AVG Email Server Edition 2013

Manual do Utilizador

Revisão do documento 2013.01 (20.11.2012)

Índice

1. Introdução

Este manual do utilizador disponibiliza informação completa para o **AVG Email Server Edition 2013**.

Parabéns pela sua aquisição do AVG Email Server Edition 2013!

O **AVG Email Server Edition 2013** é um entre um leque de premiados produtos AVG desenvolvidos para lhe proporcionar descanso e segurança absoluta para o seu servidor. Como todos os produtos AVG, o **AVG Email Server Edition 2013** foi completamente redesenhado, de raiz, para proporcionar a renomeada e acreditada proteção de segurança de uma forma nova, mais fácil de utilizar e mais eficiente.

O AVG foi concebido e desenvolvido para proteger o seu computador e atividade de rede. Desfrute da experiência da proteção total do AVG.

Nota: *esta documentação contém descrições de funcionalidades específicas da versão Email Server Edition. Se precisar de informações sobre outras funcionalidades AVG, consulte o manual do utilizador da versão Internet Security, que contém todas as informações necessárias. Pode transferir o manual a partir de http://www.avg.com.*

2. Requisitos de Instalação do AVG

2.1. Sistemas Operativos Suportados

O **AVG Email Server Edition 2013** destina-se a proteger servidores de correio em execução nos seguintes sistemas operativos:

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

2.2. Servidores de E-mail Suportados

São suportados os seguintes servidores de correio:

- MS Exchange 2003 Server
- MS Exchange 2007 Server
- MS Exchange 2010 Server
- Kerio MailServer – versão 6.7.2 e superiores

2.3. Requisitos de Hardware

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

- Intel Pentium CPU 1,5 GHz
- 500 MB de espaço livre no disco rígido (para propósitos de instalação)
- 512 MB de memória RAM

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

- Intel Pentium CPU 1,8 GHz
- 600 MB de espaço livre no disco rígido (para propósitos de instalação)
- 512 MB de memória RAM

2.4. Desinstalar Versões Anteriores

Se possuir uma versão anterior do AVG Email Server instalada, precisará de a desinstalar manualmente antes de instalar o **AVG Email Server Edition 2013**. Deve desinstalar manualmente a versão anterior através das funcionalidades tradicionais do Windows.

- A partir do menu ***Iniciar/Definições/Painel de Controlo/Adicionar ou Remover Programas***, selecione o programa pretendido na lista de software instalado (pode também proceder à desinstalação

de uma forma ainda mais fácil, através do menu ***Iniciar/Todos os programas/AVG/Desinstalar o AVG***).

- Se tiver usado o AVG 8.x ou uma versão anterior, não se esqueça de desinstalar também os plug-ins individuais do servidor.

  Nota: *será necessário reiniciar o serviço store durante o processo de desinstalação.*

  Plug-in Exchange – execute o ficheiro setupes.exe com o parâmetro /uninstall a partir da pasta onde o plug-in foi instalado.

  ex., C:\AVG4ES2K\setupes.exe /uninstall

  Plug-in Lotus Domino/Notes – execute o ficheiro setupln.exe com o parâmetro /uninstall a partir da pasta onde o plug-in foi instalado.

  ex., C:\AVG4LN\setupln.exe /uninstall

2.5. Service Packs do MS Exchange

Para o Exchange 2003 Server não é necessário nenhum pacote de serviço adicional; no entanto, recomenda-se que mantenha o sistema atualizado com os pacotes de serviço e correções mais recentes, de modo a obter a máxima segurança disponível.

Service Pack para MS Exchange 2003 Server (opcional):

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

No início da configuração, todas as versões das bibliotecas do sistema serão examinadas. Se for necessário instalar novas bibliotecas, o programa de instalação mudará o nome das versões anteriores com a extensão . delete. Estas versões serão eliminadas depois de o sistema reiniciar.

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

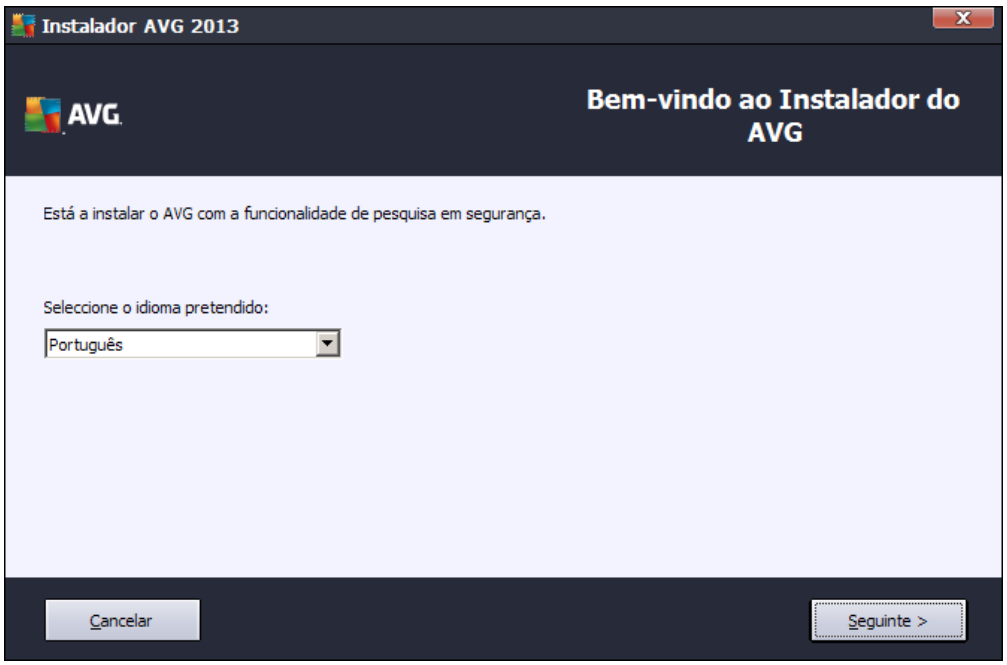
Para instalar o AVG no seu computador, precisa de obter o mais recente ficheiro de instalação. Pode utilizar o ficheiro de instalação a partir do CD facultado na caixa da sua edição, mas esse ficheiro pode estar desatualizado. Como tal, recomendamos que obtenha o ficheiro de instalação mais recente online. Pode transferir o ficheiro a partir do Website da AVG (em http://www.avg.com/download?prd=msw).

Existem dois pacotes de instalação disponíveis para o seu produto – para sistemas operativos de 32 bits (marcado como x86) e para sistemas operativos de 64 bits (marcado como x64). Certifique-se de que utiliza o pacote de instalação correto para o seu sistema operativo específico.

Durante o processo de instalação, ser-lhe-á solicitado o número de licença. Certifique-se de que o mesmo está disponível antes de iniciar a instalação. O número pode ser encontrado na embalagem do CD. Se tiver adquirido a sua cópia do AVG online, o número de licença foi-lhe enviado por e-mail.

Assim que tiver transferido e guardado o ficheiro de instalação no seu disco rígido, pode iniciar o processo de instalação. A instalação é uma sequência de janelas com uma breve descrição do que deve fazer em cada passo. De seguida facultamos uma explicação para cada janela:

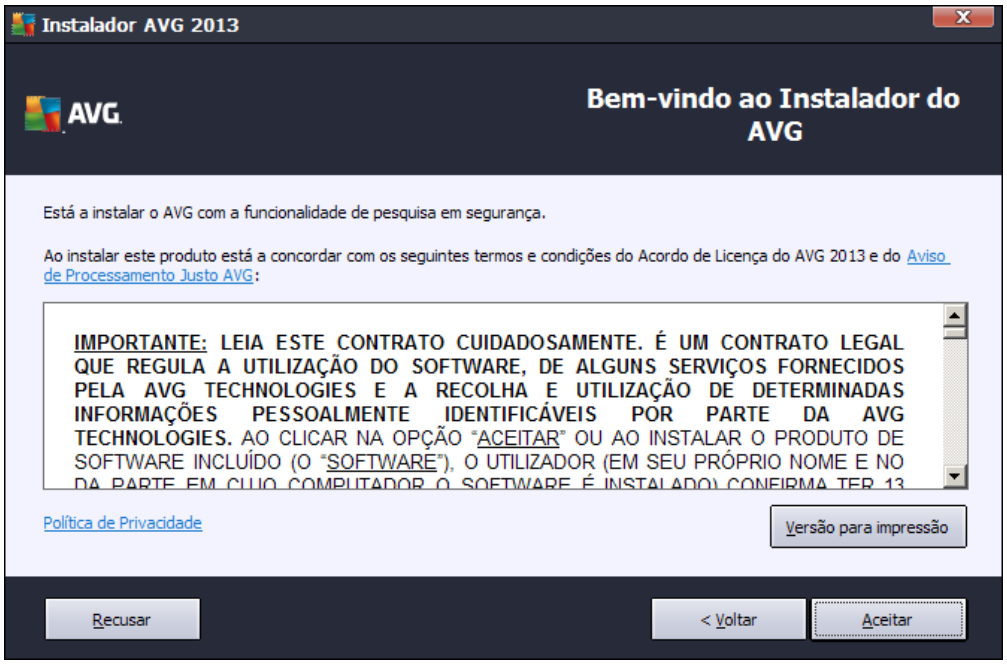
3.1. Execução da Instalação



O processo de instalação inicia com a janela ***Bem-vindo***. Nesta janela pode selecionar o idioma utilizado no processo de instalação e clicar no botão ***Seguinte***.

Poderá escolher também idiomas adicionais para a interface da aplicação mais tarde durante o processo de instalação.

3.2. Contrato de Licença

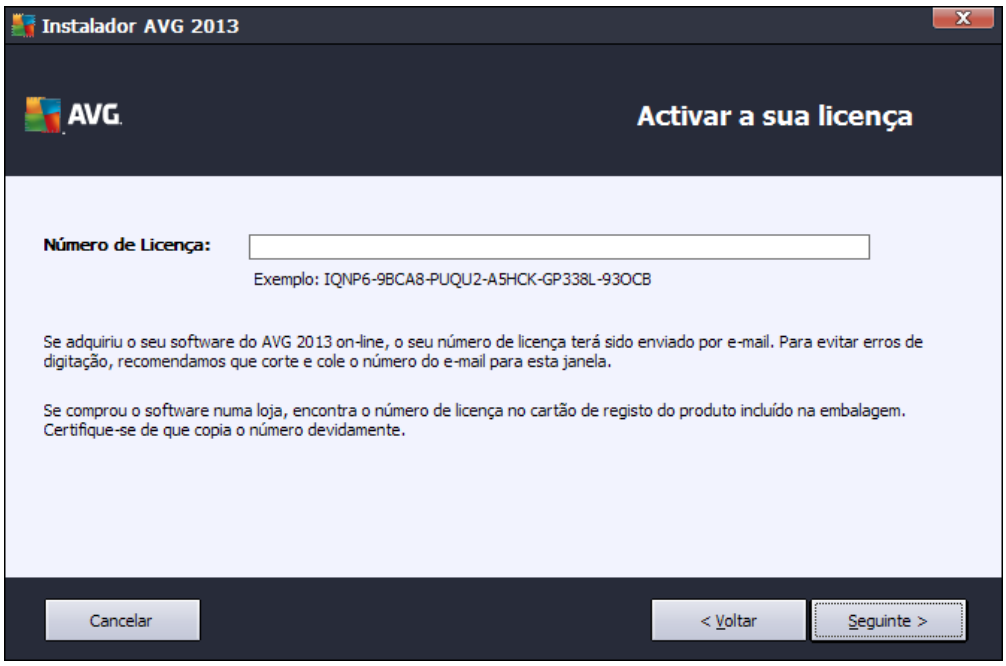


Nesta janela pode ler as condições de licenciamento. Utilize o botão ***Versão para impressão*** para abrir o texto da licença numa nova janela. Clique no botão ***Aceitar*** para confirmar e continuar para a janela seguinte.

3.3. Ativar a sua licença

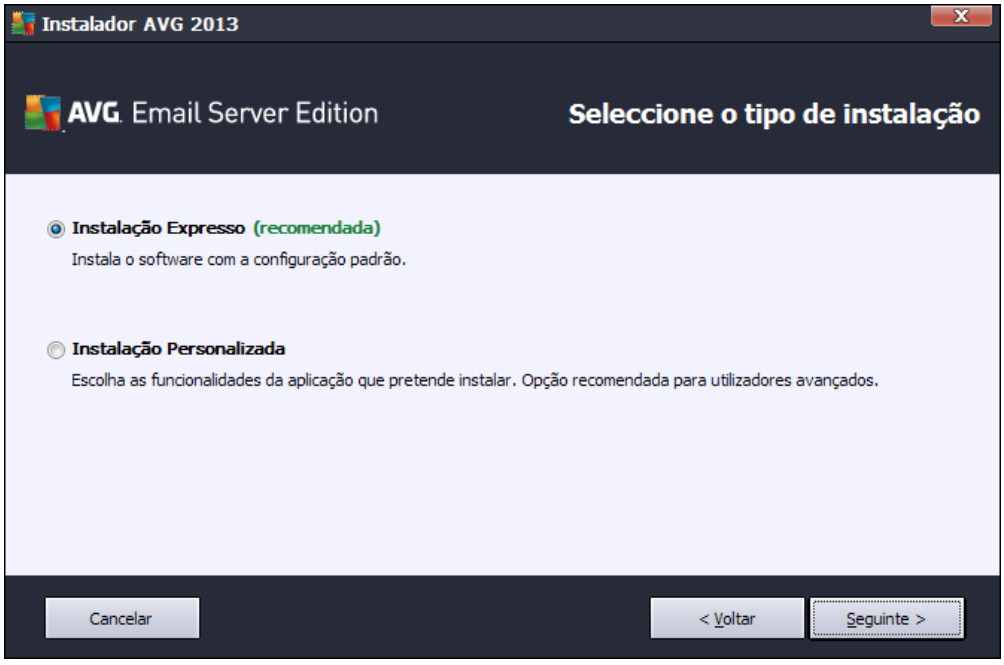
Na janela ***Ativar a sua licença*** tem de preencher o seu número de licença.

Introduza o seu número de licença no campo de texto ***Número de Licença***. O número de licença estará no e-mail de confirmação que recebeu depois de comprar o seu AVG online. Tem de digitar o número exatamente conforme apresentado. Se o formulário digital do número de licença estiver disponível (na mensagem de e-mail), é recomendável que utilize o método copiar e colar para o inserir.



Clique no botão ***Seguinte*** para continuar o processo de instalação.

3.4. Selecionar Tipo de Instalação



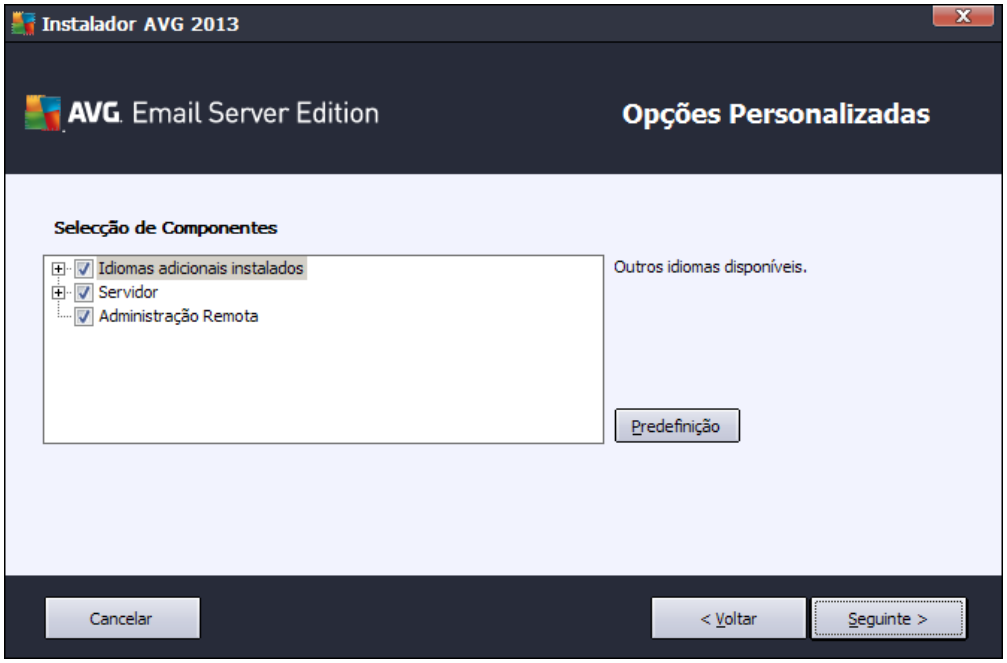
A janela ***Selecione o tipo de instalação*** disponibiliza duas opções de instalação: ***Instalação Expresso*** e ***Instalação Personalizada***.

Para a maioria dos utilizadores, é recomendável a ***Instalação Expresso***, que instala o AVG em modo totalmente automático com as definições predefinidas pelo fornecedor do programa. Esta configuração proporciona a segurança máxima combinada com uma utilização de recursos otimizada. Futuramente, se houver necessidade de alterar a configuração, tem sempre a possibilidade de o fazer diretamente na aplicação AVG.

A ***Instalação Personalizada*** só deve ser utilizada por utilizadores avançados que tenham uma razão válida para instalar o AVG com definições que não as padrão; ex. para corresponder a requisitos do sistema específicos.

Se selecionar a Instalação Personalizada, aparece a secção ***Pasta de destino*** na parte inferior da janela. Essa secção permite especificar a localização na qual pretende instalar o AVG. O AVG será instalado por predefinição na pasta de ficheiros de programas localizada na unidade C:. Se quiser alterar esta localização, utilize o botão ***Procurar*** para visualizar a estrutura da unidade e selecione a pasta respetiva.

3.5. Instalação Personalizada – Opções Personalizadas



A secção ***Seleção de Componentes*** apresenta uma síntese de todos os componentes do AVG que podem ser instalados. Se as definições predefinidas não forem da sua conveniência, pode remover/adicionar componentes específicos.

No entanto, só pode selecionar entre os componentes que estão incluídos na edição do AVG que adquiriu. Só esses componentes serão facultados para instalação na janela de Seleção de Componentes!

- ***Administração Remota*** – se pretender conectar o AVG a um Centro de Dados AVG (Edições de Rede do AVG), é necessário selecionar esta opção.

- ***Idiomas adicionais instalados*** – pode definir o(s) idioma(s) em que o AVG deverá ser instalado. Marque o item ***Idiomas adicionais instalados*** e depois selecione os idiomas pretendidos a partir do respetivo menu.

Síntese simplificada dos componentes individuais do servidor (no ramo ***Servidor***):

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

  Verifica todas as mensagens de e-mail a receber e assinala o correio não solicitado como SPAM. Utiliza vários métodos de análise para processar cada mensagem de e-mail, oferecendo o máximo de proteção possível contra mensagens de e-mail indesejadas.

- ***Verificador de E-mail para o MS Exchange (routing Transport Agent)***

  Verifica todas as mensagens de e-mail de entrada, de saída e internas que passam pela função MS Exchange HUB.

- ***Verificador de E-mail para o MS Exchange (SMTP Transport Agent)***

  Verifica todas as mensagens de e-mail que passam pela interface de SMTP do MS Exchange (pode ser instalado para as funções EDGE e HUB).

- ***Verificador de E-mail para o MS Exchange (VSAPI)***

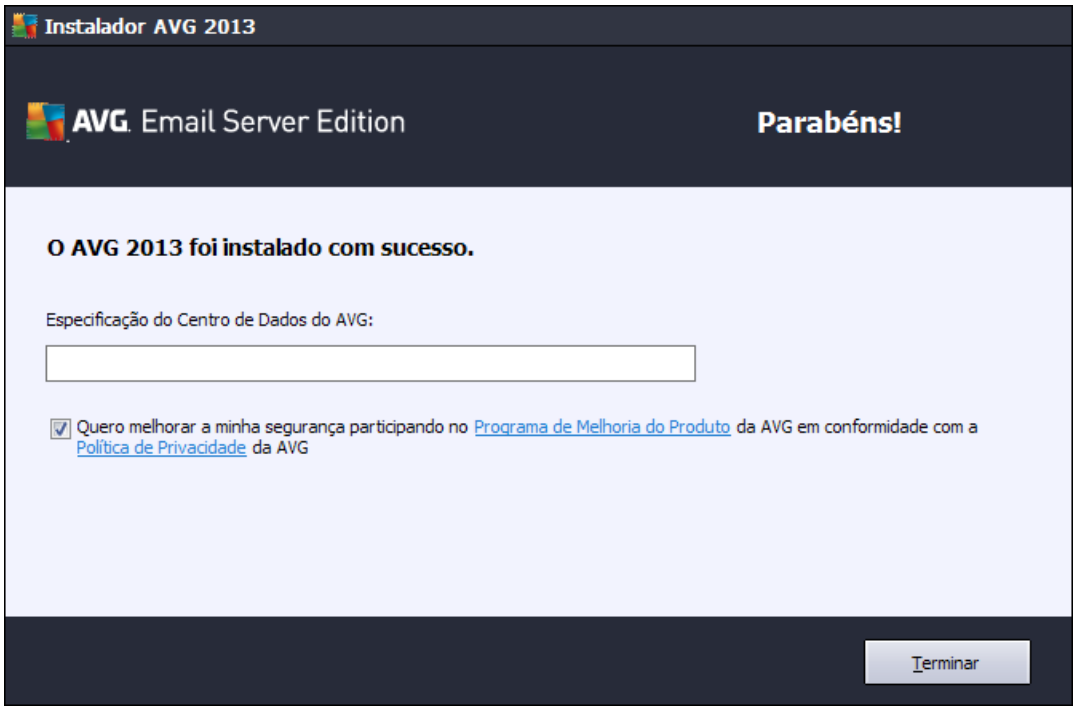
  Verifica todas as mensagens de e-mail guardadas nas caixas de correio dos utilizadores. Se for detetado algum vírus, será movido para a Quarentena de Vírus ou removido na totalidade.

Para os utilizadores do Exchange 2003, apenas estão disponíveis os componentes Anti-Spam e Verificador de E-mail (VSAPI).

Continue clicando no botão ***Seguinte***.

3.6. Conclusão da Instalação

Se tiver selecionado o módulo ***Administração Remota*** durante a seleção de módulos, pode definir neste ecrã a cadeia de caracteres de ligação ao seu Centro de Dados AVG.



Nesta janela pode também decidir se pretende participar no Programa de Melhoria do Produto, que recolhe informações anónimas sobre as ameaças detetadas para aumentar o nível de segurança geral da Internet. Se concordar com esta declaração, mantenha a opção ***Quero melhorar a minha segurança participando no Programa de Melhoria do Produto da AVG em conformidade com a Política de Privacidade da AVG*** marcada *(a opção está confirmada por predefinição)*.

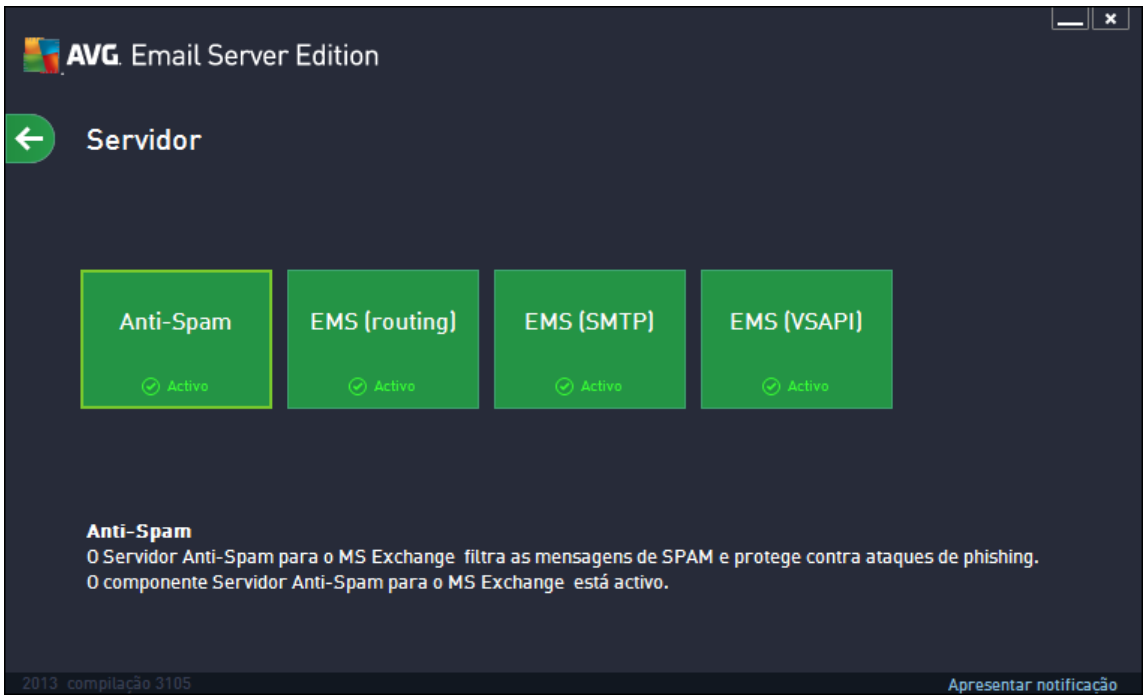
Confirme as suas escolhas clicando no botão **Terminar**.

O AVG está agora instalado no seu computador e totalmente funcional. O programa está em execução em segundo plano em modo completamente automático.

4. Após a Instalação

Imediatamente após a conclusão da instalação, aparece o ecrã principal do ***AVG Email Server Edition 2013***:

Este manual inclui apenas as funcionalidades específicas do ***AVG Email Server Edition 2013***; todos os outros componentes e definições são descritos no manual do AVG Desktop. Para aceder à janela dos componentes principais de servidor, clique no botão ***Servidor***. Será apresentado o seguinte ecrã:



Tenha em atenção que todos os componentes de servidor ficarão disponíveis (a não ser, obviamente, que opte por não instalar alguns dos componentes durante o processo de instalação) apenas se utilizar o MS Exchange 2007 ou uma versão superior. O MS Exchange 2003 suporta apenas os componentes Anti-Spam e Verificador de E-mail (VSAPI).

Para configurar individualmente a proteção do seu servidor de correio, consulte a secção correspondente:

- ***Verificadores de E-mail para o MS Exchange***
- ***Servidor Anti-Spam para o MS Exchange***
- ***AVG para Kerio MailServer***

5. Verificadores de E-mail para o MS Exchange

5.1. Síntese

Síntese simplificada dos componentes individuais do servidor do Verificador de E-mail:

- ***EMS (routing) – Verificador de E-mail para o MS Exchange (routing Transport Agent)***

  Verifica todas as mensagens de e-mail de entrada, de saída e internas que passam pela função MS Exchange HUB.

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

- ***EMS (SMTP) – Verificador de E-mail para o MS Exchange (SMTP Transport Agent)***

  Verifica todas as mensagens de e-mail que passam pela interface de SMTP do MS Exchange.

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

- ***EMS (VSAPI) – Verificador de E-mail para o MS Exchange (VSAPI)***

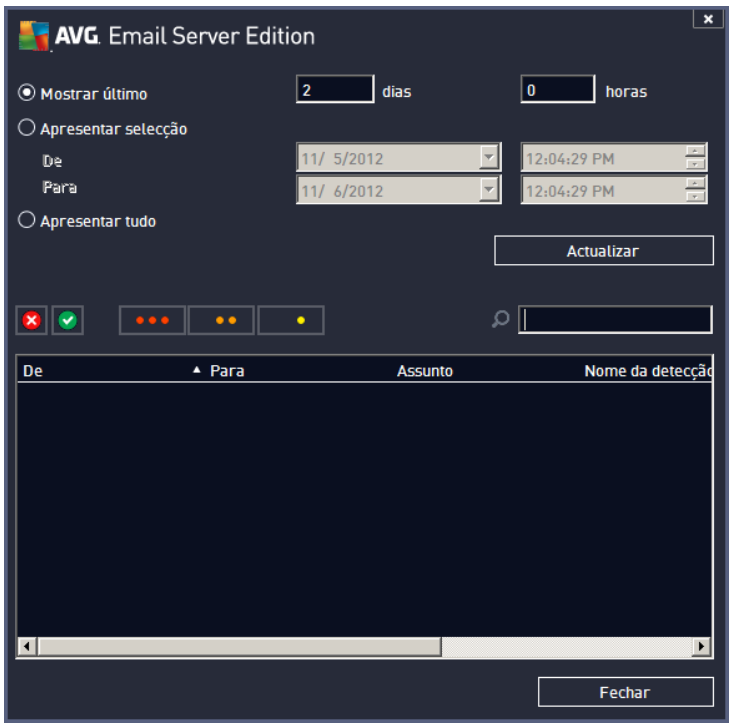
  Verifica todas as mensagens de e-mail guardadas nas caixas de correio dos utilizadores. Se for detetado algum vírus, será movido para a Quarentena de Vírus ou removido na totalidade.

Clique no ícone de um componente necessário para abrir a interface. Todos os componentes partilham os seguintes botões de controlo e as seguintes ligações comuns:

- ***ATIVADO/DESATIVADO*** – clicar neste botão permite ativar/desativar o componente selecionado (se o componente estiver ativado, o botão e o texto ficam com cor verde; se o componente estiver desativado, ficam com cor vermelha).

- ***Resultados da Análise***

  Abre uma nova janela onde pode rever os resultados da análise:



  Aqui, pode verificar mensagens divididas em vários separadores de acordo com o nível de gravidade. Consulte a configuração dos componentes individuais para corrigir a gravidade e reportação.

  Por predefinição, só são apresentados os resultados dos dois últimos dias. Pode alterar o período apresentado através da alteração das seguintes opções:

  o ***Mostrar último*** – insira os dias e as horas pretendidas.

  o ***Apresentar seleção*** – escolha uma hora pretendida e um intervalo de datas.

  o ***Apresentar tudo*** – apresenta resultados para todo o período.

  Utilize o botão ***Atualizar*** para recarregar os resultados.

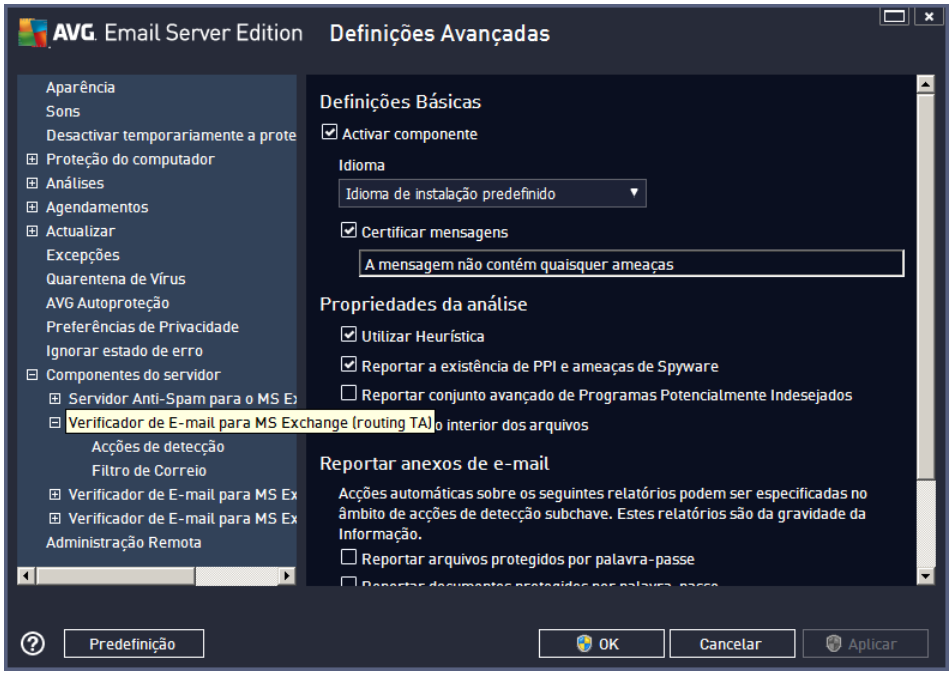
- ***Atualizar valores estatísticos*** – atualiza as estatísticas apresentadas acima.

Se clicar no botão ***Definições***, aparece um ecrã de definições avançadas relativas ao componente selecionado (pode encontrar mais informações sobre definições individuais de todos os componentes nos capítulos seguintes).

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

Para aceder às definições do ***Verificador de E-mail para o MS Exchange (routing Transport Agent)***, selecione o botão ***Definições*** na interface do componente.

Na lista de ***Componentes do servidor***, selecione o item ***Verificador de E-mail para o MS Exchange (routing TA)***:



A secção ***Definições Básicas*** contém as seguintes opções:

- ***Ativar componente*** – desmarque para desativar o componente.
- ***Idioma*** – selecione o idioma pretendido para o componente.
- ***Certificar mensagens*** – marque esta opção se quiser adicionar uma nota de certificação a todas as mensagens analisadas. Pode personalizar a mensagem no campo seguinte.

A secção ***Propriedades da análise***:

- ***Utilizar Heurística*** – marque esta caixa para ativar o método de análise heurística durante a análise.
- ***Reportar a existência de Programas Potencialmente Indesejados e ameaças de Spyware*** – marque esta opção para reportar a presença de programas potencialmente indesejados e spyware.
- ***Reportar conjunto avançado de Programas Potencialmente Indesejados*** – marque para detetar pacotes alargados de spyware: programas que são perfeitamente seguros quando adquiridos diretamente ao fabricante, mas que podem ser usados para propósitos maliciosos posteriormente, ou programas que são sempre seguros mas que podem ser indesejados (barras de ferramentas, etc.). Esta é uma medida adicional que aumenta o conforto e segurança do seu computador ainda mais; no entanto, pode potencialmente bloquear programas legais e está, como tal, desativada por predefinição. Nota: esta funcionalidade de deteção é um complemento da opção anterior, portanto, se quiser

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

- ***Pesquisa no interior dos arquivos*** – marque esta opção para permitir que o verificador analise também no interior de arquivos (zip, rar, etc.).

A secção ***Reportação de anexos de e-mail*** permite-lhe escolher os itens que deverão ser reportados durante a análise. Se marcada, cada e-mail com itens deste tipo conterá a etiqueta [INFORMAÇÃO] no assunto da mensagem. Esta é a configuração predefinida que pode ser facilmente corrigida na secção ***Ações de deteção*** , opção ***Informação*** (ver abaixo).

Estão disponíveis as seguintes opções:

- ***Reportar arquivos protegidos por palavra-passe***
- ***Reportar documentos protegidos por palavra-passe***
- ***Reportar ficheiros que contêm macros***
- ***Reportar extensões ocultas***

Também estão disponíveis os seguintes itens secundários na seguinte estrutura de árvore:

- ***Ações de deteção***
- ***Filtro de correio***

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

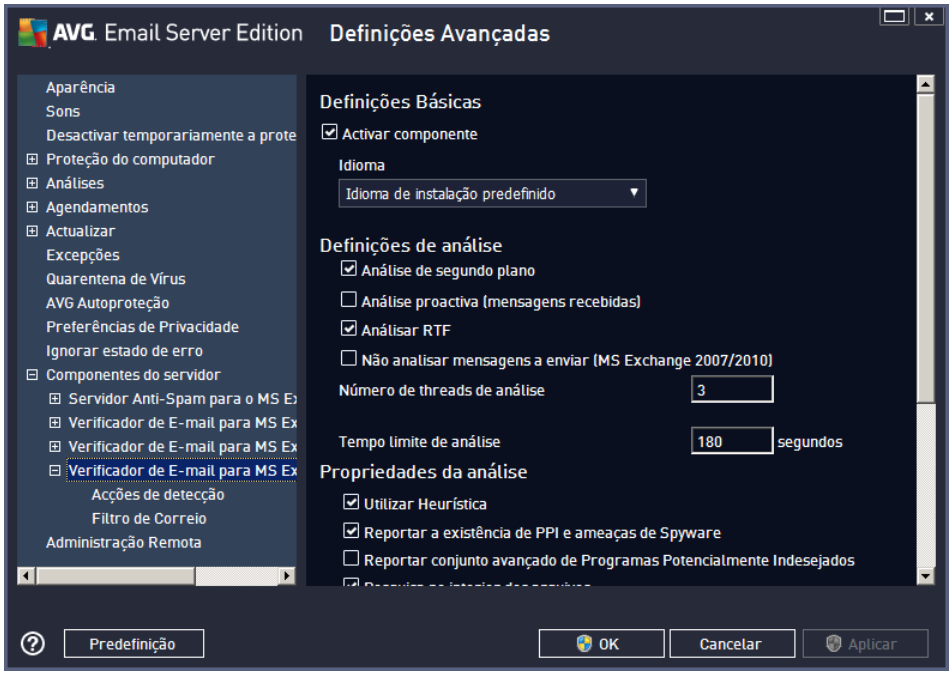
A configuração do ***Verificador de E-mail para o MS Exchange (SMTP Transport Agent)*** é exatamente a mesma que para o Routing Transport Agent. Para mais informações, consulte a secção ***Verificador de E-mail para o MS Exchange (routing TA)*** acima.

Também estão disponíveis os seguintes itens secundários na seguinte estrutura de árvore:

- ***Ações de deteção***
- ***Filtro de correio***

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

Este item contém definições do ***Verificador de E-mail para o MS Exchange (VSAPI)***.



A secção ***Definições Básicas*** contém as seguintes opções:

- ***Ativar componente*** – desmarque para desativar o componente.
- ***Idioma*** – selecione o idioma pretendido para o componente.

A secção ***Definições de análise***:

- ***Análise em Segundo Plano*** – pode ativar ou desativar o processo de análise em segundo plano. A análise em segundo plano é uma das funcionalidades da interface da aplicação VSAPI 2.0/2.5. Permite a análise por tópicos das Bases de Dados de Mensagens do Exchange. Sempre que for encontrado um item que não tenha sido analisado com as mais recentes atualizações da base de dados de vírus nas pastas da caixa de correio do utilizador, será enviado ao AVG para Exchange Server para ser analisado. A análise e a procura de objetos não examinados são executadas em paralelo.

  É usada uma classificação de prioridade baixa específica para cada base de dados, o que assegura que outras tarefas (ex. armazenamento de mensagens de correio eletrónico na base de dados do Microsoft Exchange) são sempre executadas prioritariamente.

- ***Análise Pró-ativa (mensagens de entrada)***

  Pode ativar ou desativar a função de análise pró-ativa do VSAPI 2.0/2.5 aqui. Esta análise ocorre quando um item é entregue numa pasta sem o pedido ter sido feito pelo cliente.

  Assim que as mensagens são submetidas para o Exchange, entram na fila de análise global com prioridade baixa (máximo de 30 itens). São analisadas numa base de primeiro a entrar, primeiro a sair (FIFO). Se um item for acedido enquanto ainda estiver na fila, é passado para prioridade alta.

As mensagens que excedam o número limite continuarão para o Exchange sem serem analisadas.

Mesmo que desative a ***Análise em Segundo Plano*** e a ***Análise Pró-ativa***, a análise aquando do acesso estará ativa quando o utilizador tentar transferir uma mensagem com o cliente MS Outlook.

- ***Analisar RTF*** – permite especificar se o tipo de ficheiro RTF deve ou não ser analisado.
- ***Não analisar mensagens a enviar (MS Exchange 2007/2010)*** – com ambos os componentes VSAPI e Routing Transport Agent (routing TA) instalados (não é relevante se é no mesmo servidor ou em dois servidores), o correio a enviar pode ser analisado duas vezes. A primeira análise é feita pelo verificador de acesso VSAPI, enquanto que a segunda é feita pelo Routing Transport Agent. Isso pode levar a alguma lentidão do servidor e atrasos relativos no envio de e-mails. Se tem a certeza de que tem ambos os componentes instalados e ativos, pode evitar esta dupla verificação do correio a enviar marcando esta caixa e desativando o verificador de acesso VSAPI.
- ***Número de Tópicos da Análise*** – por predefinição, a análise é processada por tópicos para aumentar o desempenho global da análise através de um certo nível de paralelismo. Neste campo, pode alterar a contagem dos tópicos.

  O número de tópicos predefinido é igual a 2 vezes o "número de processadores" + 1.

  O número mínimo de tópicos é computado como ('número de processadores'+1) dividido por 2.

  O número máximo de tópicos é computado como 'Número de processadores' multiplicado por 5 + 1.

  Se o valor for equivalente ao mínimo ou inferior, ou ao máximo ou superior, será usado o valor predefinido.

- ***Tempo Limite da Análise*** – o intervalo contínuo máximo (em segundos) para que um tópico aceda à mensagem que está a ser analisada (o valor predefinido é 180 segundos).

A secção ***Propriedades da análise***:

- ***Utilizar Heurística*** – marque esta caixa para ativar o método de análise heurística durante a análise.
- ***Reportar a existência de Programas Potencialmente Indesejados e ameaças de Spyware*** – marque esta opção para reportar a presença de programas potencialmente indesejados e spyware.
- ***Reportar conjunto avançado de Programas Potencialmente Indesejados*** – marque para detetar pacotes alargados de spyware: programas que são perfeitamente seguros quando adquiridos diretamente ao fabricante, mas que podem ser usados para propósitos maliciosos posteriormente, ou programas que são sempre seguros mas que podem ser indesejados (barras de ferramentas, etc.). Esta é uma medida adicional que aumenta o conforto e segurança do seu computador ainda mais; no entanto, pode potencialmente bloquear programas legais e está, como tal, desativada por predefinição. Nota: esta funcionalidade de deteção é um complemento da opção anterior, portanto, se quiser proteção contra os tipos básicos de spyware, mantenha sempre a caixa anterior marcada.
- ***Pesquisa no interior dos arquivos*** – marque esta opção para permitir que o verificador analise também no interior de arquivos (zip, rar, etc.).

A secção ***Reportação de anexos de e-mail*** permite-lhe escolher os itens que deverão ser reportados durante

a análise. A configuração predefinida pode ser facilmente corrigida na secção ***Ações de deteção***, opção ***Informação*** (ver abaixo).

Estão disponíveis as seguintes opções:

- ***Reportar arquivos protegidos por palavra-passe***
- ***Reportar documentos protegidos por palavra-passe***
- ***Reportar ficheiros que contêm macros***
- ***Reportar extensões ocultas***

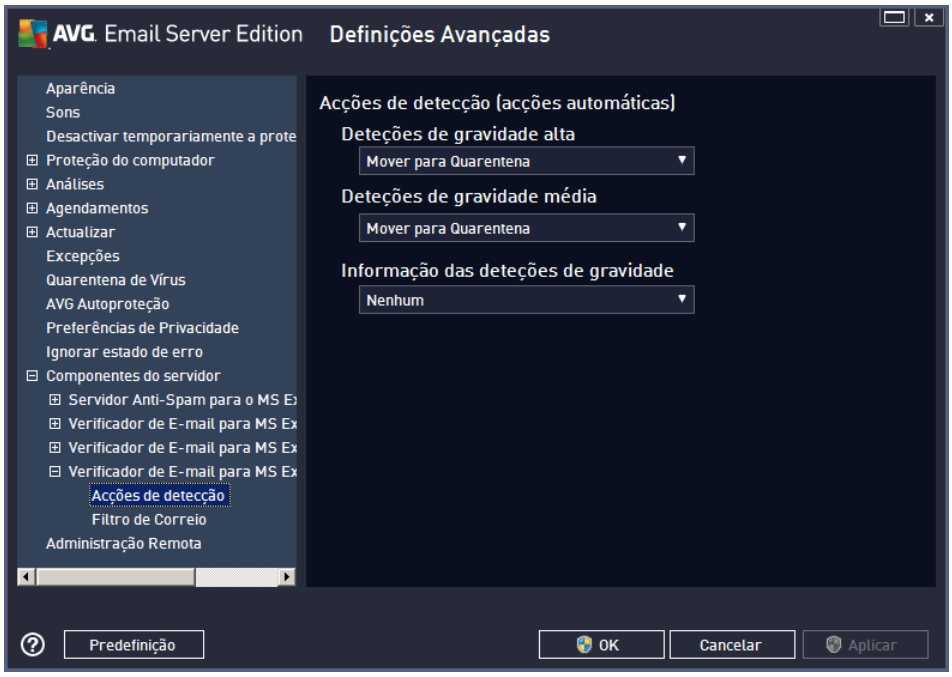
Regra geral, algumas destas funcionalidades são extensões do utilizador dos serviços da interface da aplicação Microsoft VSAPI 2.0/2.5. Para obter informações detalhadas sobre o VSAPI 2.0/2.5, aceda a uma das seguintes hiperligações (e também às hiperligações acessíveis a partir das indicadas):

- http://support.microsoft.com/default.aspx?scid=kb;en-us;328841&Product=exch2k – para mais informações sobre o Exchange e interação com software antivírus.
- http://support.microsoft.com/default.aspx?scid=kb;en-us;823166 – para mais informações sobre funcionalidades adicionais do VSAPI 2.5 na aplicação Exchange 2003 Server.

Também estão disponíveis os seguintes itens secundários na seguinte estrutura de árvore:

- ***Ações de deteção***
- ***Filtro de correio***

5.5. Ações de deteção



No item secundário ***Ações de deteção***, pode escolher ações automáticas que deverão ser executadas durante o processo de análise.

As ações estão disponíveis para os seguintes itens:

- ***Deteções de gravidade alta*** – códigos maliciosos que se copiam e disseminam, normalmente despercebidos até o mal estar feito.
- ***Deteções de gravidade média*** – programas que, regra geral, variam de positivamente graves para meras ameaças potenciais à sua privacidade.
- ***Deteções de gravidade informativa*** – incluem todas as potenciais ameaças detetadas que não podem ser classificadas em nenhuma das categorias acima.

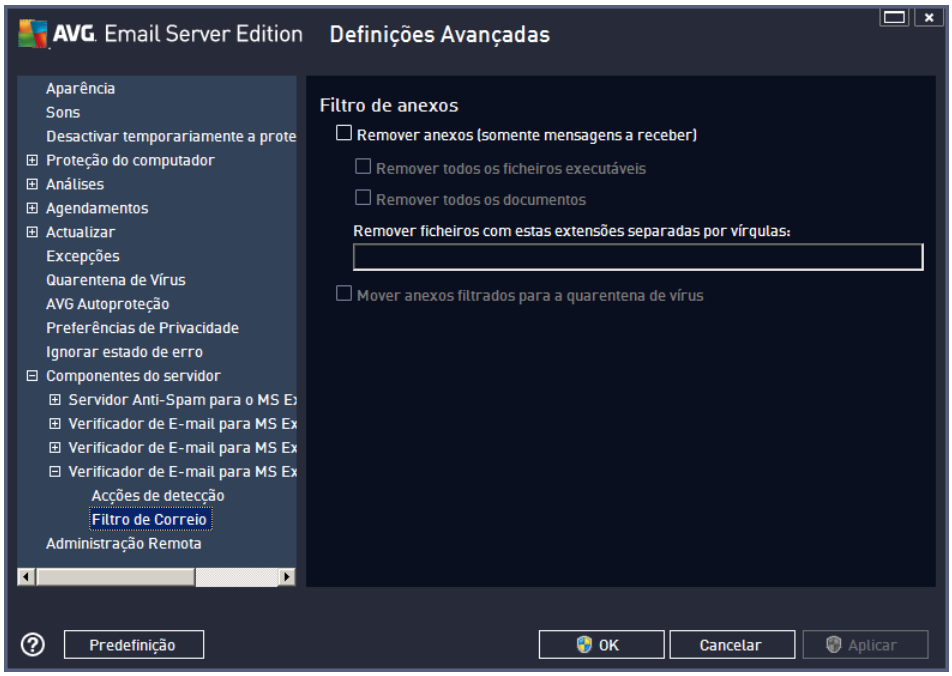
Use o menu de opções para escolher uma ação para cada item:

- ***Nenhuma*** – não será tomada nenhuma ação.
- ***Mover para Quarentena*** – a ameaça em causa será movida para a Quarentena de Vírus.
- ***Remover*** – a ameaça em causa será removida.

Para selecionar um texto personalizado para o campo Assunto das mensagens que contêm o item/ameaça, marque a caixa ***Marcar assunto com...*** e preencha o texto pretendido.

Esta funcionalidade não está disponível para o Verificador de E-mail para MS Exchange VSAPI.

5.6. Filtro de Correio



No item secundário ***Filtro de Correio***, pode escolher quais os anexos que devem ser automaticamente removidos, se quiser. Estão disponíveis as seguintes opções:

- ***Remover anexos*** – marque esta caixa para ativar a funcionalidade.
- ***Remover todos os ficheiros executáveis*** – remover todos os executáveis.
- ***Remover todos os documentos*** – remover todos os documentos.
- ***Remover ficheiros com extensões separadas por vírgula*** – preencha esta caixa com extensões de ficheiros que queira que sejam automaticamente removidas. Separe as extensões com uma vírgula.
- ***Mover anexos filtrados para a quarentena de vírus*** – marque se não quiser que os anexos filtrados sejam definitivamente removidos. Com esta caixa marcada, todos os anexos selecionados nesta janela serão automaticamente movidos para o ambiente da Quarentena de Vírus. É um local seguro para guardar ficheiros potencialmente maliciosos – pode aceder aos ficheiros e examiná-los sem colocar o sistema em perigo. A Quarentena de Vírus pode ser acedida através do menu superior da interface principal do seu **AVG Email Server Edition 2013**. Basta clicar com o botão esquerdo do rato no item ***Opções*** e escolher o item ***Quarentena de Vírus*** no menu de opções.

6. Servidor Anti-Spam para o MS Exchange

6.1. Princípios do Anti-Spam

Spam refere-se a correio eletrónico não solicitado, que normalmente publicita um produto ou serviço e que é enviado em massa para um grande número de endereços de e-mail, sobrecarregando as caixas de correio dos destinatários. Spam não se refere a correio eletrónico comercial legítimo, consentido pelos consumidores. Para além de aborrecedor, as mensagens de spam podem igualmente ser fonte de falcatruas, vírus ou conteúdo ofensivo.

O componente ***Anti-Spam*** verifica todas as mensagens de e-mail a receber e assinala o correio não solicitado como SPAM. Utiliza vários métodos de análise para processar cada mensagem de e-mail, oferecendo o máximo de proteção possível contra mensagens de e-mail indesejadas.

6.2. Interface do Anti-Spam

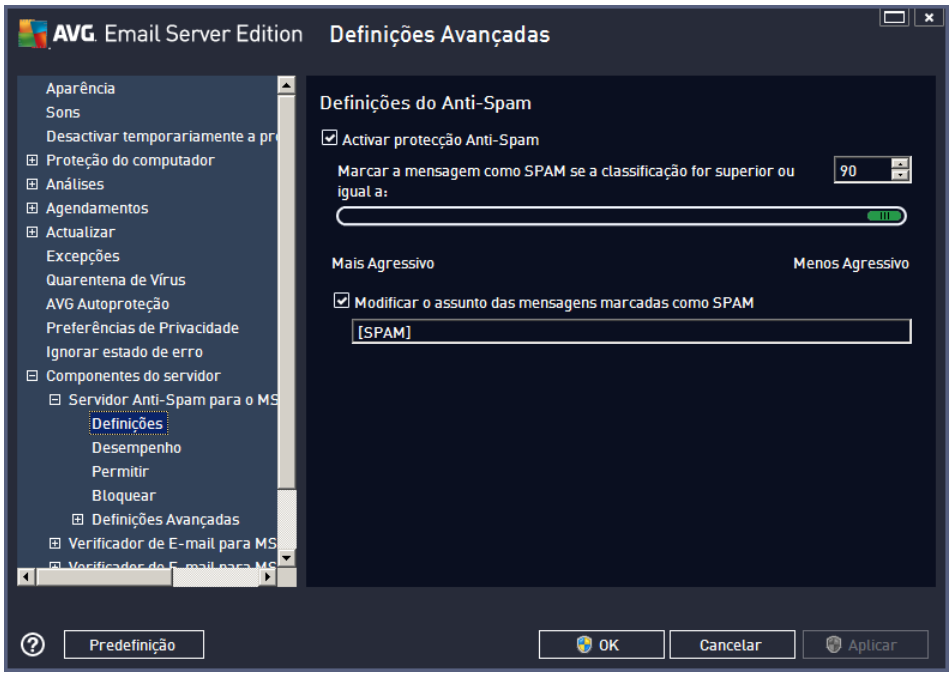
Esta janela contém um resumo da funcionalidade do componente de servidor, informação relativa ao seu estado atual (*Ativado/Desativado*) e algumas estatísticas.

Botões e ligações disponíveis:

- ***ATIVADO/DESATIVADO*** – clicar neste botão permite ativar/desativar o componente selecionado (se o componente estiver ativado, o botão e o texto ficam com cor verde; se o componente estiver desativado, ficam com cor vermelha).
- ***Atualizar valores estatísticos*** – atualiza as estatísticas apresentadas acima.
- ***Definições*** – utilize este botão para abrir as definições avançadas de Anti-Spam.

6.3. Definições Anti-Spam

6.3.1. Definições



Nesta janela pode marcar a caixa ***Ativar proteção Anti-Spam*** para permitir/interditar a análise anti-spam de comunicações de e-mail.

Nesta janela também pode selecionar medidas de classificação mais ou menos agressivas. O filtro ***Anti-Spam*** atribui uma classificação a cada mensagem (*ou seja, o quão similar o conteúdo da mensagem é a SPAM*) baseado em várias técnicas de análise dinâmica. Pode ajustar a definição ***Marcar mensagem como spam se a pontuação for superior ou igual a*** introduzindo um valor (*50 a 90*) ou fazendo deslizar o cursor para a esquerda ou para a direita.

Veja aqui uma revisão geral do limiar de classificação:

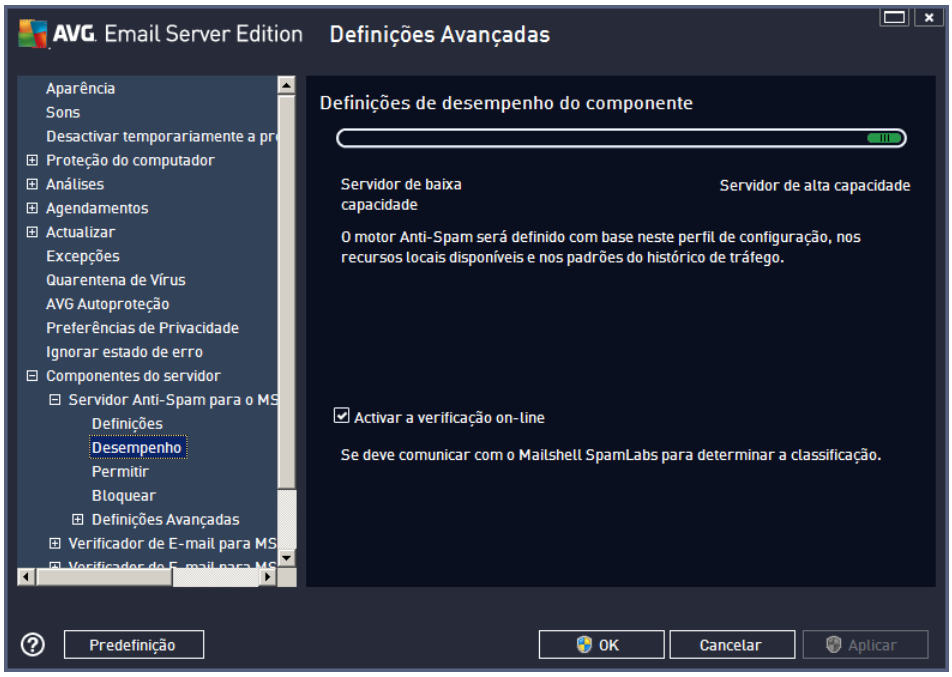
- ***Valor 90*** – A maioria das mensagens de e-mail a receber serão entregues normalmente (sem serem marcadas como spam). O spam mais facilmente identificado será filtrado, mas, mesmo assim, poderá passar uma quantidade significativa de spam.
- ***Valor 80-89*** – As mensagens de e-mail passíveis de serem spam serão filtradas. É igualmente possível que algumas mensagens que não são spam sejam incorretamente filtradas.
- ***Valor 60-79*** – Considerada uma configuração rigorosa. Os e-mails com probabilidade de serem spam serão filtrados. Os e-mails que não são spam também poderão ser apanhados.
- ***Valor 50-59*** – Configuração muito rigorosa. Existe uma forte probabilidade de considerar mensagens de e-mail que não são spam como sendo spam. Este intervalo não é recomendado para uma utilização normal.

Pode ainda definir a forma como as mensagens de e-mail classificadas como spam devem ser tratadas:

- ***Modificar o assunto das mensagens marcadas como SPAM*** – assinale esta caixa se quiser que todas as mensagens detetadas como sendo spam sejam marcadas com uma palavra ou carácter específico no campo de assunto do e-mail; o texto pretendido pode ser digitado no campo de texto ativado.

- ***Perguntar antes de reportar deteção incorreta*** – se tiver concordado com a participação no Programa de Melhoria do Produto durante o processo de instalação – este programa ajuda-nos a recolher informações atualizadas sobre as mais recentes ameaças de todos os participantes a nível mundial e, em troca, temos a possibilidade de melhorar o produto para benefício de todos – ou seja, permitiu a reportação das ameaças detetadas à AVG. A reportação é processada automaticamente. No entanto, pode querer marcar esta caixa para confirmar que pretende ser inquirido antes da reportação de qualquer deteção de spam à AVG para assegurar que a mensagem deverá efetivamente ser classificada como spam.

6.3.2. Desempenho



A janela ***Definições de desempenho do componente*** (*acessível através do item* ***Desempenho*** *na navegação à esquerda*) faculta as definições de desempenho do componente ***Anti-Spam***. Desloque o cursor para a esquerda ou para a direita para alterar o nível de desempenho de análise estabelecido entre os modos ***Memória baixa*** / ***Alto desempenho***.

- ***Memória baixa*** – não serão utilizadas quaisquer regras durante o processo de análise para identificar spam. Serão utilizados apenas dados de aprendizagem para identificação. Este modo não é recomendado para uso comum, a não ser que o hardware do computador seja muito fraco.

- ***Alto desempenho*** – este modo requer uma grande quantidade de memória. Durante o processo de análise para identificar spam, serão utilizadas as seguintes características: regras e cache de base de dados de spam, regras básicas e avançadas, endereços IP de

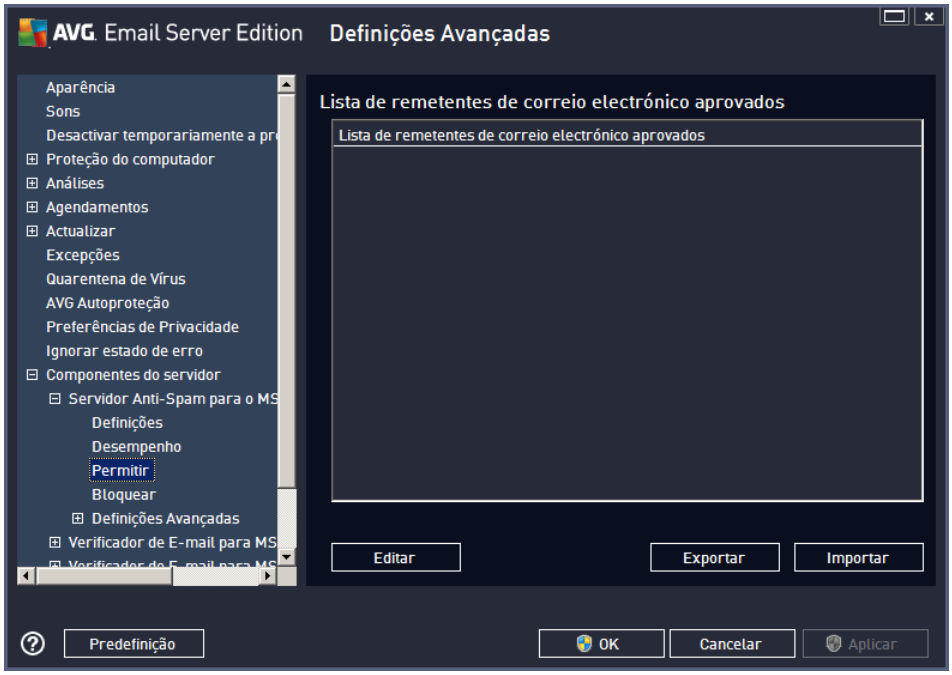
remetentes de spam e bases de dados de remetentes de spam.

O item ***Ativar a verificação on-line*** está ativado por predefinição. Resulta numa deteção de spam mais precisa via comunicação com os servidores Mailshell, ou seja, os dados analisados serão comparados com as bases de dados Mailshell online.

Normalmente é recomendável que mantenha as definições predefinidas e só as altere se tiver uma razão válida para o fazer. Quaisquer alterações à configuração devem ser efetuadas exclusivamente por utilizadores avançados!

6.3.3. Lista Branca

O item ***Lista Branca*** abre uma janela com uma lista global de endereços de e-mail e de nomes de domínios aprovados cujas mensagens nunca serão assinaladas como spam.



Na interface de edição pode compilar uma lista de remetentes dos quais nunca espera receber mensagens indesejadas (spam). Pode ainda compilar uma lista de nomes de domínios completos (ex.*avg.com*), que sabe que não geram spam.

Quando já tiver uma lista de remetentes e/ou nomes de domínio preparada, pode introduzi-los por meio de um dos seguintes métodos: via introdução direta de cada endereço de e-mail ou importando toda a lista de endereços de uma vez. Estão disponíveis os seguintes botões de controlo:

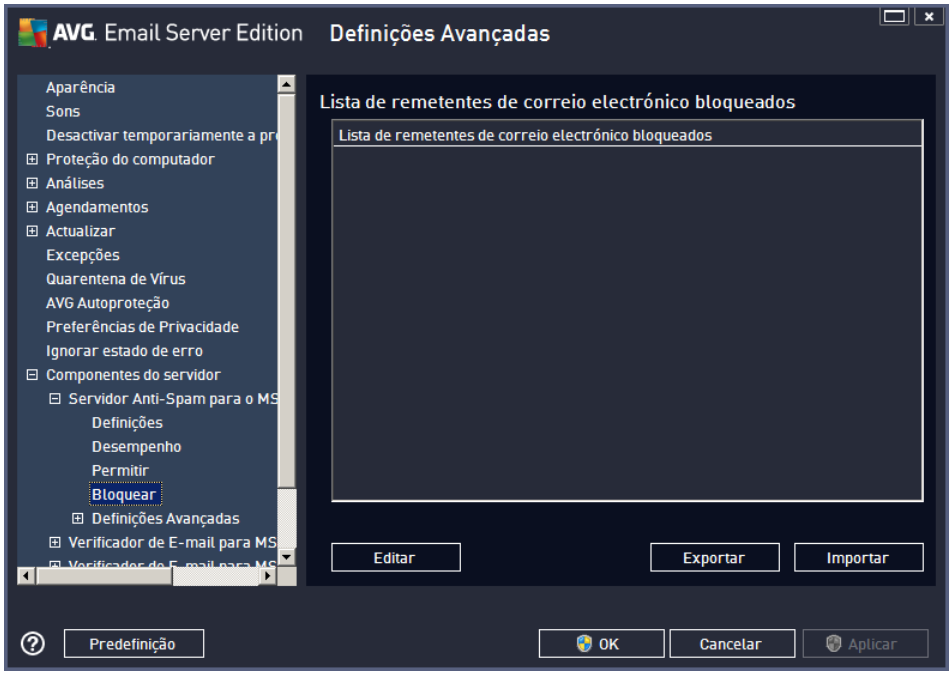
- ***Editar*** – clique neste botão para abrir uma janela onde pode inserir manualmente uma lista de endereços (também pode utilizar o método *copiar e colar*). Insira um item (remetente, nome de domínio) por linha.

- ***Importar*** – pode importar os seus endereços de e-mail através deste botão. O ficheiro de origem pode ser um ficheiro de texto (no formato de texto simples e o conteúdo só deve conter um item – endereço, nome de domínio – por linha), um ficheiro WAB ou a importação pode ser efetuada a partir do Livro de Endereços do Windows ou do Microsoft Office Outlook.

- ***Exportar*** – se decidir exportar os registos para uma determinada finalidade, pode fazê-lo clicando neste botão. Todos os registos serão guardados num ficheiro de texto simples.

6.3.4. Lista Negra

O item ***Lista Negra*** abre uma janela com uma lista global de endereços de e-mail e de nomes de domínios bloqueados cujas mensagens serão sempre assinaladas como spam.



Na interface de edição pode compilar uma lista de remetentes dos quais espera receber mensagens indesejadas (spam). Pode ainda compilar uma lista de nomes de domínios completos (ex. *spammingcompany.com*), dos quais recebe ou espera receber mensagens de spam. Todas as mensagens de e-mail dos endereços/domínios listados serão identificadas como spam.

Quando já tiver uma lista de remetentes e/ou nomes de domínio preparada, pode introduzi-los por meio de um dos seguintes métodos: via introdução direta de cada endereço de e-mail ou importando toda a lista de endereços de uma vez. Estão disponíveis os seguintes botões de controlo:

- ***Editar*** – clique neste botão para abrir uma janela onde pode inserir manualmente uma lista de endereços (também pode utilizar o método *copiar e colar*). Insira um item (remetente, nome de domínio) por linha.

- ***Importar*** – pode importar os seus endereços de e-mail através deste botão. O ficheiro de origem pode ser um ficheiro de texto (no formato de texto simples e o conteúdo só deve conter um item – endereço, nome de domínio – por linha), um ficheiro WAB ou a importação pode ser efetuada a partir do Livro de Endereços do Windows ou do Microsoft Office Outlook.

- ***Exportar*** – se decidir exportar os registos para uma determinada finalidade, pode fazê-lo clicando neste botão. Todos os registos serão guardados num ficheiro de texto simples.

6.3.5. Definições Avançadas

Este separador contém opções de definições suplementares para o componente Anti-Spam. Estas definições destinam-se exclusivamente a utilizadores experientes, regra geral administradores de redes que precisem de configurar detalhadamente a proteção anti-spam para uma proteção superior dos servidores de correio. Como tal, não existe qualquer ajuda suplementar disponível para as janelas individuais; no entanto, está disponível uma pequena descrição de cada opção diretamente na interface do utilizador.

Recomendamos vivamente que não altere quaisquer definições a menos que esteja perfeitamente familiarizado com as definições avançadas do Spamcatcher (MailShell Inc.). Quaisquer alterações inadequadas podem resultar numa diminuição de desempenho ou num mau funcionamento do componente.

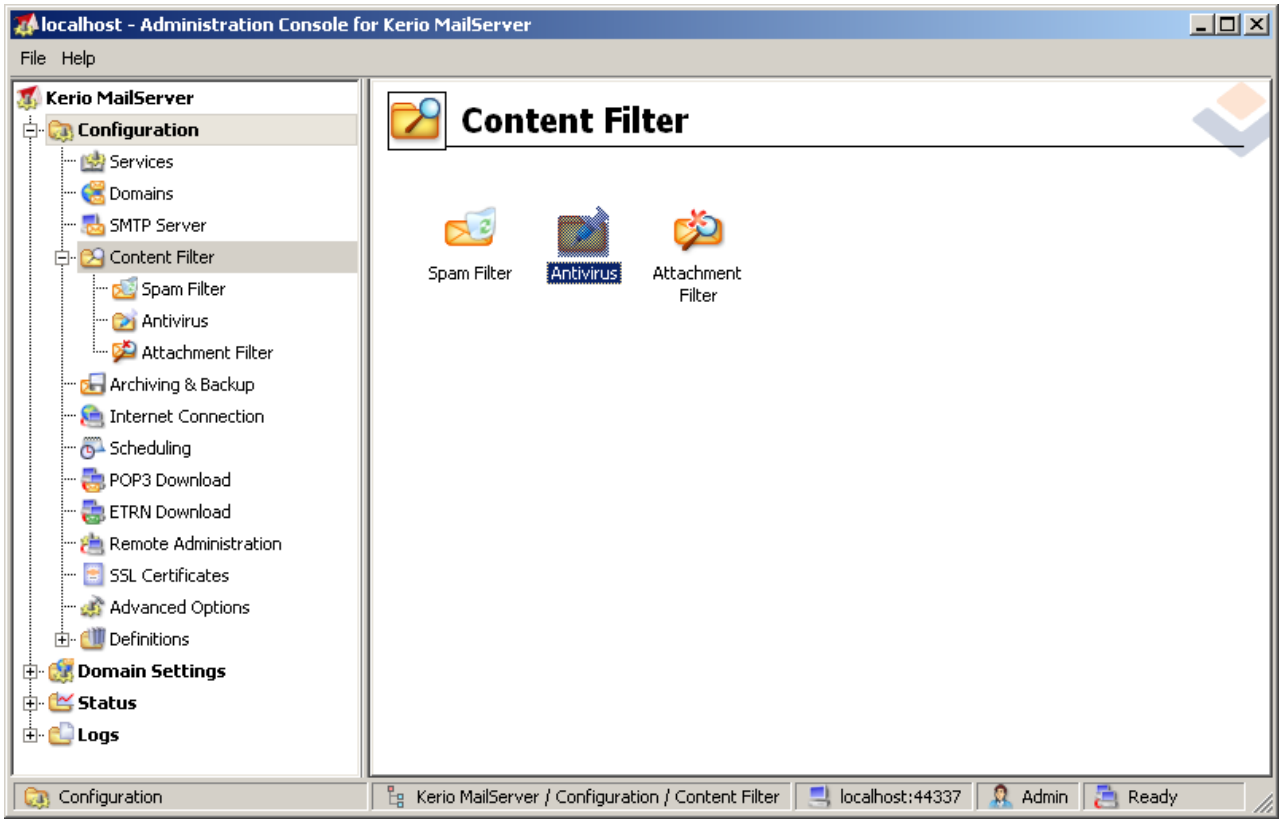
Se contudo necessitar imperativamente de alterar a configuração do componente Anti-Spam nos módulos mais avançados, por favor siga as instruções facultadas na interface do utilizador. Regra geral, encontrará em cada janela uma única funcionalidade específica que pode editar – a descrição da mesma está sempre incluída na própria janela:

- ***Filtragem*** – lista de idiomas, lista de países, IPs aprovados, IPs bloqueados, países bloqueados, conjuntos de caracteres bloqueados, remetentes falsificados
- ***RBL*** – servidores RBL, multicorrespondências, limiar, tempo limite, máximo de IPs
- ***Ligação à Internet*** – tempo limite, servidor proxy, autenticação de servidor proxy

7. AVG para Kerio MailServer

7.1. Configuração

O mecanismo de proteção antivírus está integrado diretamente na aplicação do Kerio MailServer. Para ativar a proteção de e-mail do Kerio MailServer pelo componente de análise AVG, inicie a aplicação Consola de Administração Kerio. Na árvore de controlo situada no lado esquerdo da janela da aplicação, selecione o ramo secundário Filtro de Conteúdos no ramo Configuração:

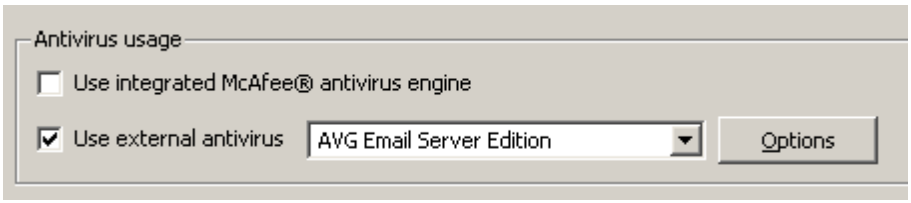


Se clicar no item Filtro de Conteúdos, será apresentada uma janela com três itens:

- ***Filtro Anti-spam***
- ***Antivírus*** (consulte a secção ***Antivírus***)
- ***Filtro de anexos*** (consulte a secção ***Filtro de anexos***)

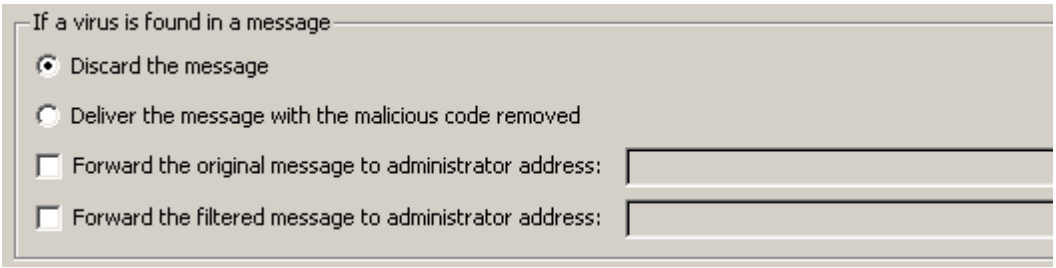
7.1.1. Antivírus

Para ativar o AVG para Kerio MailServer, selecione a caixa Utilizar antivírus externo e selecione a versão AVG Email Server Edition no menu de software externo do quadro Utilização Antivírus da janela de configuração:



Na secção seguinte, especifique o procedimento para uma mensagem infetada ou filtrada:

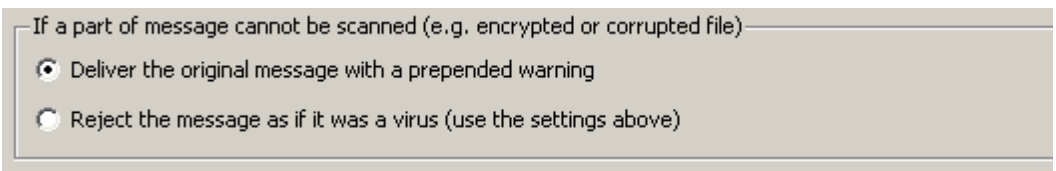
- ***Se for detetado um vírus numa mensagem***



Este quadro especifica a ação a executar quando é detetado um vírus numa mensagem ou quando uma mensagem é filtrada por um filtro de anexos:

  - ***Eliminar a mensagem*** – se selecionada, a mensagem infetada ou filtrada será eliminada.
  - ***Entregar a mensagem com o código malicioso removido*** – se selecionada, a mensagem será entregue ao destinatário, mas sem o anexo potencialmente perigoso.
  - ***Reencaminhar a mensagem original para o endereço do administrador*** – se selecionada, a mensagem infetada com vírus será reencaminhada para o endereço especificado no campo de texto do endereço.
  - ***Reencaminhar a mensagem filtrada para o endereço do administrador*** – se selecionada, a mensagem filtrada será reencaminhada para o endereço especificado no campo de texto do endereço.

- ***Se não for possível analisar uma parte da mensagem (por exemplo, um ficheiro encriptado ou danificado)***



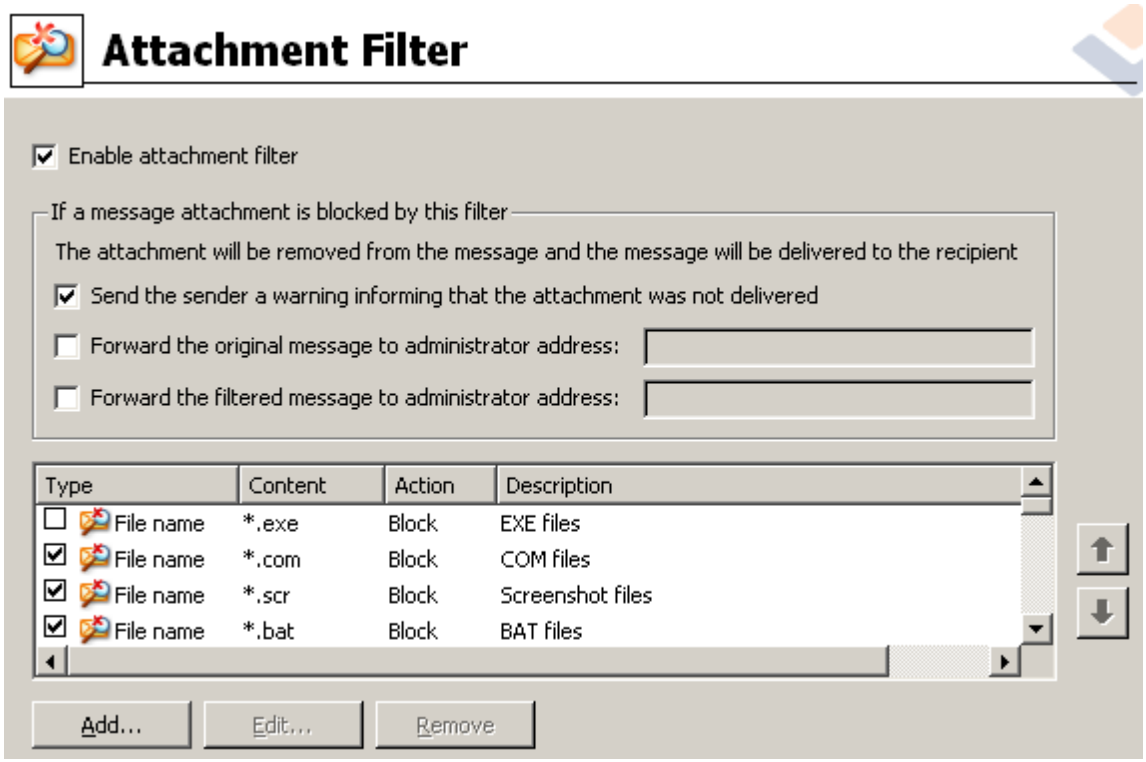
Este quadro especifica a ação a executar se não for possível analisar uma parte da mensagem ou do anexo:

- ***Entregar a mensagem original com um aviso preparado*** – a mensagem (ou anexo) será entregue sem ser analisada. O utilizador será avisado de que a mensagem ainda pode conter vírus.

- ***Rejeitar a mensagem como se fosse um vírus*** – o sistema reagirá de forma idêntica a quando é detetado um vírus (ou seja, a mensagem será entregue sem nenhum anexo ou rejeitada). Esta opção é segura, mas o envio de arquivos protegidos por palavra-passe será virtualmente impossível.

7.1.2. Filtro de anexos

No menu Filtro de Anexos existe uma lista de várias definições de anexos:



Selecione a caixa de verificação Ativar filtro de anexos para ativar/desativar a filtragem de anexos de correio. Opcionalmente, pode alterar as seguintes definições:

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

  O remetente receberá um aviso do Kerio MailServer a informá-lo que enviou uma mensagem com um vírus ou um anexo bloqueado.

- ***Reencaminhar a mensagem original para o endereço do administrador***

  A mensagem será reencaminhada (tal como está – com o anexo infetado ou interdito) para um endereço de e-mail definido, local ou externo.

- ***Reencaminhar a mensagem filtrada para o endereço do administrador***

A mensagem sem o anexo infetado ou interdito será (independentemente das ações selecionadas abaixo) reencaminhada para o endereço de e-mail especificado. Esta opção pode ser utilizada para verificar o funcionamento correto do antivírus e/ou do filtro de anexos.

Na lista de extensões, cada item tem quatro campos:

- ***Tipo*** – especificação do tipo de anexo determinado pela extensão fornecida do campo Conteúdo. Os tipos possíveis são Nome de ficheiro ou MIME. Selecione a caixa respetiva neste campo para incluir/ excluir o item da filtragem de anexos.
- ***Conteúdo*** – permite especificar uma extensão a filtrar. Pode utilizar caracteres universais do sistema operativo (por exemplo, a cadeia "*.doc.*" significa qualquer ficheiro com a extensão .doc e qualquer outra extensão subsequente).
- ***Ação*** – define a ação a executar com o anexo em causa. As ações possíveis são Aceitar (aceitar o anexo) e Bloquear (será executada uma ação conforme definido acima da lista de anexos desativados).
- ***Descrição*** – a descrição do anexo é definida neste campo.

Para remover um item da lista, clique no botão Remover. Pode adicionar outro item à lista clicando no botão ***Adicionar...***. Ou, pode editar um registo existente clicando no botão ***Editar...***. Será apresentada a seguinte janela:

- No campo Descrição, escreva uma breve descrição do anexo a filtrar.
- No campo Se uma mensagem de correio contém um anexo em que, selecione o tipo de anexo (Nome de ficheiro ou MIME). Também pode escolher uma extensão específica na lista de extensões fornecida ou digitar diretamente os caracteres universais da extensão.

No campo Em seguida, decida se o anexo definido deve ser bloqueado ou aceite.

8. Perguntas Frequentes e Suporte Técnico

Se tiver qualquer tipo de problemas com o seu AVG, de natureza comercial ou técnica, por favor consulte a secção ***Perguntas Frequentes (FAQ)*** do website da AVG em http://www.avg.com.

Se não conseguir obter ajuda por este meio, contacte o departamento de suporte técnico por e-mail. Por favor utilize o formulário de contacto acessível a partir do menu de sistema via ***Ajuda / Obter ajuda on-line***.