxy

7. AVG para Kerio MailServer

7.1. Configuração

O mecanismo de proteção antivírus é integrado diretamente ao aplicativo Kerio MailServer. Para ativar a proteção de email do Kerio MailServer através do mecanismo de verificação AVG, inicie o aplicativo Kerio Administration Console. Na árvore de controle à esquerda da janela do aplicativo, escolha a sub-ramificação Filtro de Conteúdo na ramificação Configuração:

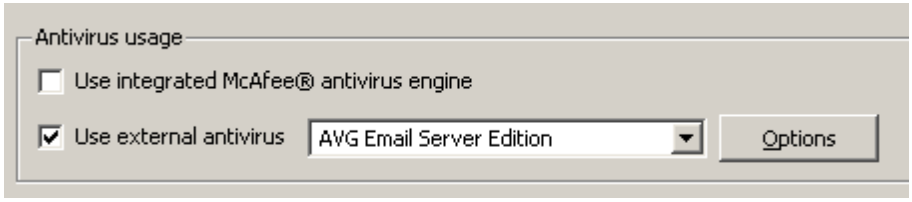


Se você clicar no item Filtro de conteúdo, aparecerá uma caixa de diálogo com três itens:

- ***Filtro de Spam***
- ***Antivírus*** (consulte a seção ***– Antivírus***)
- ***Filtro de Anexo*** (consulte a seção ***– Filtro de Anexo***)

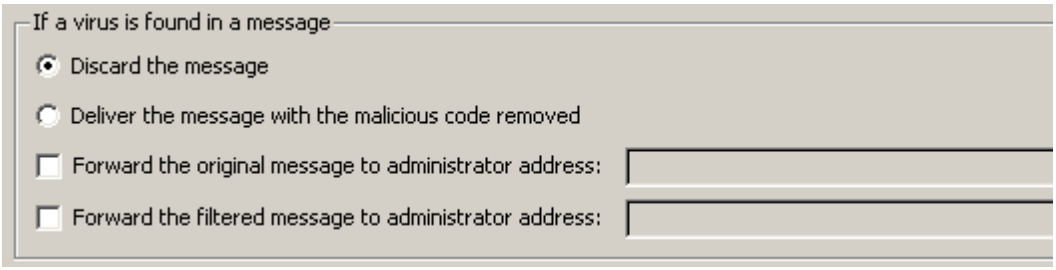
7.1.1. Antivírus

Para ativar o AVG para Kerio MailServer, marque a caixa de seleção Usar antivírus externo e escolha a edição do AVG Email Server Edition no menu de software externo no quadro Uso de antivírus da janela de configuração:



Na seguinte seção, você pode especificar o que fazer com um arquivo infectado ou mensagem filtrada:

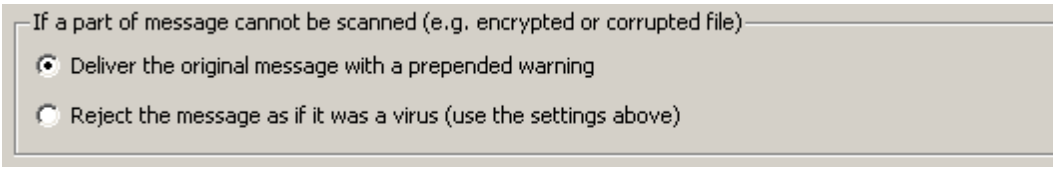
- ***Se um vírus for encontrado em uma mensagem***



Este quadro especifica a ação a ser executada quando um vírus é detectado em uma mensagem ou quando uma mensagem é filtrada por um filtro de anexo:

  - ***Descartar a mensagem*** – quando selecionada, a mensagem infectada ou filtrada será excluída.
  - ***Entregar a mensagem com o código mal-intencionado removido*** – quando selecionada, a mensagem será entregue ao destinatário, mas sem o anexo possivelmente prejudicial.
  - ***Encaminhar a mensagem original ao endereço do administrador*** – quando selecionada, a mensagem infectada com vírus será encaminhada ao endereço especificado no campo de texto de endereço.
  - ***Encaminhar a mensagem filtrada ao endereço do administrador*** – quando selecionada, a mensagem filtrada será encaminhada ao endereço especificado no campo de texto de endereço.

- ***Se não for possível verificar parte da mensagem (por exemplo, arquivo criptografado ou corrompido)***



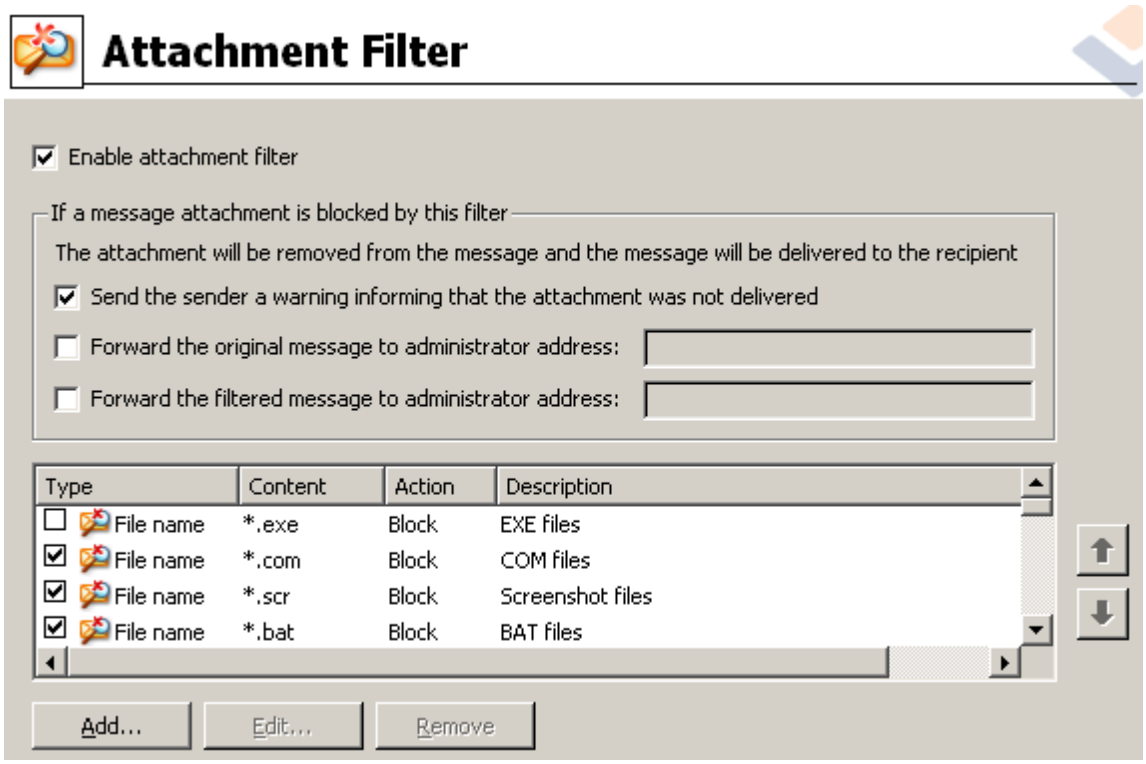
Este quadro especifica a ação a ser executada quando não é possível verificar parte da mensagem ou do anexo:

  - ***Entregar a mensagem original com um aviso preparado*** – a mensagem (ou anexo) será entregue desmarcada. O usuário será informado que a mensagem ainda contém vírus.
  - ***Recusar a mensagem como se fosse um vírus*** – o sistema reagirá da mesma forma que quando um vírus for detectado (isto é, a mensagem será entregue sem nenhum anexo ou será

recusada). Essa opção é segura, mas o envio de arquivos compactados protegidos com senha será praticamente impossível.

7.1.2. Filtro de anexo

No menu Filtro de anexo há uma lista de várias definições de anexos:



Para ativar ou desativar a filtragem de anexos de email, marque a caixa de seleção Ativar filtro de anexo. Se preferir, altere as seguintes configurações:

- ***Enviar um aviso ao remetente informando que o anexo não foi entregue***

  O remetente receberá um aviso do Kerio MailServer informando que ele enviou uma mensagem com vírus ou anexo bloqueado.

- ***Encaminhar a mensagem original ao endereço do administrador***

  A mensagem será encaminhada (no estado em que se encontra – com o anexo infectado ou proibido) a um endereço de email definido, independentemente de se tratar de um endereço local ou externo.

- ***Encaminhar a mensagem filtrada ao endereço do administrador***

  A mensagem, sem seu anexo infectado ou proibido, será (além das ações selecionadas abaixo) encaminhada ao endereço de email especificado. Esta opção poderá ser usada para verificar o funcionamento correto do antivírus e/ou filtro de anexo.

Na lista de extensões, cada item tem quatro campos:

- ***Tipo*** – especificação do tipo de anexo determinado pela extensão atribuída no campo Conteúdo. Os

tipos possíveis são Nome do arquivo ou Tipo de MIME. Selecione a respectiva caixa neste campo para incluir/excluir o item da filtragem de anexo.

- ***Conteúdo*** – é possível especificar aqui uma extensão a ser filtrada. Use os curingas do sistema operacional aqui (por exemplo, a string '*.doc.* indica qualquer arquivo com a extensão .doc).

- ***Ação*** – defina a ação a ser executada com o anexo específico. As possíveis ações são Aceitar (aceitar o anexo) e Bloquear (uma ação será executada conforme definido abaixo na lista de anexos desativados).

- ***Descrição*** – a descrição do anexo é definida neste campo.

Para remover um item da lista, pressione o botão Remover. Para adicionar outro item à lista, pressione o botão ***Adicionar...***. Se preferir, edite um registro existente pressionando o botão Editar.... A janela a seguir é exibida:

- No campo Descrição, você pode inserir uma pequena descrição do anexo a ser filtrado.

- No campo Se um email contiver um anexo em que, selecione o tipo de anexo (Nome do arquivo ou Tipo de MIME). Também é possível escolher uma determinada extensão na lista de extensões oferecidas ou digitar o curinga da extensão diretamente.

No campo Então, especifique se deseja bloquear ou aceitar o anexo definido.

8. Perguntas frequentes e suporte técnico

Se você tiver algum problema com o seu , seja comercial ou técnico, consulte a seção ***Perguntas Freqüentes*** do site da AVG em http://www.avg.com.

Caso não consiga obter ajuda dessa forma, contate o departamento de suporte técnico por email. Use o formulário de contato que pode ser acessado do menu do sistema via ***Ajuda/Obter ajuda online***.