AVG 9.0 Email Server Edition

Manual do Usuário

Revisão do documento 90.1 (5. 9. 2009)

Conteúdo

1. Introdução

Este manual do usuário fornece uma documentação completa para o **AVG 9.0 Email Server Edition**.

Parabéns pela aquisição do AVG 9.0 Email Server Edition!

AVG 9.0 Email Server Editioné um dos vários produtos premiados do AVG criados para fornecer a você paz de espírito e total segurança para o seu computador. Como ocorreu com todos os produtos do AVG, o **AVG 9.0 Email Server Edition** foi completamente reprojetado para fornecer a proteção e a segurança certificada e renomada do AVG em 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 de E-mail 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 no http://www.avg.com.*

2. Requisitos de instalação do AVG

2.1. Sistemas operacionais com suporte

AVG 9.0 Email Server Edition foi criado para proteger servidores de e-mail em execução nos seguintes sistemas operacionais:

- Windows 2008 Server Edition (x86 e x64)
- Windows 2003 Server (x86, x64 e Itanium) SP1
- Windows 2000 Server SP4 + Update Rollup 1

2.2. Servidores de e-mail suportados

Os servidores de e-mail a seguir são suportados:

- ***Versão do MS Exchange 2000 Server (com Service Pack 1 ou superior)***

  Nota: para o Exchange 2000 Server - Service Pack 1 (ou posterior) deve ser aplicado antes de você usar o mecanismo do AVG; **AVG para MS Exchange 2000/2003 Server** utiliza a interface de aplicativo VSAPI 2.0 (ou 2.5 com o Exchange 2003 Server), coberta neste Service Pack.

- ***Versão do MS Exchange 2003 Server***
- ***Versão do MS Exchange 2007 Server***
- ***AVG para Kerio MailServer*** – versão 5.x/6.x e superior

2.3. Requisitos de hardware

Os requisitos mínimos de hardware para **AVG 9.0 Email Server Edition** são:

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

Requisitos recomendados de hardware para **AVG 9.0 Email Server Edition** 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 já tiver uma versão mais antiga do AVG Email Server instalada, deverá desinstalá-la antes de instalar o **AVG 9.0 Email Server Edition**. Você deve executar a desinstalação da versão anterior manualmente, utilizando a funcionalidade do Windows.

- No menu inicial ***Iniciar/Configurações/Painel de Controle/Adicionar ou Remover Programas***, selecione o programa correto na lista de softwares instalados. Tome cuidado ao selecionar o programa AVG para desinstalação. Você precisa desinstalar o Email Server Edition antes de desinstalar o AVG File Server Edition.
- Quando tiver desinstalado o Email Server Edition, você poderá prosseguir para desinstalar a versão anterior do AVG File Server Edition. Isso pode ser feito facilmente no menu inicial ***Iniciar/Todos os Programas/AVG/Desinstalar AVG***
- Se você já usou o AVG 8.x ou versão mais antiga, não se esqueça de desinstalar também plug-ins de servidor individual.

2.5. MS Exchange Service Packs

Como o **AVG para MS Exchange 2000/2003 Server** usa a interface de verificação de vírus VSAPI 2.0/2.5, é necessário ter o Service Pack 1 (ou posterior) para o MS Exchange 2000 Server aplicado ao seu sistema. Siga o link abaixo para obter o Service Pack 1 para MS Exchange 2000 Server mais recente:

Service Pack para MS Exchange 2000 Server:

http://www.microsoft.com/technet/prodtechnol/exchange/downloads/2000/sp3/default.mspx

Para o MS Exchange 2003 Server nenhum outro service pack é necessário; no entanto, é recomendável manter o sistema o mais atualizado possível com os últimos service packs e hotfixes, de modo a obter o máximo de segurança disponível.

Service Pack para MS Exchange 2003 Server (opcional):

http://www.microsoft.com/exchange/evaluation/sp2/overview.mspx

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

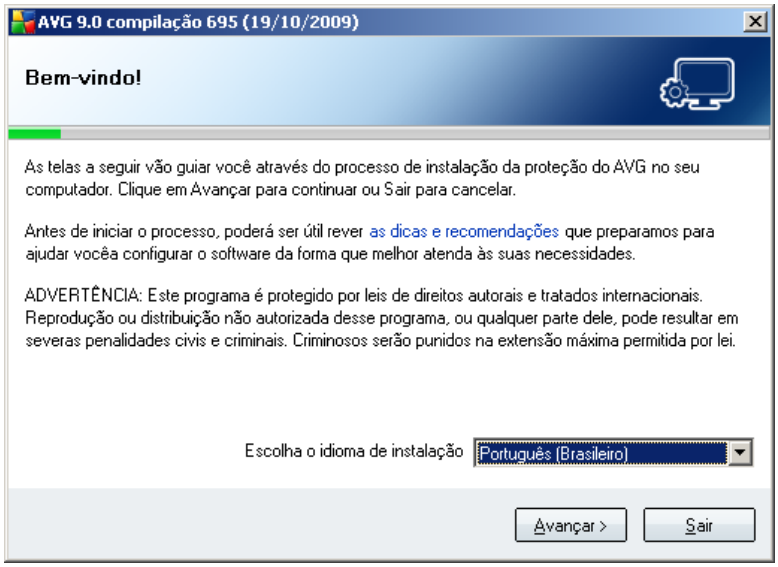
3. Processo de instalação do AVG

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).

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 de venda 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 e-mail.

Após fazer download e salvar o arquivo de instalação no drive rígido, você poderá iniciar o processo de instalação. A instalação é uma seqüência 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



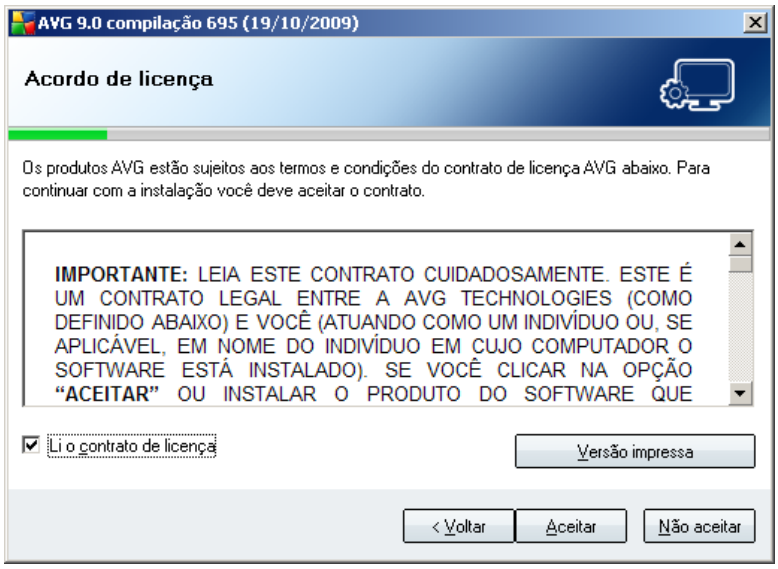
O processo de instalação é iniciado com a janela de ***boas-vindas***. Nela você seleciona o idioma usado na instalação. Na parte inferior da janela da caixa de diálogo, localize o item ***Selecionar seu idioma da instalação*** e selecione o idioma desejado no menu suspenso. Em seguida, pressione o botão ***Avançar*** para confirmar e continuar para a próxima caixa de diálogo.

Atenção: *aqui você está selecionando o idioma usado somente no processo de instalação. Você não está selecionando o idioma do aplicativo AVG. Isso poderá ser especificado posteriormente, durante o processo de instalação.*

3.2. Contrato de licença

A caixa de diálogo ***Contrato de Licença*** indica o texto completo do contrato de licença do AVG. Leia-o cuidadosamente e confirme se leu, compreendeu e aceitou o contrato, marcando a caixa de seleção ***Li o contrato de licença*** e pressionando o botão ***Aceitar.*** Se você não concordar com o contrato de licença, pressione o botão ***Não aceito*** e o processo de instalação será encerrado imediatamente.

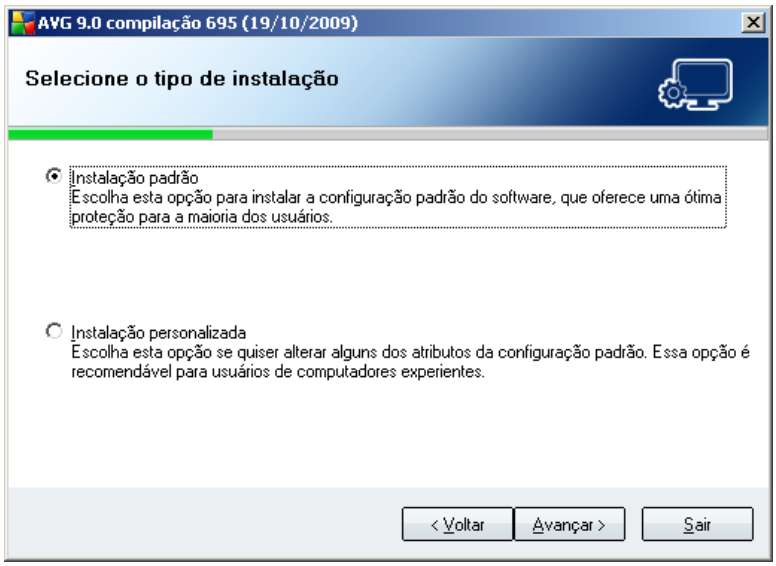
Use o botão ***Versão impressa***para abrir o contrato de licença em uma nova janela ajustada para impressão.



3.3. Verificando o status do sistema

Depois de confirmar o contrato de licença, você será redirecionado para a caixa de diálogo ***Verificação do Status do Sistema***. Essa caixa de diálogo não requer nenhuma intervenção; o sistema está sendo verificado antes da inicialização da instalação do AVG. Aguarde a conclusão do processo e continue automaticamente para a caixa de diálogo seguinte.

3.4. Selecionar o tipo de instalação



A caixa de diálogo ***Selecionar Tipo de Instalação*** oferece duas opções de instalação como alternativa: ***padrão*** e ***personalizada.***

Para a maioria dos usuários, é altamente recomendável manter a ***instalação padrão*** 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.

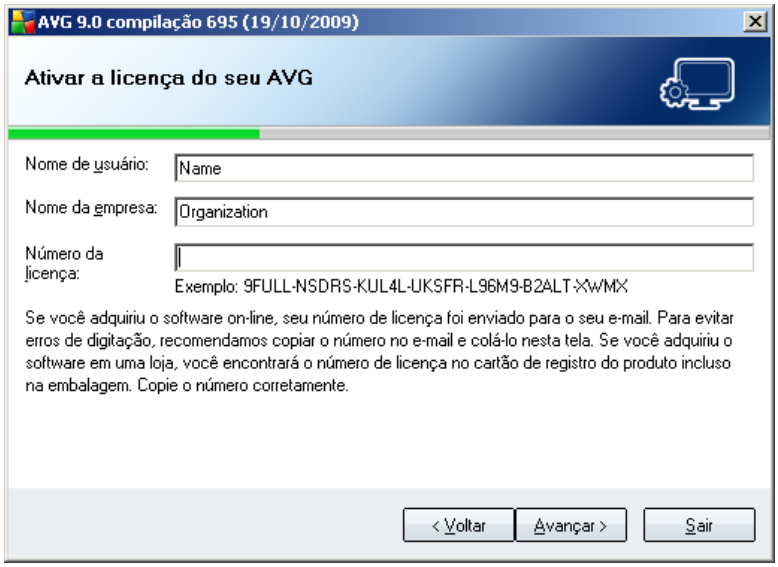
A instalação personalizada só deve ser usada por usuários experientes que tenham um motivo válido para instalar o AVG com configurações diferentes das padrão, ou seja, para se ajustar aos requisitos específicos do sistema.

3.5. Ativar o AVG

Na caixa de diálogo ***Ativar sua Licença do AVG*** , você deverá preencher o registro. Digite seu nome (campo ***Nome do Usuário***) e o nome da sua empresa (***Nome da Empresa).***

Em seguida, digite seu número de licença no campo de texto ***Número da Licença*** O número da licença está no e-mail 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 e-mail), é recomendável usar o método de copiar e

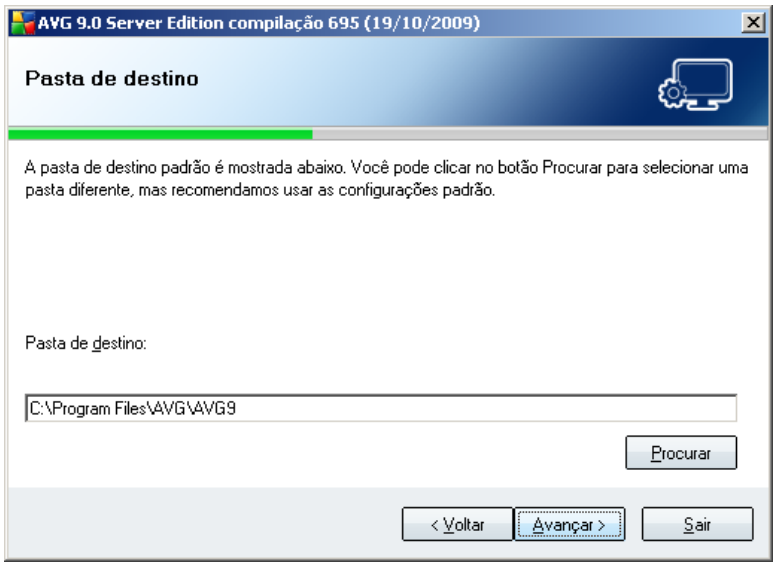
colar para inseri-lo.



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

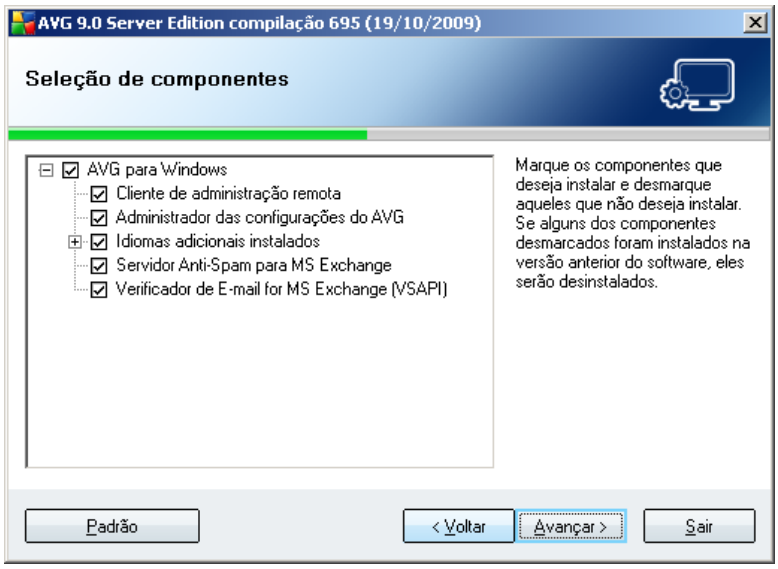
Se na etapa anterior tiver selecionado a instalação padrão, você será redirecionado para a caixa de diálogo ***Resumo da Instalação*** . Se a instalação personalizada tiver sido selecionada, você continuará na caixa de diálogo ***Pasta de Destino***.

3.6. Instalação personalizada - Pasta de destino



A caixa de diálogo ***Pasta de destino*** permite especificar o local de instalação do AVG. Por 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 pasta respectiva. Pressione o botão ***Avançar*** para confirmar.

3.7. Instalação personalizada - Seleção de componentes



A caixa de diálogo ***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.

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

  Observação: *Apenas dois componentes de servidores disponíveis na lista podem ser gerenciados remotamente!*

- ***Gerenciador de Configurações do AVG*** - uma ferramenta adequada principalmente aos administradores de redes que permite copiar, editar e distribuir as configurações do AVG. A configuração pode ser salva em um dispositivo portátil (unidade flash USB etc.) e aplicados manualmente ou por qualquer outra forma para estações escolhidas.

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

Visão geral básica dos componentes individuais de servidor:

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

  Verifica todas as mensagens de e-mail recebidas e marca os e-mails indesejáveis como SPAM. Ele usa diversos métodos de análise para processar cada mensagem de e-mail, oferecendo o máximo de proteção possível contra mensagens de e-mail indesejáveis.

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

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

  Disponível para MS Exchange 2007 e poder ser instalado somente para a função HUB.

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

  Verifica todas as mensagens de e-mail recebidos através da interface do MS Exchange SMTP.

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

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

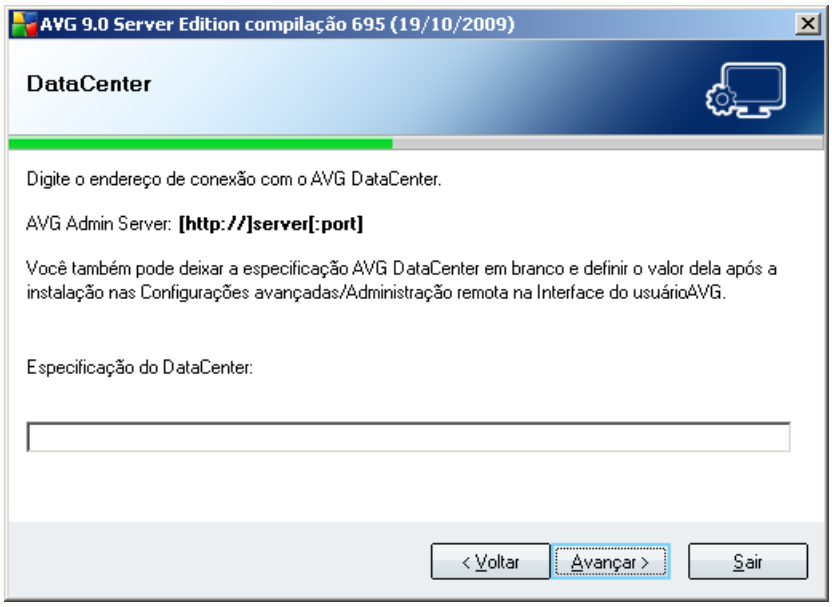
  Verifica todas as mensagens de e-mail armazenadas nas caixas de correio dos usuários. Se algum vírus for detectado, será movido para a Quarentena de vírus, ou removido completamente.

Observação: *Há diferentes opções disponíveis para MS Exchange 2007 e MS Exchange 2003.*

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

3.8. Instalação Personalizada - DataCenter

Se você selecionou o módulo ***Componente de administração remota*** durante a seleção de módulo, nesta tela poderá definir a string de conexão para conectar em seu AVG DataCenter.



3.9. Resumo da instalação

A caixa de diálogo ***Resumo da instalação*** oferece uma visão geral de todos os parâmetros do processo de instalação. Certifique-se de que todas as informações estejam corretas. Nesse caso, pressione o botão ***Concluir*** para continuar. Caso contrário, você pode usar o botão ***Voltar*** para voltar para a caixa de diálogo respectiva e corrigir as informações.

3.10. Instalando

A caixa de diálogo ***Instalação mostra o andamento do processo de instalação e não requer intervenção.*** Aguarde a conclusão da instalação e você será redirecionado à caixa de diálogo ***Instalação Concluída***.

3.11. Instalação concluída

A caixa de diálogo ***Instalação Concluída*** é a última etapa do processo de instalação do AVG. Agora o AVG está instalado no computador e funcionando perfeitamente. O programa está sendo executado em segundo plano, em modo totalmente automático.

Para configurar a proteção individualmente para o seu servidor de e-mail, siga o capítulo apropriado:

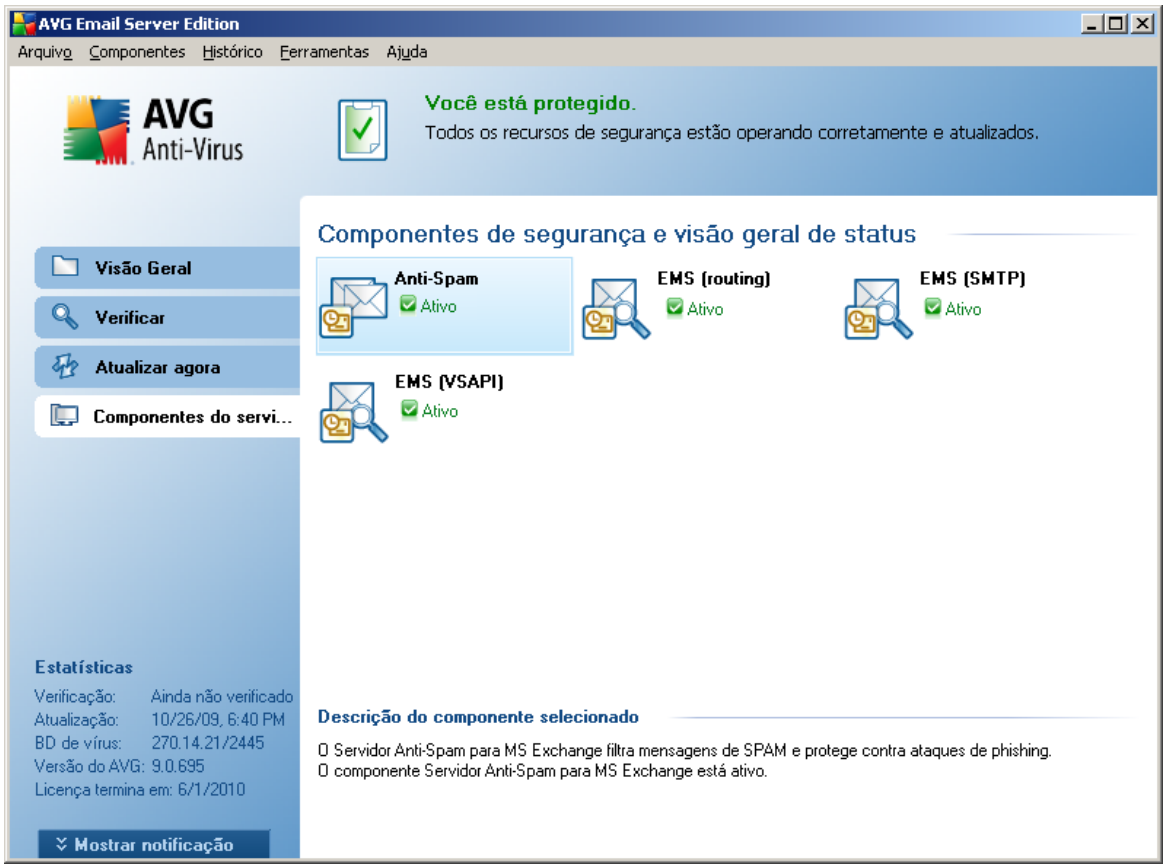
- ***Verificador de e-mail do para MS Exchange Server 2007***

- ***Verificador de e-mail do para MS Exchange Server 2000/2003***
- ***AVG para Kerio MailServer***

4. Verificador de e-mail para MS Exchange Server 2007

4.1. Visão Geral

A AVG para MS Exchange Server 2007 configuration opções are fully integrated within the AVG 9.0 Email Server Edition as servidor components.



Visão geral básica dos componentes individuais de servidor:

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

  Verifica todas as mensagens de e-mail recebidas e marca os e-mails indesejáveis como SPAM. Ele usa diversos métodos de análise para processar cada mensagem de e-mail, oferecendo o máximo de proteção possível contra mensagens de e-mail indesejáveis.

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

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

  Disponível para MS Exchange 2007 e poder ser instalado somente para a função HUB.

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

  Verifica todas as mensagens de e-mail recebidos através da interface do MS Exchange SMTP.

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

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

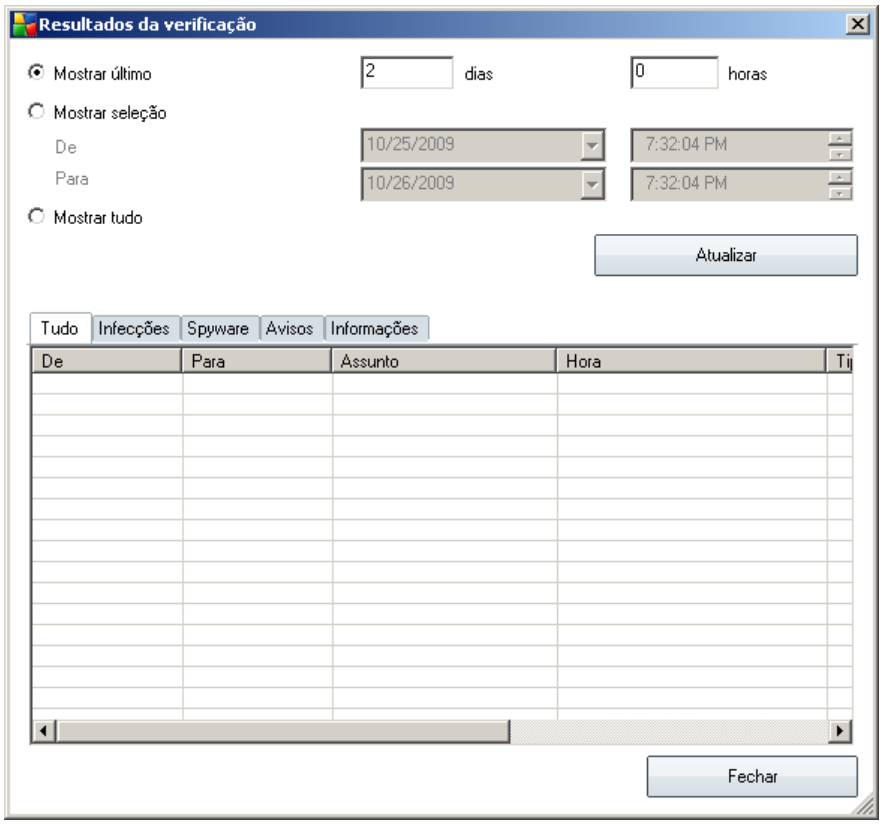
  Verifica todas as mensagens de e-mail armazenadas nas caixas de correio dos usuários. Se algum vírus for detectado, será movido para a Quarentena de vírus, ou removido completamente.

Dê um clique duplo em um componente necessário para abrir sua interface. Com a exceção do anti-spam, todos os componentes compartilham os seguintes links e botões de controle comum:

Links disponíveis:

- ***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*** - inserir dias e horas d preferência.
- ***Mostrar seleção*** - selecionar 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.
- ***Redefinir valores estatísticos*** - redefine todas as estatísticas para zero.

Os botões operacionais são os seguintes:

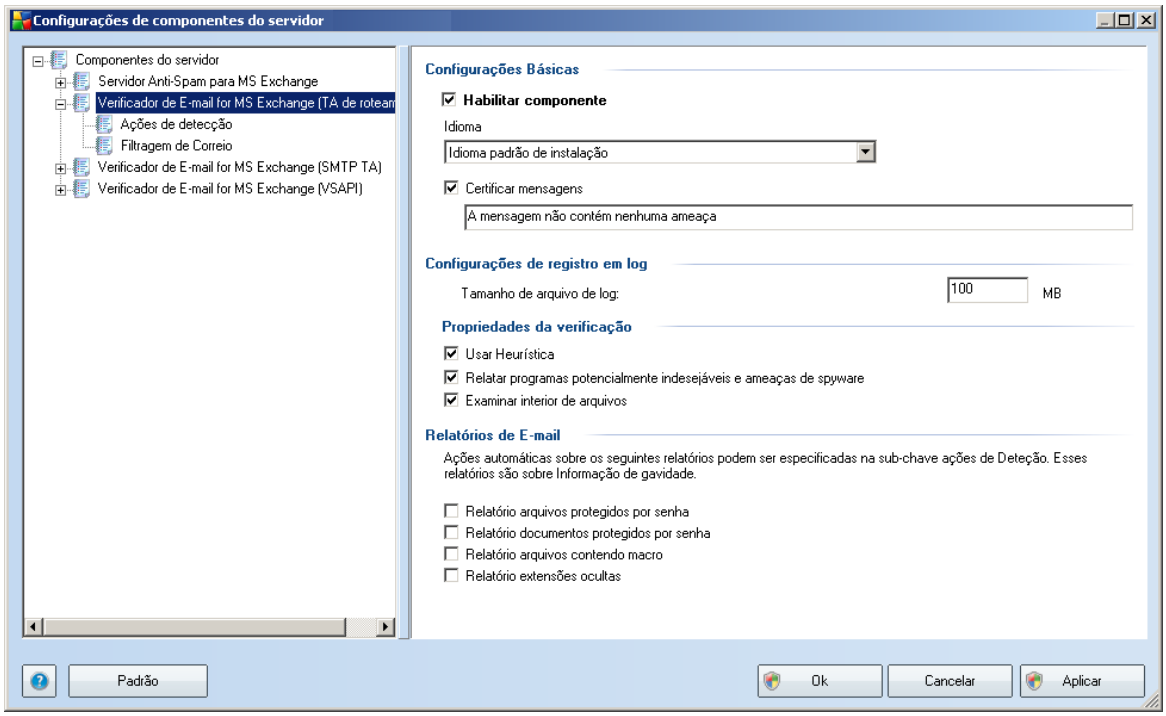
- ***Configurações*** - use este botão para abrir as configurações do componente.
- ***Voltar*** - pressione este botão para voltar para a visão geral dos componentes do Servidor

Você encontrará mais informações sobre configurações individuais de todos os componentes nos capítulos abaixo.

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

Para open the configurações de ***Verificador de E-mail para MS Exchange ((routing transport agent)***, select the ***Configurações*** button de the interface de the componente.

A partir de ***Componentes do servidor*** list select the ***Verificador de E-mail para MS Exchange ((routing TA)*** item:



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

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

A seção ***Configurações de registro em log***:

- ***Tamanho de arquivo de log*** - escolha o tamanho preferido do arquivo de log. Valor padrão: 100 MB.

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

- ***Use heurística*** - selecione esta caixa para ativar método de análise heurística durante a verificação.
- ***Informar ameaças de spyware e programas potencialmente indesejados*** - selecione está opção para informar a presença de spyware e programas potencialmente indesejados.
- ***Verificar dentro de arquivos*** - selecionar esta opção para permitir que o verificado busque dentro de arquivos de compactação(CEP, rar, etc.)

A seção***Informação de anexos de e-mail*** permite que você escolha quais itens devem ser informados durante a verificação. Se verificado, cada e-mail 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:

- ***Informar arquivos protegidos por senha***
- ***Informar documentos protegidos por senha***
- ***Informar arquivos de contenham macro***
- ***Informar extensões ocultas***

Há também estes subitens disponíveis na seguinte estrutura de árvore:

- ***Ações de detecção***

- ***Filtragem de correio***

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

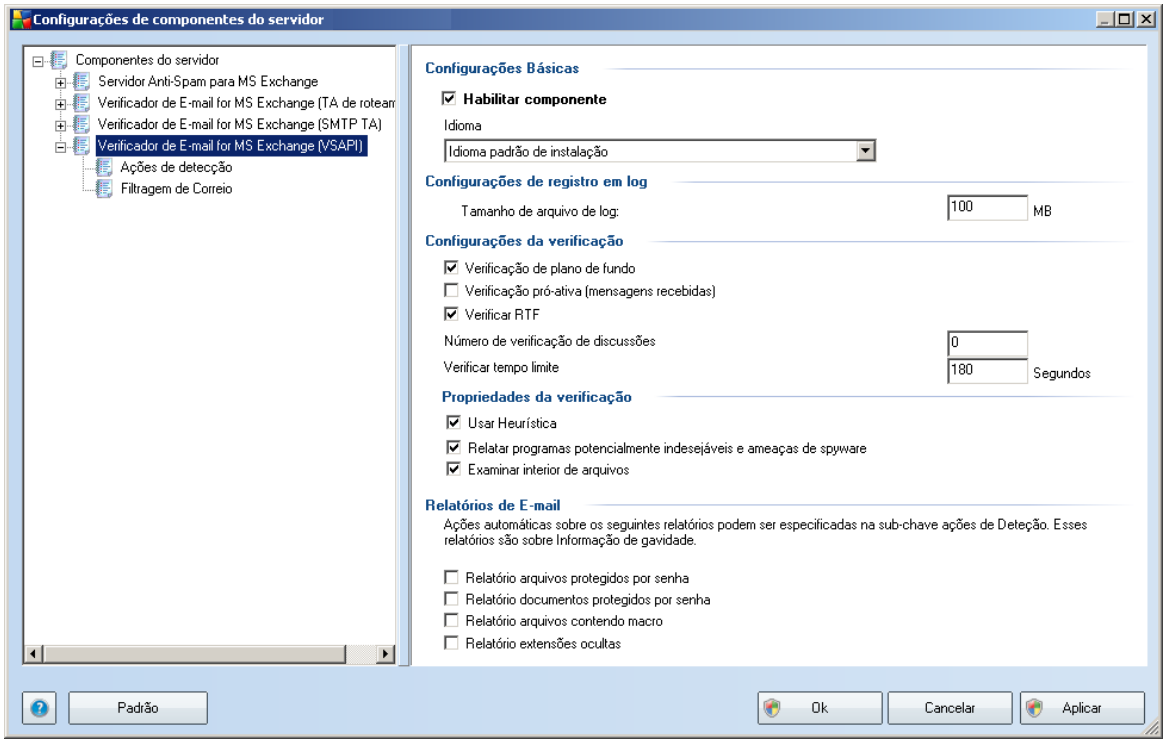
A configuração para o ***Verificador de E-mail para MS Exchange (agente de transporte do SMTP)*** é exatamente o mesmo como no caso do agente de transporte de roteamento. Para maiores informações, consulte o capítulo acima ***Verificador de E-mail para MS Exchange (roteamento TA)***.

Há também estes subitens disponíveis na seguinte estrutura de árvore:

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

4.4. Verificador de e-mail para MS Exchange (VSAPI)

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



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

- ***Habilitar componente*** - desmarque para desativar todo o componente.
- ***Idioma*** - Selecione o idioma do componente preferida.

A seção ***Configurações de registro em log***:

- ***Tamanho de arquivo de log*** - escolha o tamanho preferido do arquivo de log. Valor padrão: 100 MB.

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

- ***Verificação em Segundo Plano***– *você pode ativar ou desativar ao processo de verificação em segundo plano aqui.* 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 2007 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 e-mail 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.

  Nota: *: O excesso de mensagens continuará para a loja não autorizada.*

Observação: *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.

- ***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.

- Χαμπο ***Tempo Limite de Verificação*** - o intervalo contínuo máximo (em segundos) para que um processo acesse a mensagem sendo verificada).

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

- ***Use heurística*** - selecione esta caixa para ativar método de análise heurística durante a verificação.

- ***Informar ameaças de spyware e programas potencialmente indesejados*** - selecione está opção para informar a presença de spyware e programas potencialmente indesejados.

- ***Verificar dentro de arquivos*** - selecionar esta opção para permitir que o verificado busque dentro de arquivos de compactação(CEP, rar, etc.)

A seção***Informação de anexos de e-mail*** 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:

- ***Informar arquivos protegidos por senha***

- ***Informar documentos protegidos por senha***

- ***Informar arquivos de contenham macro***

- ***Informar extensões ocultas***

Geralmente alguns destes recursos são extensões de usuário dos serviços da interface

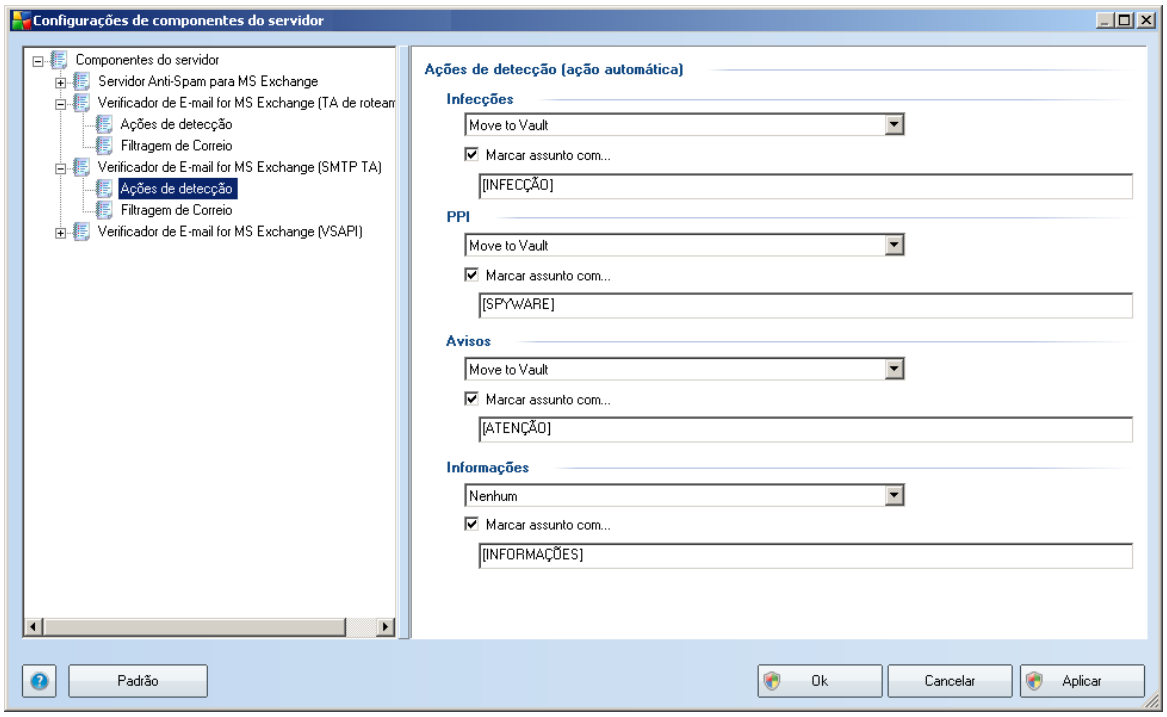
de aplicativo Microsoft VSAPI 2.0/2.5. Para obter informações detalhadas sobre a VSAPI 2.0/2.5, consulte os seguintes links (e também os links acessíveis pelos indicados):

- 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***

4.5. Detection_Actions



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:

- ***Infecções***
- ***PPI (Programas Potencialmente Indesejáveis)***
- ***Avisos***
- ***Informações***

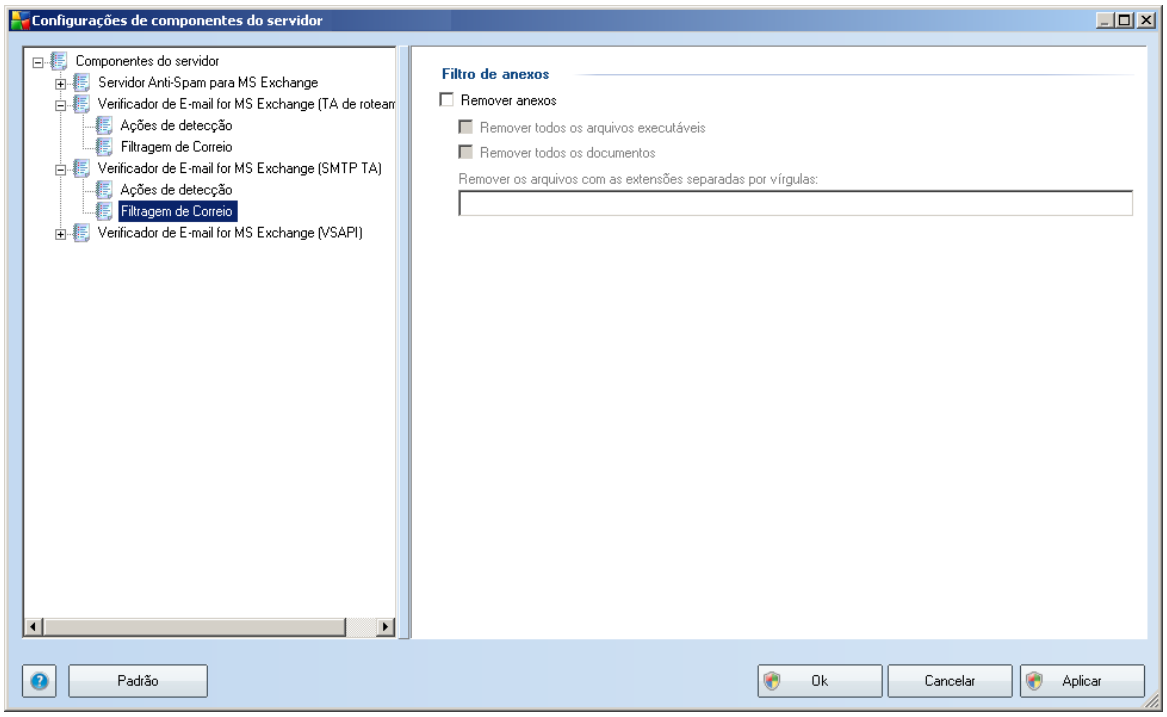
Use o menu suspenso para escolher uma ação para cada item:

- ***Nenhuma*** - nenhuma ação será realizada.
- ***Mover para Quarentena*** - a ameaça determinada vírus será movida para a Quarentena de Vírus do
- ***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.

Nota: *: O último recurso mencionado não está disponível para o Verificador de e-mail para VSAPI para MS Exchange.*

4.6. Filtragem de correio



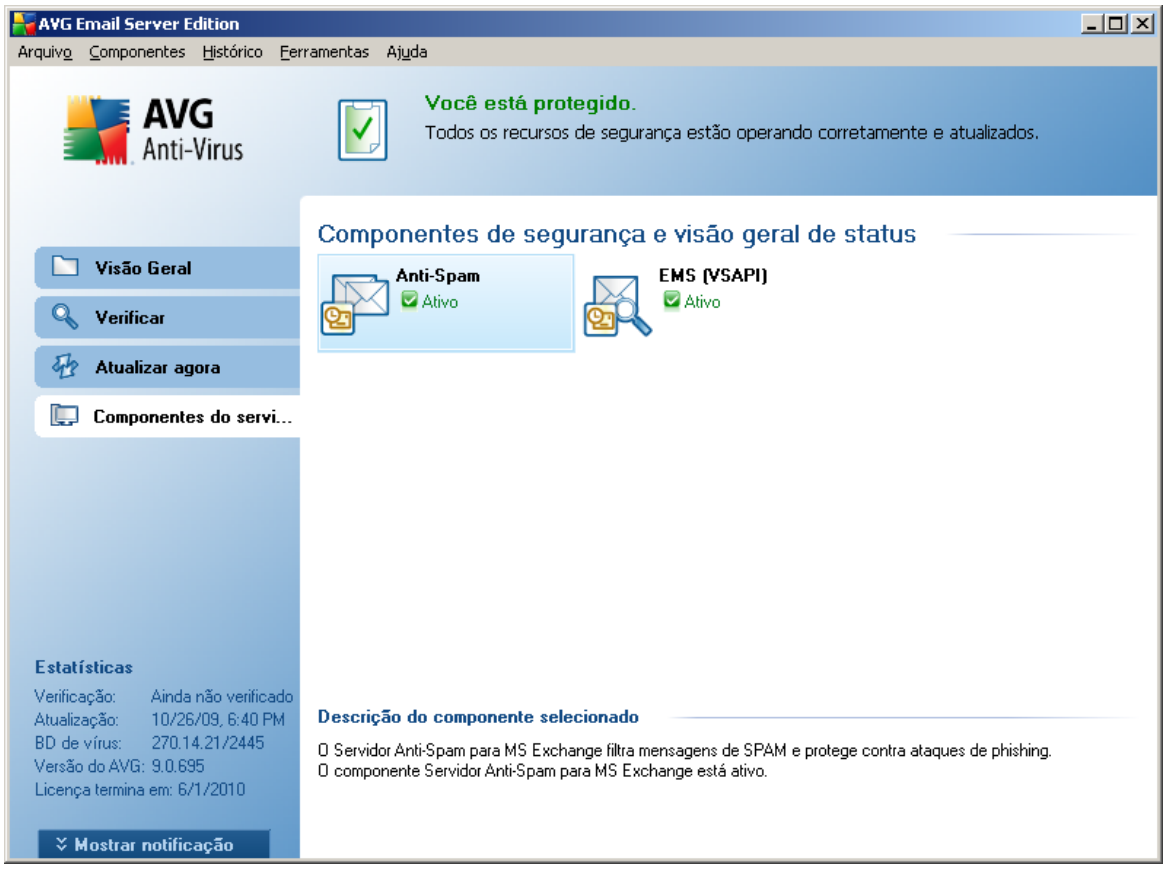
No subitem***Filtragem de correio*** é possível escolher quais anexos devem ser automaticamente removidos, se houver. As seguintes opções estão disponíveis:

- ***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.

5. Verificador de e-mail do para MS Exchange Server 2000/2003

5.1. Visão Geral

As opções de configuração para o Verificador de E-mail para MS Exchange Server 2000/2003 estão totalmente integradas no AVG 9.0 Email Server Edition como um componente de servidor.



Os componentes de servidor incluem o seguinte:

Visão geral básica dos componentes individuais de servidor:

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

  Verifica todas as mensagens de e-mail recebidas e marca os e-mails indesejáveis

como SPAM. Ele usa diversos métodos de análise para processar cada mensagem de e-mail, oferecendo o máximo de proteção possível contra mensagens de e-mail indesejáveis.

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

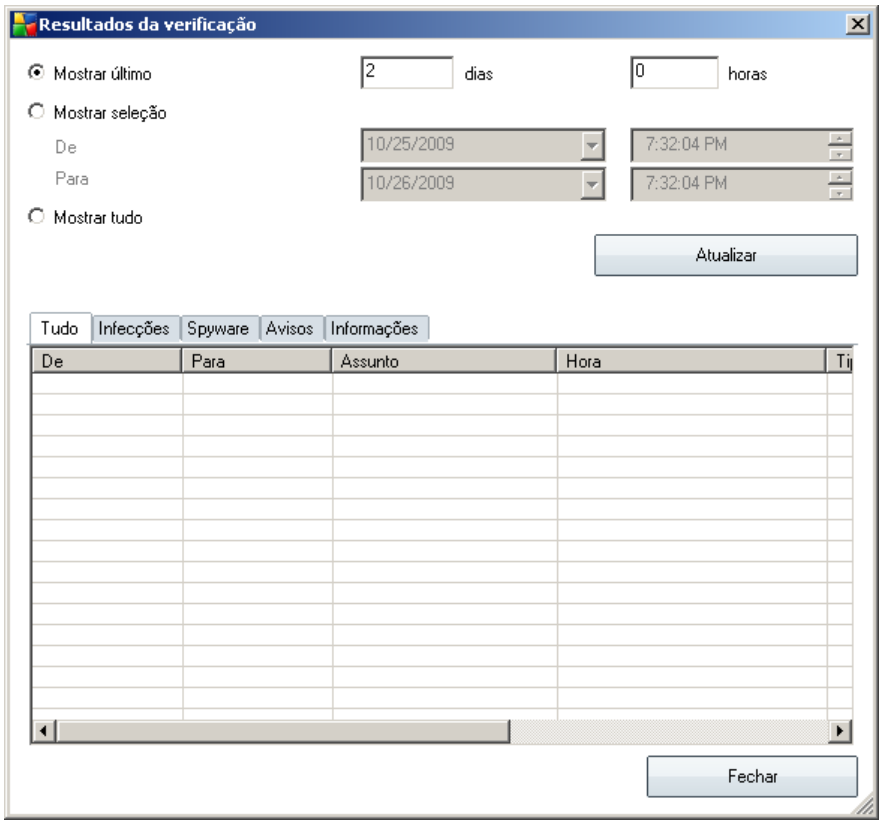
  Verifica todas as mensagens de e-mail armazenadas nas caixas de correio dos usuários. Se algum vírus for detectado, será movido para a Quarentena de vírus, ou removido completamente.

Dê um clique duplo em um componente necessário para abrir sua interface. Com a exceção do anti-spam, todos os componentes compartilham os seguintes links e botões de controle comum:

Links disponíveis:

- ***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*** - inserir dias e horas d preferência.
- ***Mostrar seleção*** - selecionar 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.
- ***Redefinir valores estatísticos*** - redefine todas as estatísticas para zero.

Os botões operacionais são os seguintes:

- ***Configurações*** - use este botão para abrir as configurações do componente.
- ***Voltar*** - pressione este botão para voltar para a visão geral dos componentes do Servidor

Você encontrará mais informações sobre configurações individuais de todos os componentes nos capítulos abaixo.

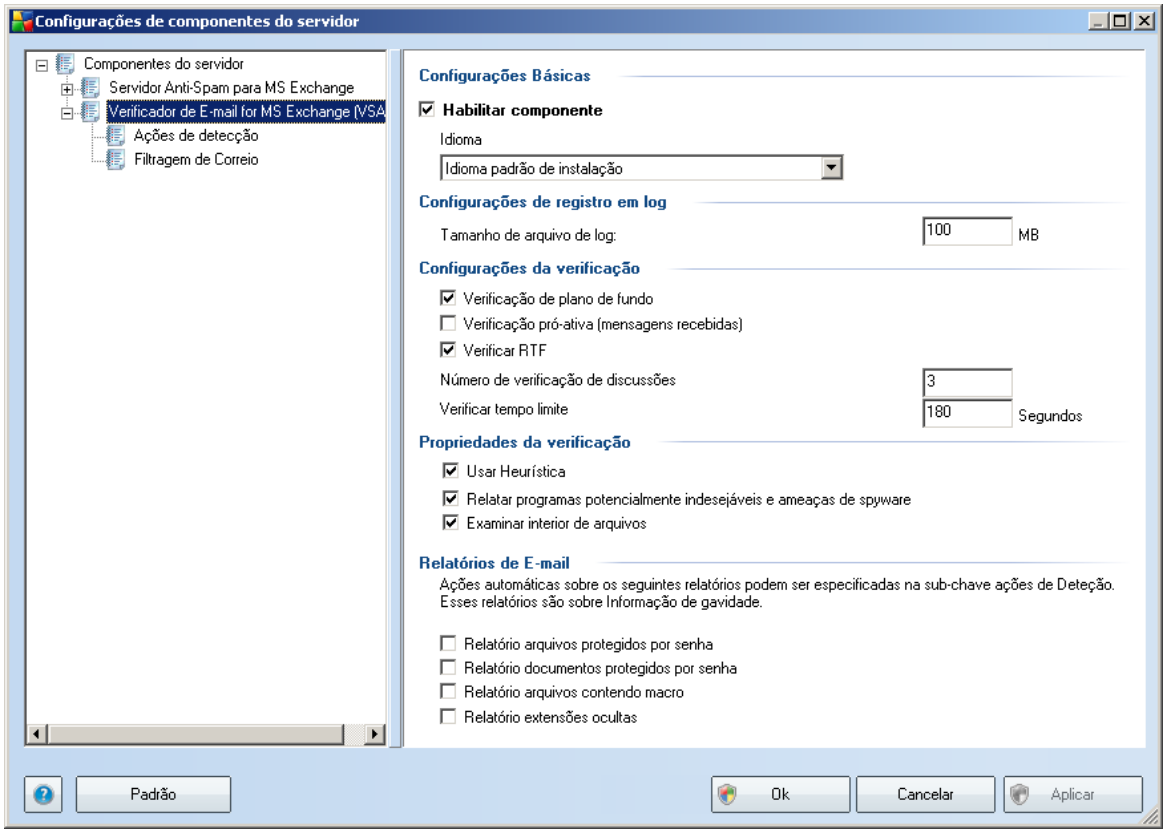
5.2. VSAPI 2.0

API 2.0 (VSAPI 2.0 conforme indicado no MS Exchange 2000 Server) de verificação de vírus não permite a exclusão de arquivos de e-mail infectados. Como não é possível excluir o anexo do e-mail infectado, seu nome de arquivo é alterado: o AVG para Exchange 2000/2003 Server anexa a extensão .virusinfo.txt ao nome do arquivo original. O conteúdo do arquivo é substituído por uma mensagem sobre o vírus conhecido. Se um vírus for encontrado diretamente na mensagem, todo o corpo dessa mensagem será substituído por um aviso informando que um vírus foi encontrado nela.

API 2.5 *(VSAPI 2.5 conforme indicado no MS Exchange 2003 Server)* de verificação de vírus também permite a exclusão de mensagens infectadas. Esse recurso pode ser definido na caixa de diálogo de configuração do AVG para MS Exchange 2000/2003 Server.

5.3. Verificador de e-mail para MS Exchange (VSAPI)

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



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

- ***Habilitar componente*** - desmarque para desativar todo o componente.
- ***Idioma*** - Selecione o idioma do componente preferida.

A seção ***Configurações de registro em log***:

- ***Tamanho de arquivo de log*** - escolha o tamanho preferido do arquivo de log. Valor padrão: 100 MB.

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

- ***Verificação em Segundo Plano****– você pode ativar ou desativar ao processo de verificação em segundo plano aqui.* 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 2007 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 e-mail 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.

  Nota: *: O excesso de mensagens continuará para a loja não autorizada.*

Observação: *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.
- ***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.

- Χαμπο ***Tempo Limite de Verificação*** - o intervalo contínuo máximo (em segundos) para que um processo acesse a mensagem sendo verificada).

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

- ***Use heurística*** - selecione esta caixa para ativar método de análise heurística durante a verificação.
- ***Informar ameaças de spyware e programas potencialmente indesejados*** - selecione está opção para informar a presença de spyware e programas potencialmente indesejados.
- ***Verificar dentro de arquivos*** - selecionar esta opção para permitir que o verificado busque dentro de arquivos de compactação(CEP, rar, etc.)

A seção***Informação de anexos de e-mail*** 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:

- ***Informar arquivos protegidos por senha***
- ***Informar documentos protegidos por senha***
- ***Informar arquivos de contenham macro***
- ***Informar extensões ocultas***

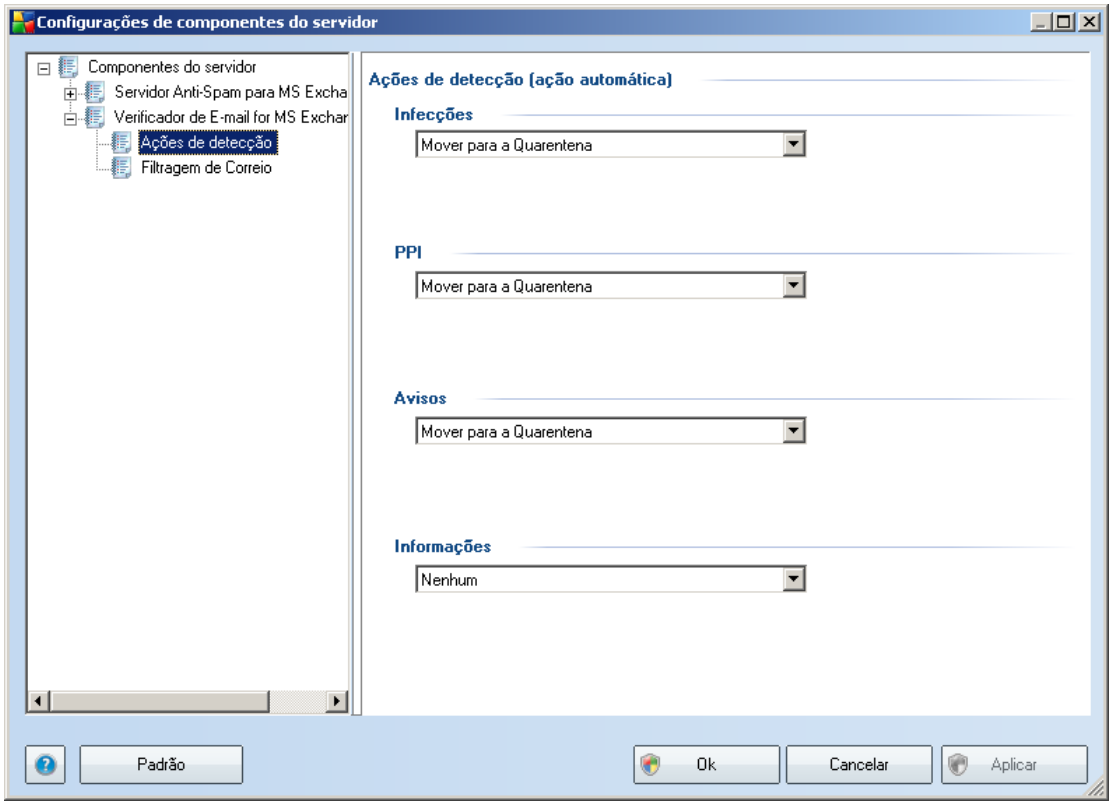
Geralmente, todos os recursos são extensões de usuário dos serviços da interface de aplicativo Microsoft VSAPI 2.0/2.5. Para obter informações detalhadas sobre a VSAPI 2.0/2.5, consulte os seguintes links (e também os links acessíveis pelos indicados):

- http://support.microsoft.com:80/support/kb/articles/Q285/6/67.ASP para obter informações gerais sobre a VSAPI 2.0 no Exchange 2000 Server Service Pack 1
- 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***

5.4. Detection_Actions



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:

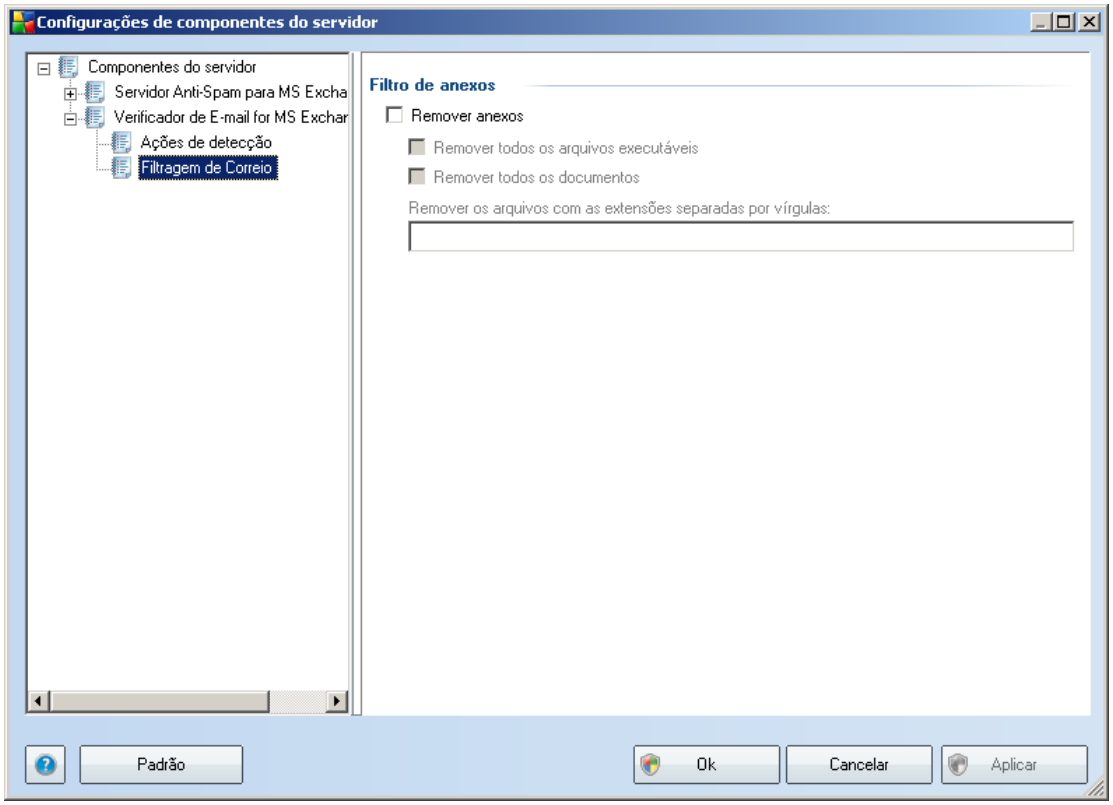
- ***Infecções***
- ***PPI (Programas Potencialmente Indesejáveis)***
- ***Avisos***

- ***Informações***

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

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

5.5. Filtragem de correio



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

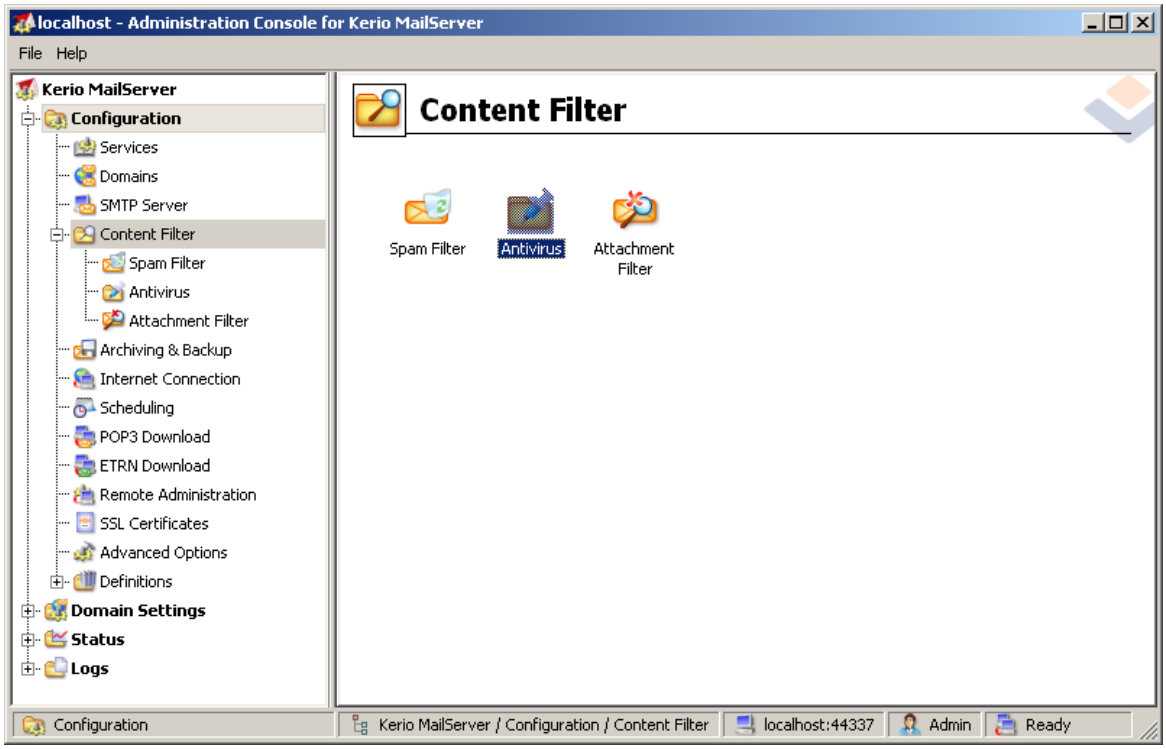
- ***Remover anexos*** - selecione esta caixa para ativar o recurso.

- ***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.

6. AVG para Kerio MailServer

6.1. Configuração

O mecanismo de proteção antivírus é integrado diretamente ao aplicativo Kerio MailServer. Para ativar a proteção de e-mail do Kerio MailServer pelo 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:

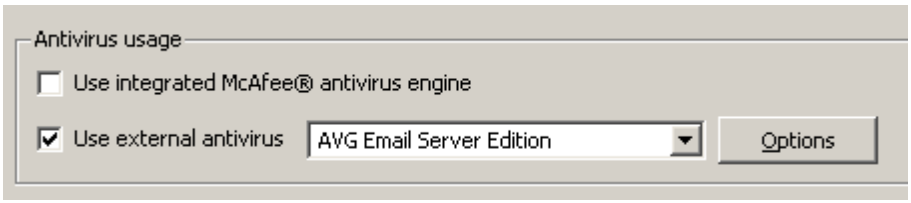


Se você clicar no item Filtro de conteúdo, aparecerá uma caixa de diálogo com três itens:

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

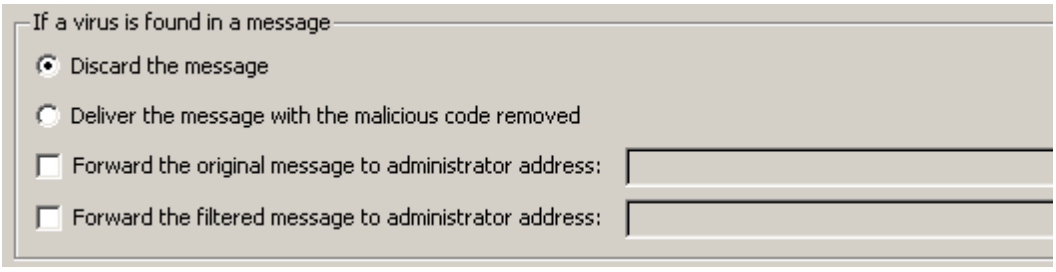
6.1.1. Antivírus

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:

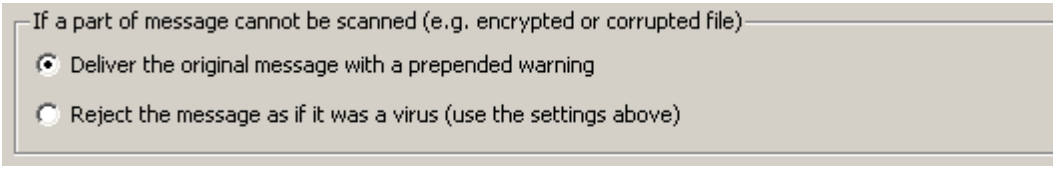
- ***Se um vírus for encontrado em uma mensagem***



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)***



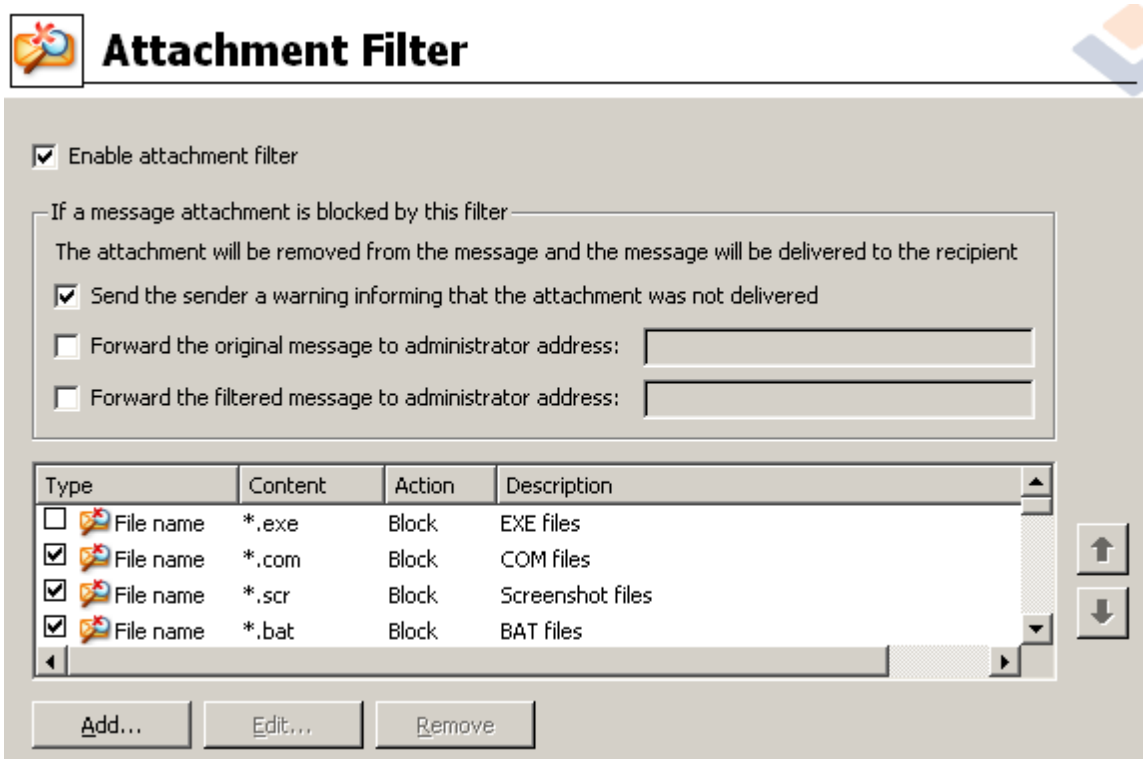
Este quadro especifica a ação a ser executada quando não é possível verificar parte da mensagem ou do anexo:

  - ***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.

6.1.2. 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 e-mail, 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 e-mail definido, independentemente de se tratar de um endereço local ou externo.

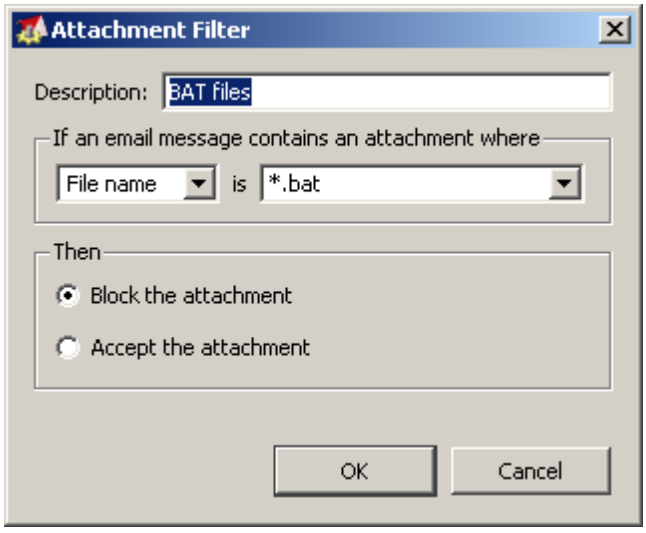
- ***Encaminhar a mensagem filtrada ao endereço do administrador***

A mensagem, sem seu anexo infectado ou proibido, será (além das ações selecionadas abaixo) encaminhada ao endereço de e-mail especificado. Essa 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*** – uma extensão a ser filtrada pode ser especificada aqui. 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 em particular. As ações possíveis são Aceitar (aceitar o anexo) e Bloquear (bloquear o anexo conforme definido na caixa de diálogo da guia Ação).
- ***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 escrever uma pequena descrição do anexo a ser

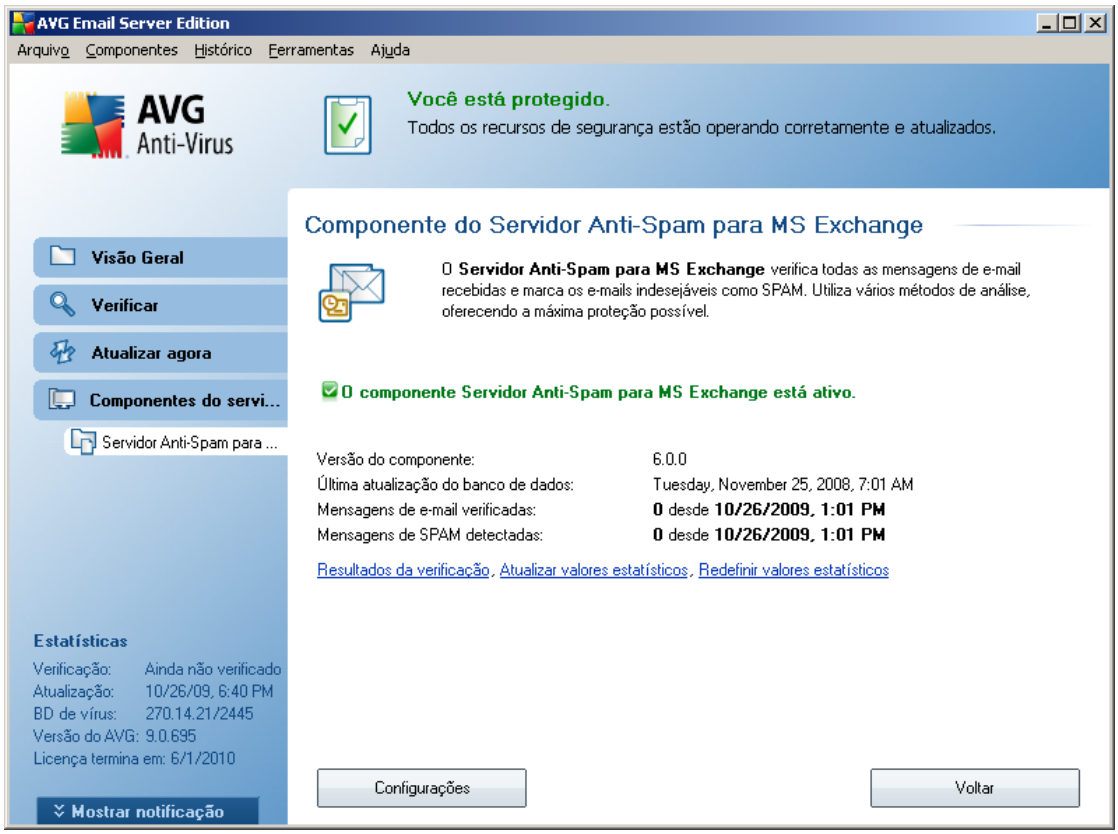
filtrado.

- No campo Se um e-mail 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.

7. Configuração Anti-Spam

7.1. Interface do Anti-Spam

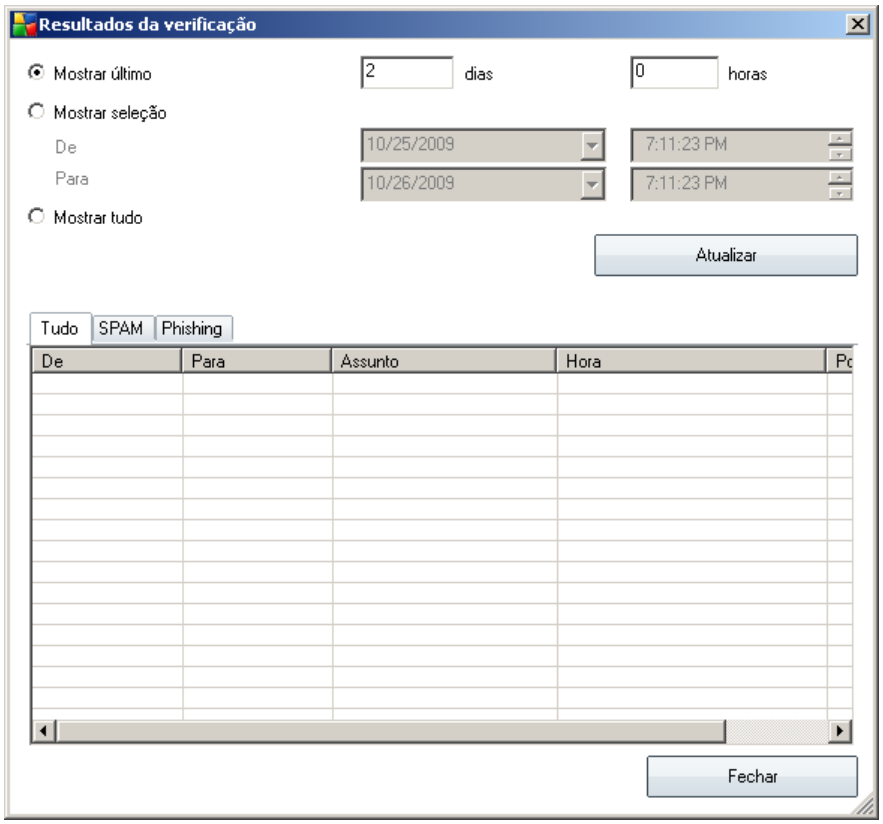


Você encontrará a caixa de diálogo do componente ***servidor*** Anti-spam na seção ***Componentes de Servidor*** (menu à esquerda). Ela contém uma breve informação sobre a funcionalidade do componente de servidor, informações sobre o status atual (*O componente Anti-Spam Server for MS Exchange está ativo.*) e algumas estatísticas.

Links disponíveis:

- ***Resultados da Verificação***

  Abre uma nova caixa de diálogo em que você pode revisar os resultados de verificação do anti-spam:



Aqui você pode verificar as mensagens detectadas como SPAM (mensagens indesejadas) ou como tentativa de phishing (um esforço para roubar seus dados pessoais, dados bancários, de identidade, etc). Por padrão são exibidos apenas os resultados dos últimos dois dias. Você pode alterar o período exibido, alterando as seguintes opções:

- ***Mostrar último*** - inserir dias e horas d preferência.
- ***Mostrar seleção*** - selecionar 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.
- ***Redefinir valores estatísticos*** - redefine todas as estatísticas para zero.

Os botões operacionais são os seguintes:

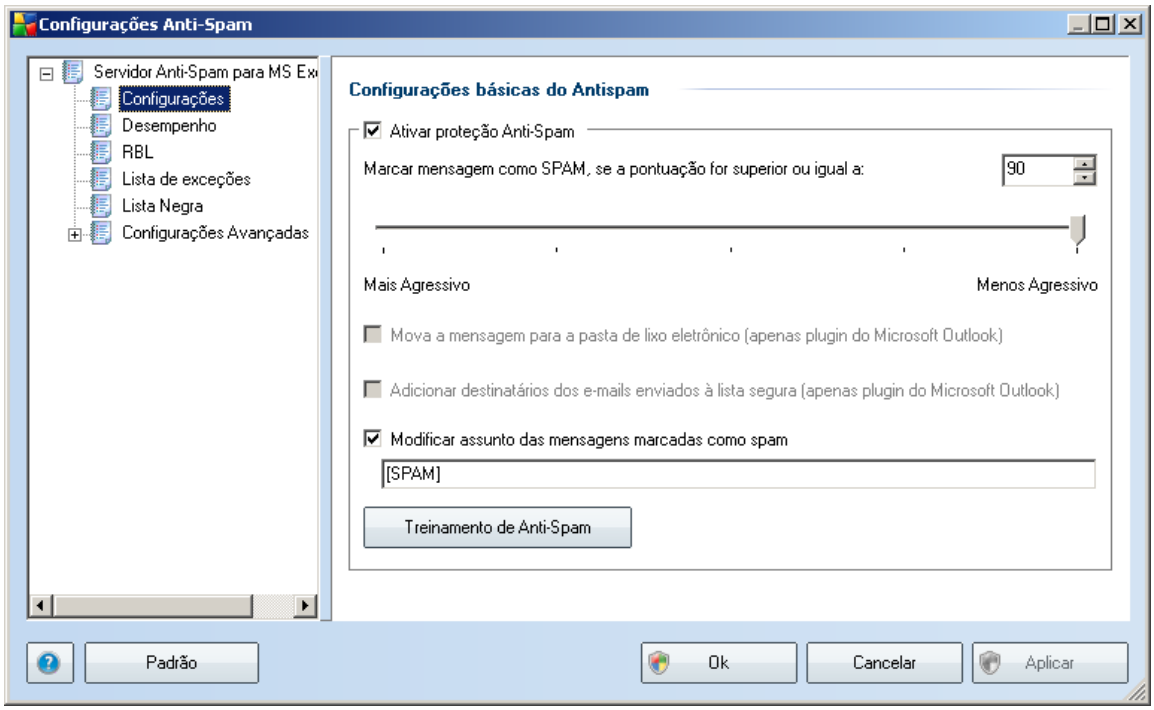
- ***Configurações*** - use este botão para abrir Configurações de anti-Spam
- ***Voltar*** - pressione este botão para voltar para a visão geral dos componentes do Servidor

7.2. Princípios do Anti-Spam

Spam refere-se a e-mail não solicitado, a maioria sendo propaganda de produto ou de serviço, enviada em grande quantidade para um grande número de endereços de e-mail ao mesmo tempo, enchendo as caixas de correio. O Spam não se refere a e-mail comercial válido, cujo envio conta com o consentimento por parte do cliente. 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 e-mail recebidas e marca os e-mails indesejáveis como SPAM. Ele usa diversos métodos de análise para processar cada mensagem de e-mail, oferecendo o máximo de proteção possível contra mensagens de e-mail indesejáveis.

7.3. Configurações Anti-Spam



Na caixa de diálogo ***Configurações básicas de anti-spam***, marque a caixa de seleção ***Ativar proteção do Anti-Spam*** para permitir/proibir a verificação anti-spam da comunicação por e-mail.

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 (*0 a 100*) ou movendo o controle deslizante para a esquerda ou para a direita (*usando o controle deslizante, o intervalo dos valores é limitado a 50 a 90*).

Em geral, recomendamos a definição do limite entre 50 e 90 ou, em caso de dúvidas, como 90. Veja uma análise geral do limite de pontuação:

- ***Valor entre 90 e 99*** - a maioria das mensagens de e-mail 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 e-mail 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 e-mail que provavelmente são spam serão filtradas. É provável que mensagens não spam também sejam bloqueadas

- ***Valor entre 1 e 59*** - configuração muito agressiva. É provável que mensagens de e-mail não spam sejam bloqueadas como verdadeiras mensagens spam. Esse intervalo limite não é recomendado para uso normal.

- ***Valor 0*** - nesse modo, você apenas receberá mensagens de e-mail de remetentes da sua ***Lista de Exceções*** . Todas as outras mensagens de e-mail serão consideradas spam.***Esse intervalo limite não é recomendado para uso normal.***

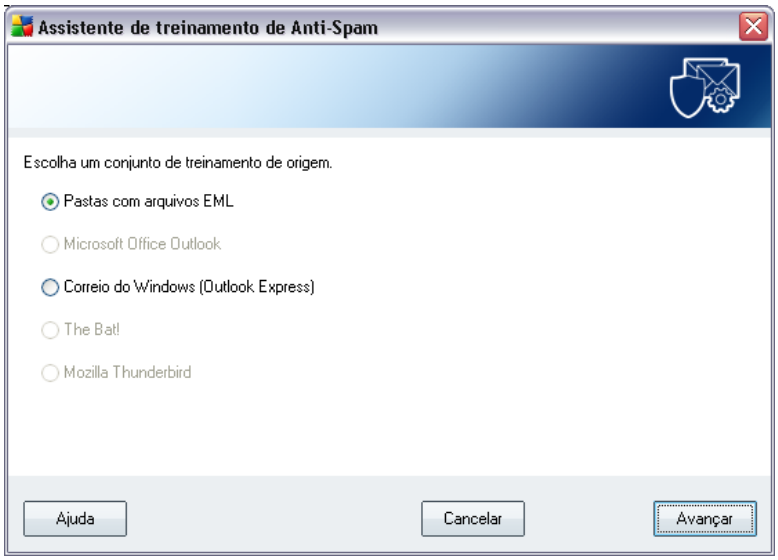
Você pode definir mais tarde como a mensagem de e-mail com spamdetectada deve ser tratada:

- ***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 e-mail. O texto desejado pode ser digitado no campo de texto ativado.

Botão Treinamento Anti-Spam abre o ***Assistente de treinamento Anti-Spam*** descrito de maneira detalhada no próximo capítulo.

7.3.1. Assistente de Treinamento Anti-Spam

A primeira caixa de diálogo do ***Assistente de treinamento de anti-spam*** solicita que você selecione a origem das mensagens de e-mail que deseja usar para treinamento. Normalmente, convém usar e-mails marcados incorretamente como SPAM ou mensagens de spam que não foram reconhecidas.



Existem as seguintes opções dentre as quais escolher:

- ***Um cliente de e-mail específico*** - se você usa um dos clientes de e-mail listados (*MS Outlook, Outlook Express, The Bat!, Mozilla Thunderbird*), basta selecionar a respectiva opção

- ***Pasta com arquivos EML*** - se você usa qualquer outro programa, salve primeiro as mensagens em uma pasta específica (em formato *.eml*) ou certifique-se de que conhece o local das pastas de mensagens do clente de e-mail. Em seguida, selecione ***Pasta com arquivos EML***, o que permitirá que você localize a pasta desejada na próxima etapa

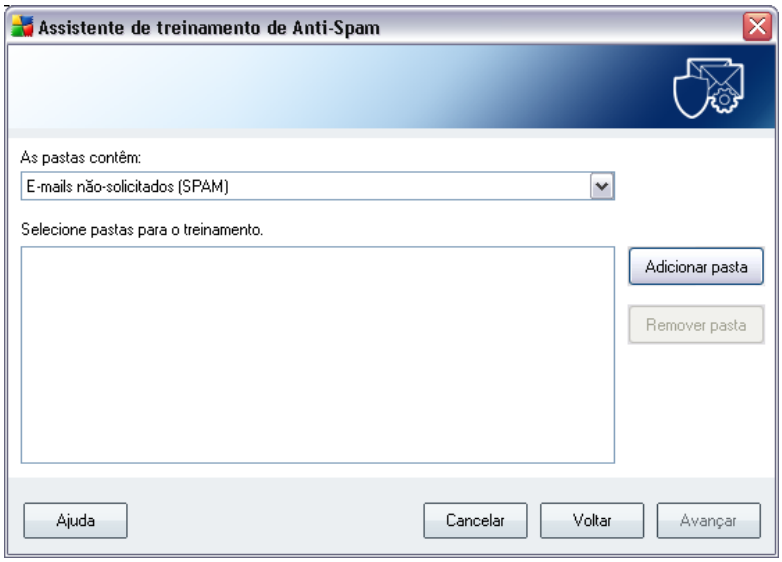
Para um processo de treinamento mais rápido e fácil, é uma boa idéia organizar os e-mails nas pastas antecipadamente, para que a pasta que você usará para treinamento contenha apenas as mensagens de treinamento (desejadas ou indesejadas). Entretanto, isso não é necessário, uma vez que você poderá filtrar os e-mails posteriormente.

Selecione a opção apropriada e clique em ***Avançar*** para continuar com o assistente.

7.3.2. Selecionar Pasta com Mensagens

A caixa de diálogo exibida nesta etapa depende da seleção anterior.

Pastas com arquivos EML



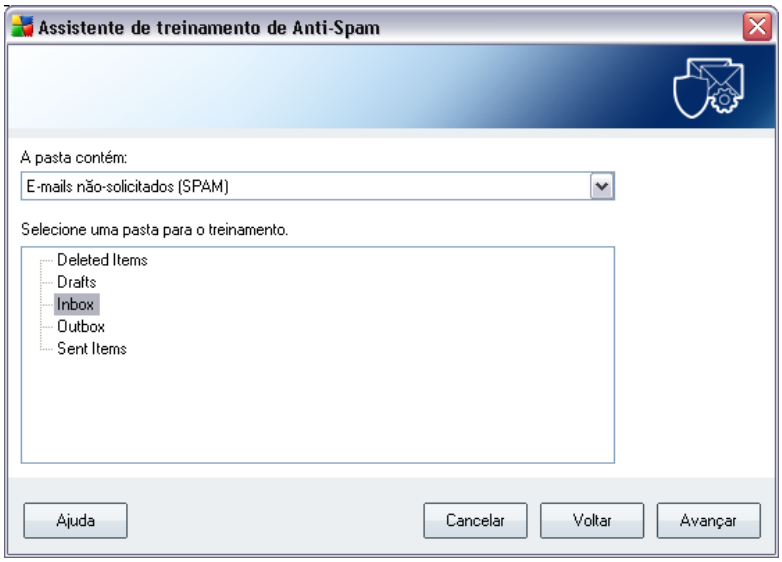
Nesta caixa de diálogo, selecione a pasta com as mensagens que deseja usar para treinamento. Pressione o botão ***Adicionar pasta*** para localizar a pasta com os arquivos .eml (*mensagens de e-mail salvas*). A pasta selecionada será exibida na caixa de diálogo.

No menu suspenso ***As pastas contêm***, defina uma das duas opções - se a pasta selecionada deve conter mensagens desejadas (*HAM*) ou mensagens não solicitadas (*SPAM*). Lembre-se de que você poderá filtrar as mensagens na próxima etapa, de modo que a pasta não precisa conter somente e-mails de treinamento. Você pode também remover as pastas selecionadas não desejadas da lista clicando no botão ***Remover pasta***.

Quando terminar, clique em ***Avançar*** e passe para ***Opções de filtragem de mensagem***.

Cliente de e-mail específico

Após confirmar uma das opções, será exibida uma nova caixa de diálogo.

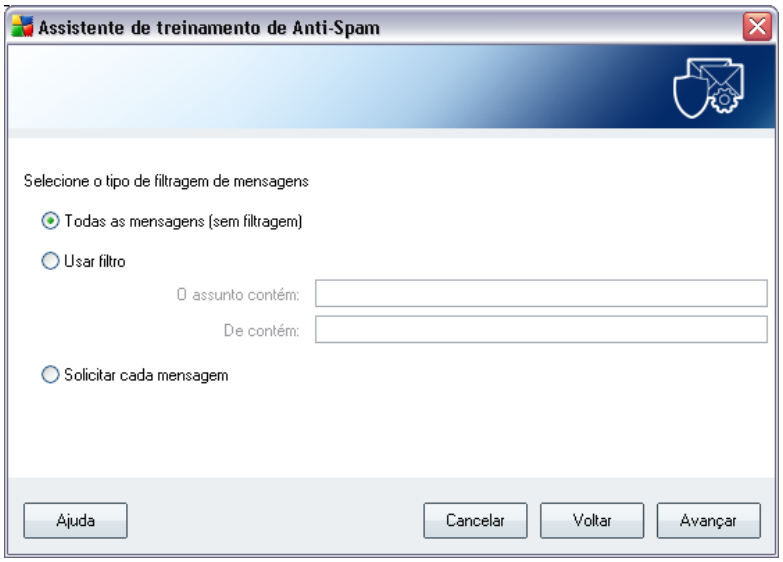


Nota: *No caso do Microsoft Office Outlook, será necessário selecionar o perfil do MS Office Outlook primeiro.*

No menu suspenso ***As pastas contêm***, defina uma das duas opções - se a pasta selecionada deve conter mensagens desejadas (*HAM*) ou mensagens não solicitadas (*SPAM*). Lembre-se de que você poderá filtrar as mensagens na próxima etapa, de modo que a pasta não precisa conter somente e-mails de treinamento. Uma árvore de navegação do cliente de e-mail selecionado já está exibida na seção principal da caixa de diálogo. Localize a pasta desejada na árvore e realce-a com o seu mouse.

Quando terminar, clique em ***Avançar*** e passe para ***Opções de filtragem de mensagem***.

7.3.3. Opções de filtragem de mensagens



Nesta caixa de diálogo, você poderá definir a filtragem das mensagens de e-mail.

Se tiver certeza de que a pasta selecionada contém apenas as mensagens que deseja usar para treinamento, selecione a opção ***Todas as mensagens (sem filtragem)***.

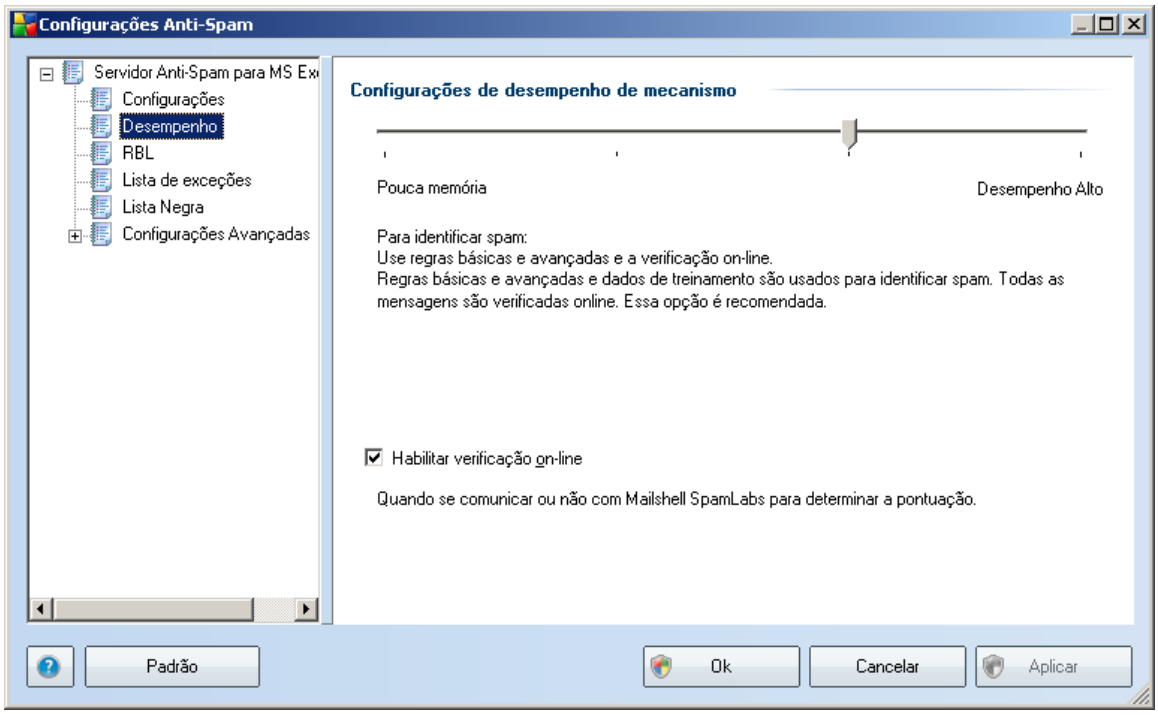
Se você não estiver certo sobre as mensagens contidas na pasta e quiser que o assistente faça perguntas sobre cada mensagem (para poder determinar se ela deve ser usada para treinamento ou não), selecione a opção ***Perguntar por cada mensagem***.

Para uma filtragem mais avançada, selecione a opção ***Usar filtro***. Você pode inserir uma palavra *nome*), parte de uma palavra ou frase a ser pesquisada no assunto de e-mail e/ou no campo do remetente. Todas as mensagens que corresponderem exatamente aos critérios inseridos serão utilizadas para treinamento, sem outras perguntas.

Atenção!: *Quando você preenche ambos os campos de texto, os endereços que correspondem a apenas uma das duas condições serão usados também!*

Quando a opção apropriada for selecionada, clique em ***Avançar***. A caixa de diálogo a seguir terá caráter apenas informativo, informando que o assistente está pronto para processar as mensagens. Para iniciar o treinamento, clique no botão ***Avançar*** novamente. O treinamento será iniciado de acordo com as condições selecionadas previamente.

7.4. 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.

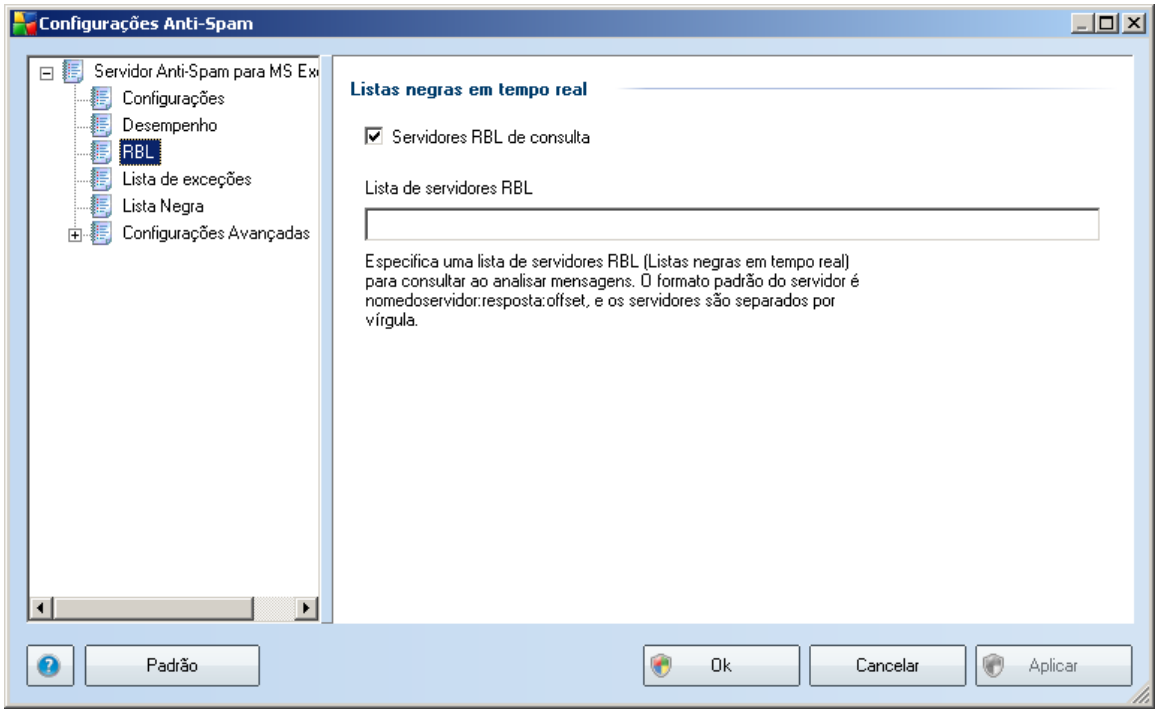
- ***Alto desempenho*** - Esse modo consumirá muita memória. Durante o processo de verificação para identificar um spam, os seguintes recursos serão usados: cache do banco de dados de regras e spam, regras básicas e avançadas, endereços IP de spam e bancos de dados de spam.

O item ***Habilitar verificação online*** fica ativado por padrão. Ele resulta em uma detecção de spam mais precisa por meio da comunicação com os servidores Mailshell, isto é, os dados verificados serão comparados com o.

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

7.5. RBL

O item ***RBL*** abre uma caixa de diálogo denominada ***Realtime Blackhole Lists***:



Nessa caixa de diálogo, você pode ativar/desativar a função ***Consultar servidores RBL***.

O servidor RBL (*Realtime Blackhole Lists*) é um servidor DNS com um amplo banco de dados de remetentes de spam. Quando esse recurso estiver ativado, todas as mensagens de e-mail serão verificadas no banco de dados do servidor RBL e marcadas como spam, se forem idênticas a qualquer uma das entradas do banco de dados.

Os bancos de dados dos servidores RBL contêm as impressões de spam atualizadas por minuto, mais recentes, para fornecer a melhor e mais precisa detecção de spam. Este recurso é especialmente útil para usuários que recebem grandes quantidades de spam que não estão sendo detectados normalmente pelo mecanismo de Anti-Spam.

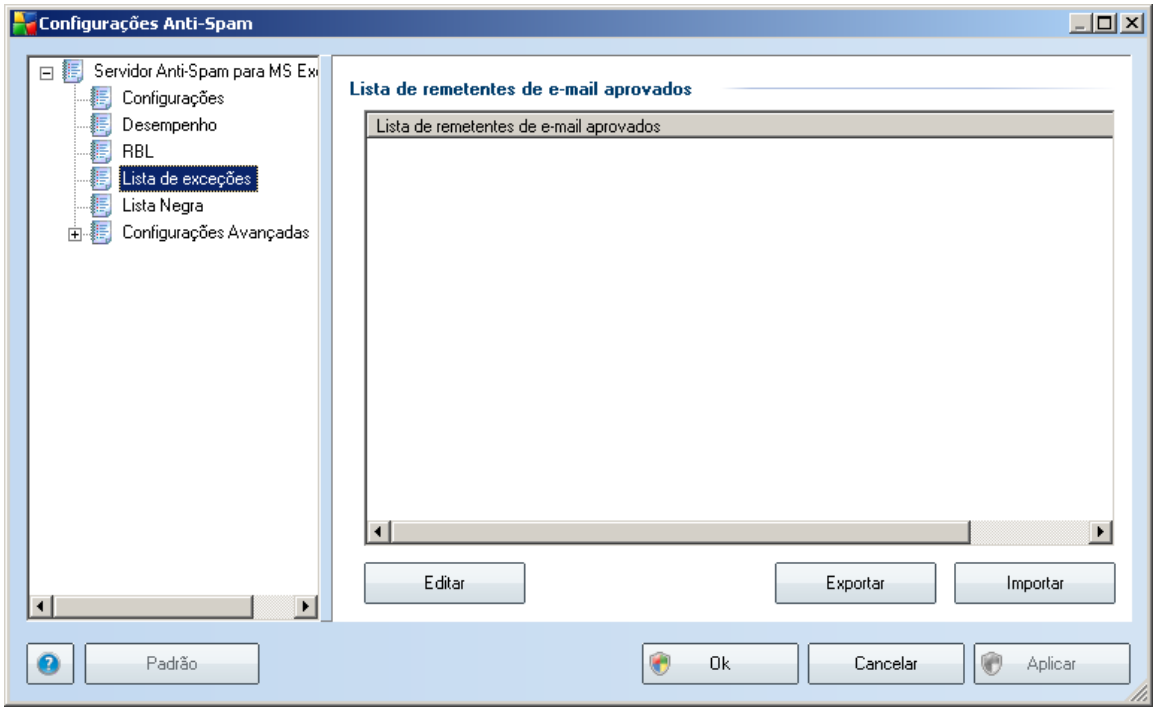
A ***Lista de servidores RBL*** permite definir locais de servidores RBL específicos. Por padrão, dois endereços de servidores RBL são especificados. Recomendamos manter as configurações padrão, a menos que você seja um usuário experiente e precise realmente alterar essas configurações!

Observação: *ativar este recurso poderá reduzir a velocidade do processo de recebimento de e-mail em alguns sistemas e configurações, pois cada mensagem deve ser verificada no banco de dados do servidor RBL.*

Nenhum dado pessoal é enviado ao servidor!

7.6. Lista de exceções

O item ***Lista de exceções*** abre uma caixa de diálogo com uma lista global de endereços de e-mail 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 e-mail ou importando toda a lista de endereços de uma vez. Os seguintes botões estão disponíveis:

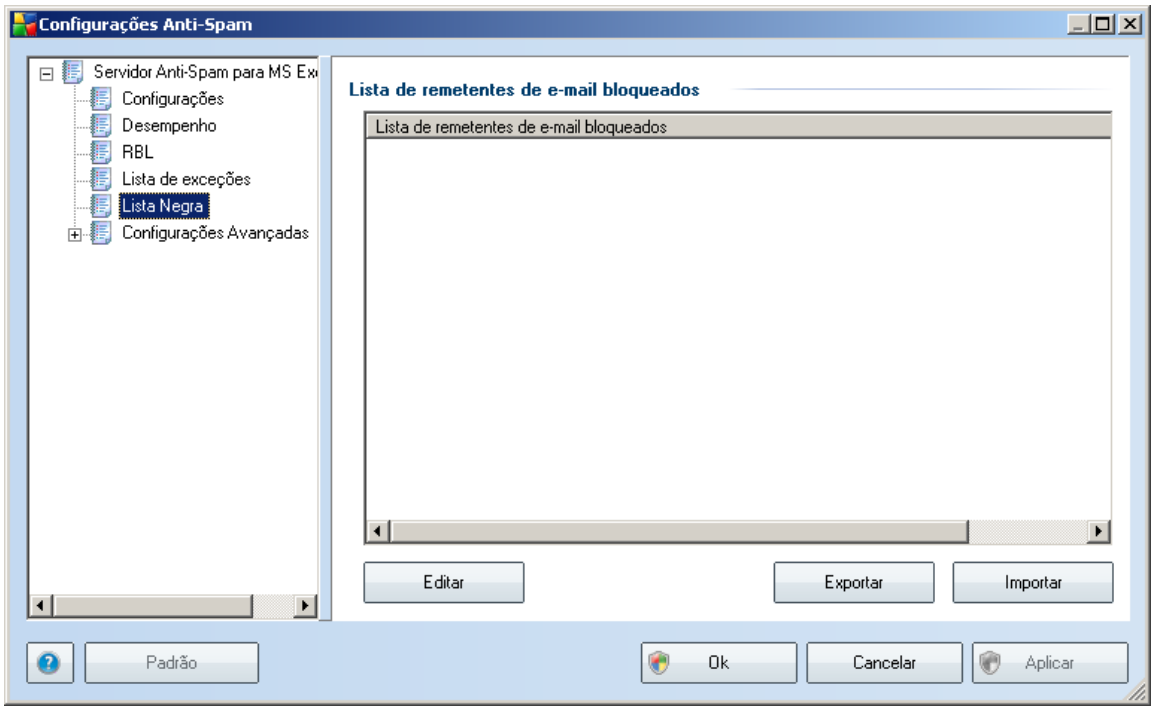
- ***Editar*** - pressione este botão para abrir uma caixa de diálogo na qual é possível inserir manualmente uma lista de endereços (você pode usar *o método copiar/ colar*). Insira um item (remetente, nome do domínio) por linha.

- ***Importar*** - se você já tiver preparado um arquivo de texto contendo os endereços de e-mail ou nomes de domínio, basta importá-lo, selecionando este botão. O arquivo de entrada deve estar no formato de texto simples e o conteúdo deve ter um item apenas (endereço, nome do domínio) por linha.

- ***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.

7.7. Lista Negra

O item ***Lista negra*** abre uma caixa de diálogo com uma lista global de endereços de e-mail 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 e-mail/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 e-mail 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*** - se você já tiver preparado um arquivo de texto contendo os endereços de e-mail ou nomes de domínio, basta importá-lo, selecionando este botão. O arquivo de entrada deve estar no formato de texto simples e o conteúdo deve ter um item apenas (endereço, nome do domínio) por linha.
- ***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.

7.8. Configurações Avançadas

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

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 e poderá editá-lo. Sua descrição é sempre incluída na caixa.

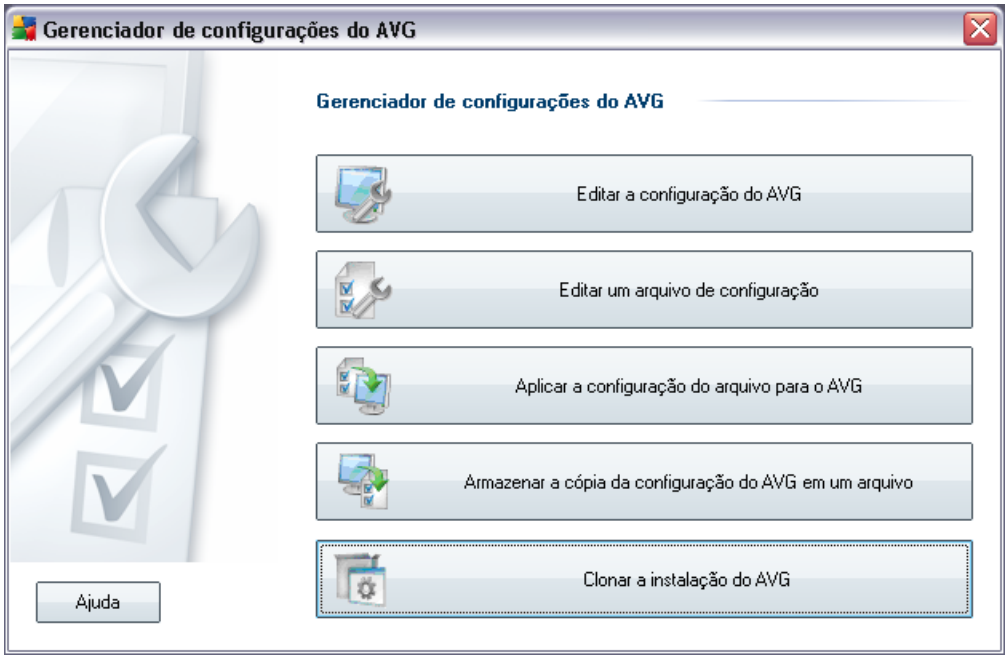
- ***Cache*** - impressão digital, reputação do domínio, LegitRepute
- ***Treinamento*** - treinamento da palavra, histórico da pontuação, deslocamento da pontuação, máximo de entradas de palavras, limite do auto-treinamento, peso, buffer para gravação
- ***Filtragem*** - lista de idiomas, lista de países, 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*** - tempo limite, servidor proxy, autenticação de servidor proxy

8. Gerenciador de Configurações do AVG

O ***Gerenciador de Configurações do AVG*** é uma ferramenta adequada principalmente para redes pequenas que permite copiar, editar e distribuir as configurações do AVG. A configuração pode ser salva em um dispositivo portátil (unidade flash USB etc.) e aplicada manualmente nas estações escolhidas.

A ferramenta está inclusa na instalação do AVG e disponível no menu Iniciar do Windows:

Todos os programas/ <%VER%>AVG/Gerenciador de Configurações do AVG



- ***Editar as configurações do AVG neste computador***

  Use esse botão para abrir a caixa de diálogo com as configurações avançadas do seu AVG local. Todas as modificações feitas aqui também refletirão na instalação local do AVG.

- ***Carregar e editar o arquivo de configuração do AVG***

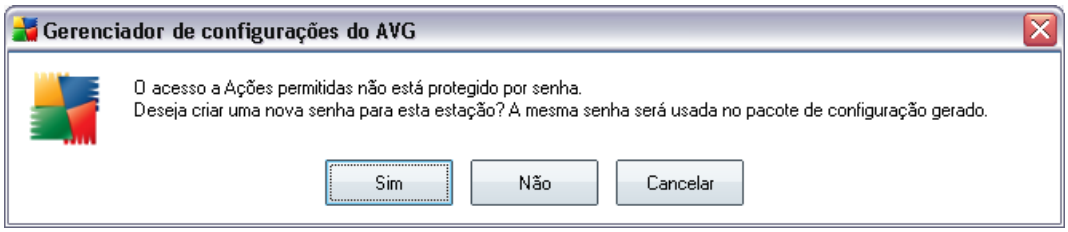
  Se você já possui um arquivo de configuração do AVG (.pck), use este botão para abri-lo e editá-lo. Quando você confirmar as suas modificações com o botão ***OK*** ou ***Aplicar***, o arquivo será substituído pelas novas configurações!

- ***Aplicar configurações de arquivo ao AVG neste computador***

  Use este botão para abrir um arquivo de configuração do AVG (.pck) e aplicá-lo à instalação local do AVG.

- ***Armazenar a configuração do AVG local em um arquivo***

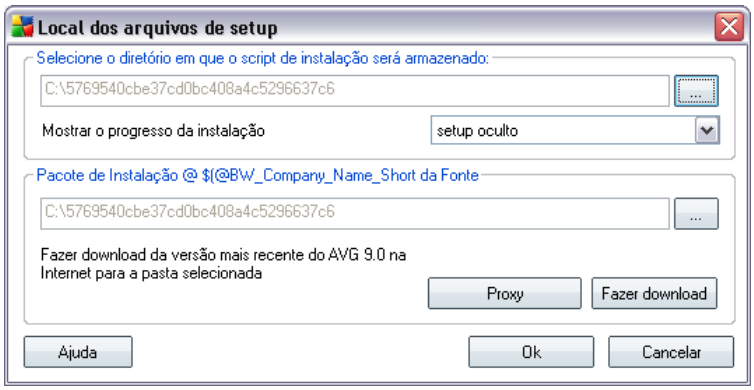
  Use este botão para salvar o arquivo de configuração da (.pck) instalação local do AVG. Se não tiver configurado uma senha para as Ações permitidas, pode ocorrer a seguinte caixa de diálogo:



Responder ***Sim*** se desejar configurar a senha para acesso para Itens permitidos agora, preencha as informações solicitadas e confirme sua escolha. Responder ***Não*** para ignorar a criação de senha e continuar para salvar a configuração do AVG local para um arquivo.

- ***Clonar instalação do AVG***

  Esta opção permite que você faça uma cópia exata do local de instalação do AVG através da criação de um pacote de instalação com opções personalizadas. Para continuar, primeiro selecione a pasta na qual o script de instalação será salvo.



No menu suspenso selecione uma das seguintes opções:

- ***Instalação oculta*** - nenhuma informação será exibida durante o processo de instalação.

- ***Exibir apenas progresso de instalação*** - a instalação não exigirá nenhuma atenção do usuário, mas o progresso estará totalmente visível.

- ***Exibir assistente de instalação*** - a instalação estará visível e o usuário precisará confirmar manualmente todas as etapas.

Use o botão ***Download***

Você pode usar o botão ***Proxy*** para definir as configurações do servidor proxy se sua rede exigir isto para uma conexão com sucesso.

Clicando em ***OK*** o processo de clonagem iniciará e deve terminar em breve. Também pode aparecer uma caixa de diálogo perguntando sobre a senha de configuração para os itens Permitidos (veja acima). Assim que terminar, o ***AvgSetup.bat*** deve estar disponível na pasta escolhida junto com outros arquivos. Se você executar o arquivo ***AvgSetup.bat***, ele instalará o AVG de acordo com os parâmetros escolhidos acima.

9. Perguntas Freqüentes 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 e-mail. Use o formulário de contato que pode ser acessado do menu do sistema via ***Ajuda/Obter ajuda online***.