AVG Email Server Edition 2011

Manual do Usuário

Revisão do documento 2011.01 (22. 9. 2010)

Conteúdo

1. Introdução

Este manual do usuário fornece uma documentação completa para o **AVG Email Server Edition 2011**.

Parabéns pela aquisição do AVG Email Server Edition 2011!

O AVG Email Server Edition 2011**é um dos vários produtos AVG premiados 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 Email Server Edition 2011** foi completamente reprojetado para fornecer a proteção e a segurança certificada e renomada do AVG em uma nova forma, mais eficiente e amigável. Seu novo produto AVG Email Server Edition 2011 **tem uma interface simples combinada com uma verificação mais agressiva e rápida.** Mais recursos de segurança foram automatizados para sua conveniência e novas e inteligentes opçõespara o usuário foram incluídas, de forma que você possa adequar nossos recursos de segurança à sua forma de vida. A utilização não será mais comprometida em função da segurança!

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

Todos os produtos AVG oferecem

- Proteção relevante para a forma como você usa seu computador e a Internet: transações bancárias e compras, navegação e pesquisa, bate-papo e envio de email ou download de arquivos e redes sociais - a AVG tem o produto de proteção certo para você
- Proteção isenta de problemas confiável usada por mais de 110 milhões de pessoas em todo o mundo e alimentada por uma rede global de pesquisadores altamente experientes
- Proteção com suporte especializado

2. Requisitos de instalação do AVG

2.1. Sistemas operacionais suportados

O **AVG Email Server Edition 2011** destina-se à proteção de estações de trabalho/ servidores com os seguintes sistemas operacionais:

- Windows 2003 Server e Windows 2003 Server x64 Edition
- Windows 2008 Server e Windows 2008 Server x64 Edition

(e possíveis service packs posteriores para sistemas operacionais específicos)

2.2. Requisitos de HW mínimos e recomendados

Requisitos mínimos de hardware para **AVG Email Server Edition 2011**:

- CPU Intel Pentium 1,5 GHz
- 512 MB de memória RAM
- 470 MB de espaço livre em disco rígido (para fins de instalação)

Requisitos recomendados de hardware para **AVG Email Server Edition 2011**:

- CPU Intel Pentium 1,8 GHz
- 512 MB de memória RAM
- 600 MB de espaço livre em disco rígido (para fins de instalação)

3. Opções de instalação do AVG

O AVG pode ser instalado a partir do arquivo de instalação disponível no CD de instalação, ou você pode baixar o arquivo de instalação mais recente no site da AVG (http://www.avg.com).

Antes de começar a instalar o AVG, é recomendável que você visite o site da AVG (http://www.avg.com) para verificar se há um novo arquivo de instalação. Dessa forma, você poderá ter certeza de instalar a versão mais recente disponível de AVG Email Server Edition 2011.

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 sua cópia do AVG on-line, o número da licença foi enviado para você por e-mail.

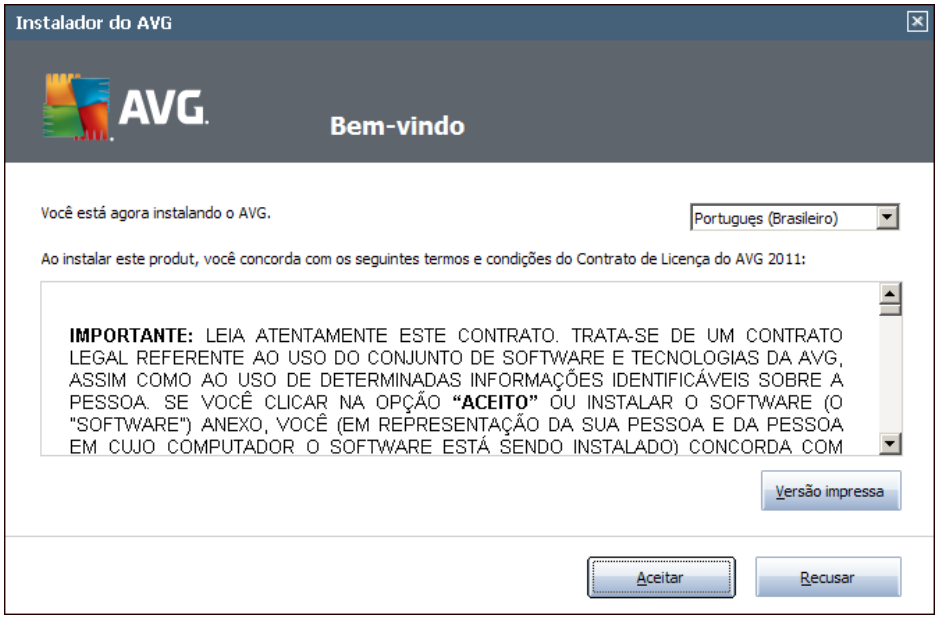
4. Processo de instalação do AVG

Para instalar o **AVG Email Server Edition 2011** em seu computador, você precisa 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 http://www.avg.com), seção ***Suporte e Download.***

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:

4.1. Bem-vindo

O processo de instalação é iniciado com a janela da caixa de diálogo ***Boas-vindas***. Aqui, é possível selecionar o idioma usado para o processo de instalação e o idioma padrão da interface do usuário do AVG. Na seção superior da janela da caixa de diálogo, localize o menu suspenso com a lista dos idiomas que podem ser escolhidos:



Atenção: *aqui você está selecionando o idioma para o processo de instalação. O idiomas selecionado será instalado como padrão para a interface do usuário do AVG, junto com inglês, que é instalado automaticamente. Se quiser instalar outros idiomas para a interface do usuário, defina-os na caixa de diálogo de configuração* ***Opções Personalizadas****.*

Além disso, essa caixa de diálogo fornece o contrato de licença completo do AVG. Leia-o com atenção. Para confirmar que leu, compreendeu e aceita o contrato, pressione o botão ***Aceitar***. Se você não concordar com o contrato de licença, pressione o botão Recusar e o processo de instalação será encerrado imediatamente.

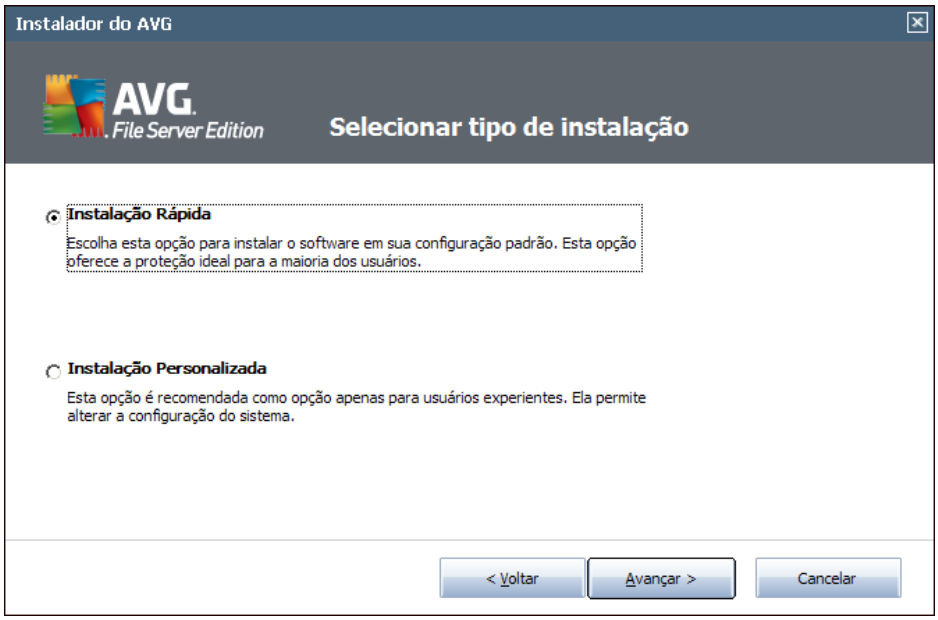
4.2. Ativar sua licença do AVG

Na caixa de diálogo ***Ativar sua Licença***, você deverá fornecer o número da sua licença no campo de texto fornecido.

O número de vendas pode ser encontrado no CD fornecido na embalagem do **AVG Email Server Edition 2011**. O número da licença está no e-mail de confirmação recebido depois da aquisição do AVG Email Server Edition 2011 **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.

4.3. Selecionar tipo de instalação



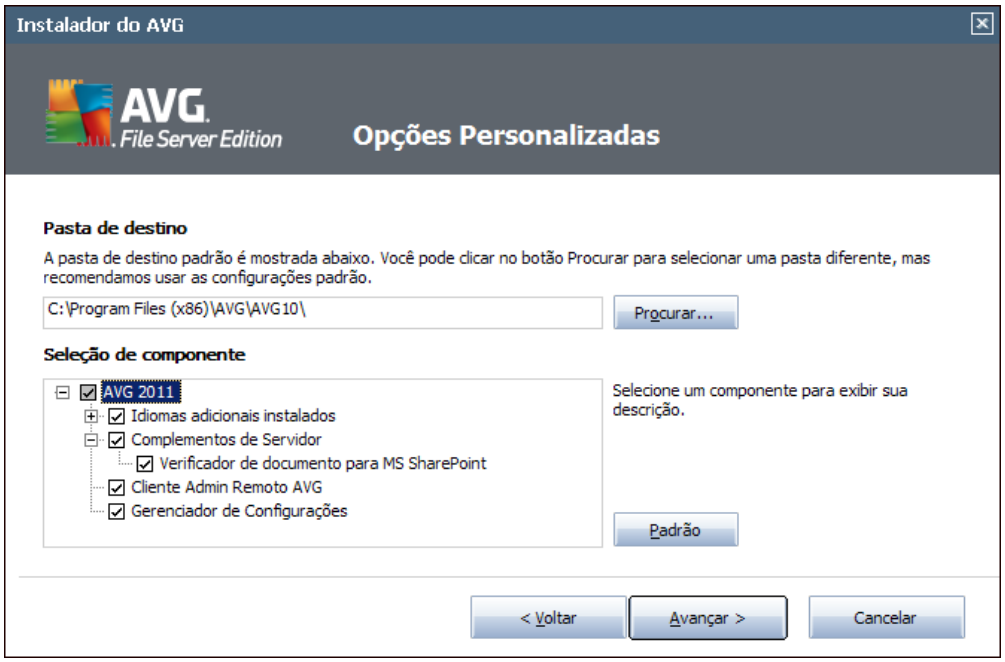
A caixa de diálogo ***Selecionar tipo de instalação*** oferece duas opções de instalação: ***Instalação Rápida*** e ***Instalação Personalizada***.

Para a maioria dos usuários, é altamente recomendável manter a ***Instalação Rápida*** 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. Se você tiver selecionado a opção ***Instalação Rápida***, pressione o botão ***Próximo*** para avançar para a caixa de diálogo ***Progresso da Instalação*** seguinte.

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. Após selecionar esta opção, pressione o botão ***Próximo*** para avançara para a caixa de diálogo ***Opções Personalizadas***.

4.4. Opções personalizadas

A caixa de diálogo ***Opções Personalizadas*** permite configurar dois parâmetros da instalação:



Pasta de destino

Na seção ***Pasta de Destino*** da caixa de diálogo, você deve especificar o local onde o **AVG Email Server Edition 2011** deve ser instalado. Por padrão, o AVG será instalado na pasta Arquivos de programas da unidade C:. Se a pasta ainda não existir, uma nova caixa de diálogo solicitará que você confirme se deseja que o AVG a crie agora. Se você desejar alterar esse local, use o botão ***Procurar*** para exibir a estrutura da unidade e selecionar a respectiva pasta.

Seleção de componente

A seção ***Seleção de Componente*** exibe uma visão geral de todos os componentes **AVG Email Server Edition 2011** 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!

Selecione qualquer item na lista ***Seleção de Componente***, e uma breve descrição do respectivo componente será exibida no lado direito desta seção.

- ***Seleção de idioma***

  Na lista de componentes a serem instalados, você poderá definir em que idioma (s) o AVG deverá ser instalado. Marque o item ***Idiomas adicionais instalados*** e selecione os idiomas desejados no respectivo menu.

- ***Suplementos do servidor - Verificador de Documentos para MS SharePoint***

  Este componente verifica arquivos de documento armazenados no MS É uma parte essencial do todo **AVG Email Server Edition 2011**, portanto é recomendável instalá-lo.

- ***Cliente de Administração Remota do AVG***

  Se você planeja conectar o computador à Administração Remota do AVG, marque o respectivo item para que ele também seja instalado.

- ***Gerenciador de Configurações***

  O Gerenciador de Configurações do é um pequeno aplicativo que permite configurar, de maneira simples e rápida, instalações locais (mesmo as que não estiverem em execução no Administração Remota). Ele usa arquivos de configuração (em formato .pck) que podem ser criados facilmente usando o Gerenciador de Configurações do AVG em todo computador com o aplicativo AVG instalado. Você pode então copiar esses arquivos para qualquer dispositivo removível e usá-los em qualquer computador. Obviamente, o mesmo se aplica ao Gerenciador de configurações em si. Para obter mais informações sobre esse aplicativo, clique **aqui**.

Pressione o botão ***Avançar*** para continuar.

4.5. Progresso da Instalação

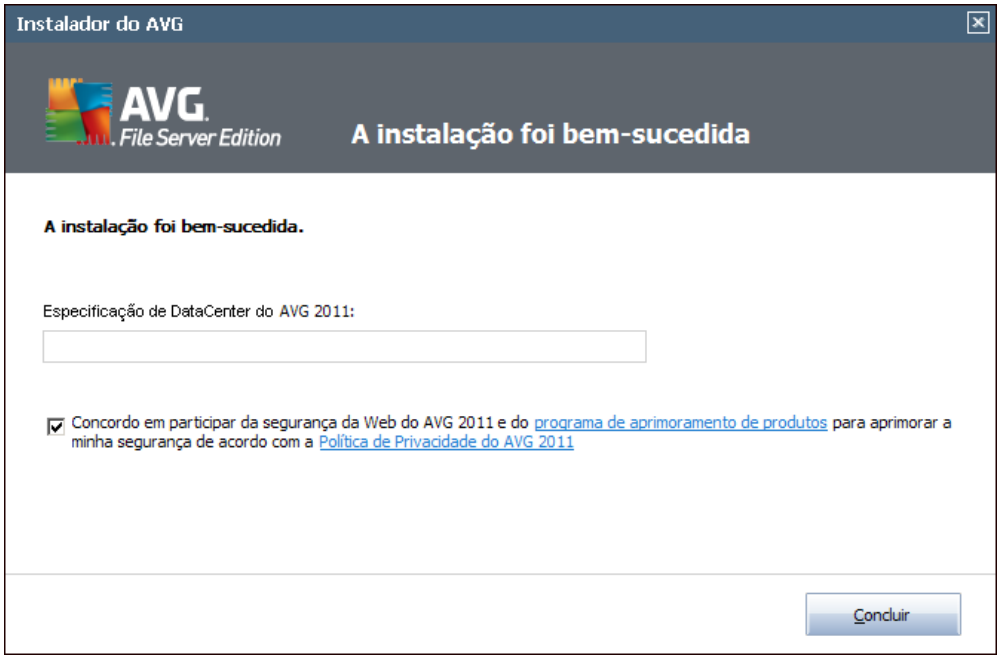
A caixa de diálogo ***Progresso da Instalação*** mostra o andamento do processo de instalação e não requer intervenção.

Após o processo de instalação terminar, o programa e o banco de dados de vírus serão atualizados automaticamente. Em seguida, você será redirecionado à próxima caixa de diálogo.

4.6. Instalação bem sucedida

A caixa de diálogo ***Instalação realizada com êxito*** confirma que o **AVG Email Server Edition 2011** foi totalmente instalado e configurado.

Se você tiver selecionado anteriormente o item Cliente de Administração Remota do AVG para ser instalado (consulte Opções Personalizadas), a caixa de diálogo aparecerá com a seguinte interface:



É preciso especificar os parâmetros do AVG DataCenter - forneça a string de conexão para o AVG DataCenter, no formato servidor:porta. Se essas informações não estiverem disponíveis no momento, deixe o campo em branco, e você poderá definir a configuração mais tarde, na caixa de diálogo Configurações avançadas / Administração remota. Para obter informações detalhadas sobre a administração remota do AVG, consulte o manual do usuário do AVG Business Edition, que pode ser baixado no site da AVG (http://www.avg.com).

Concordo em participar do Programa de Aprimoramento de Produto e Segurança na Web do AVG 2011 ... - marque esta caixa de seleção para concordar que deseja participar do Programa de Aprimoramento de Produto (*para mais detalhes, veja o capítulo Configurações Avançadas/Programa de Aprimoramento de Produto AVG*) que coleta informações anônimas sobre ameaças detectadas para aumentar o nível de segurança geral na Internet.

5. Após a instalação

5.1. Registro do produto

Ao concluir a instalação do **AVG Email Server Edition 2011**, registre o produto online no site do AVG (http://www.avg.com), página ***Registro*** *(siga as instruções fornecidas diretamente na página*). Depois do registro, você terá acesso completo à sua conta de usuário do AVG, ao boletim informativo de atualização do AVG e a outros serviços fornecidos exclusivamente para usuários registrados.

5.2. Acesso à interface do usuário

A ***Interface do Usuário do AVG*** pode ser acessada de várias formas:

- clique duas vezes no ***ícone da bandeja de sistema do AVG***
- clique duas vezes no ícone do AVG na área de trabalho
- no menu ***Iniciar/Programas/AVG 2011/Interface do Usuário do AVG***

5.3. Verificação de todo o computador

Existe um risco potencial de um vírus de computador ter sido transmitido ao seu computador antes da instalação do **AVG Email Server Edition 2011** . Por esse motivo, você deve executar uma ***verificação de todo o computador*** para assegurar que seu PC não esteja infectado.

Para obter instruções sobre a ***Verificação em todo o computador,*** consulte o capítulo ***Verificação do AVG***.

5.4. Configuração padrão do AVG

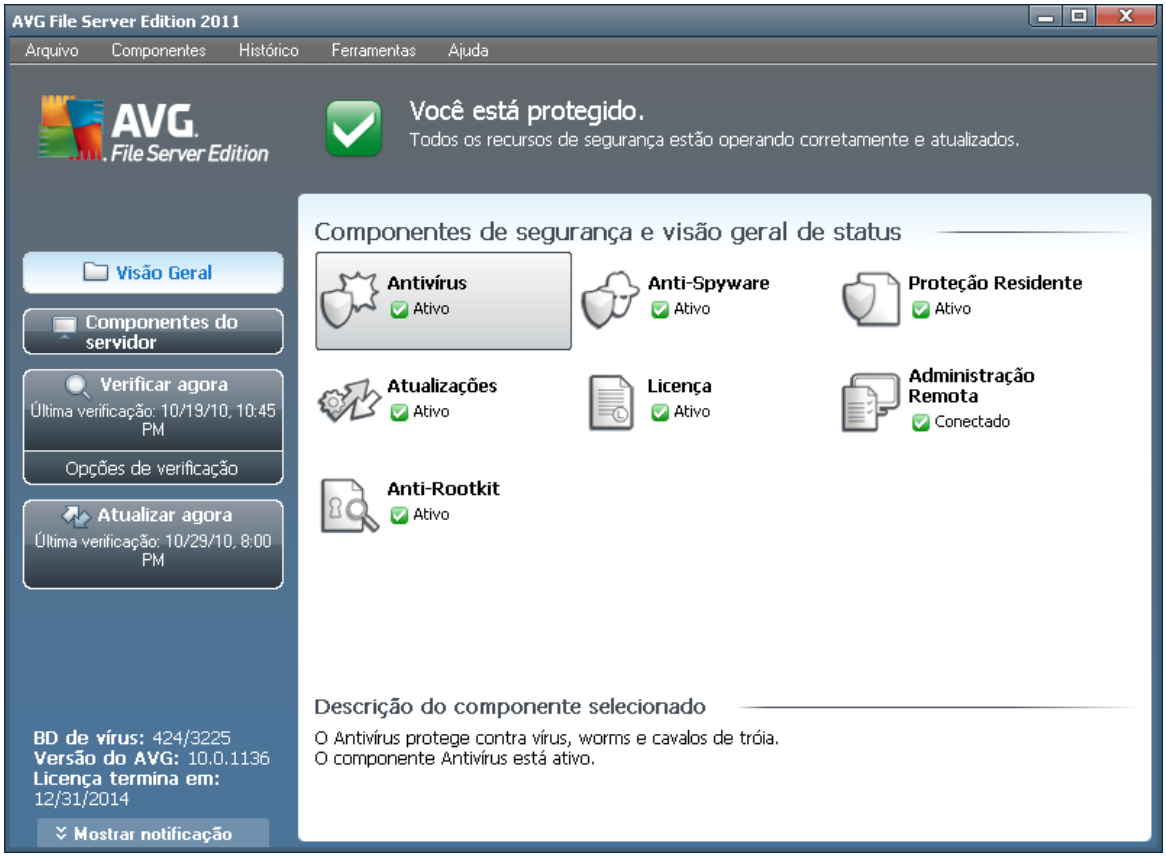
A configuração padrão (*isto é, como o aplicativo é configurado logo após a instalação*) de **AVG Email Server Edition 2011**é definida pelo fornecedor do software, de forma que todos os componentes e funções sejam ajustados para obter um desempenho ideal.

A menos que você tenha um motivo real para isso, não mude as configurações do AVG! Alterações nas configurações devem ser realizadas somente por um usuário experiente.

É possível acessar algumas edições menos importantes das configurações dos ***componentes do AVG*** diretamente na interface do usuário do componente específico. Se você tiver necessidade de alterar a configuração do AVG de acordo com suas necessidades, vá para ***Configurações Avançadas do AVG***: selecione o item de menu do sistema ***Ferramentas/Configurações avançadas*** e edite a configuração do AVG na nova caixa de diálogo aberta, a ***Configurações avançadas do AVG***.

6. Interface de usuário do AVG

O **AVG Email Server Edition 2011** é aberto com a janela principal:



A janela principal é dividida em várias seções:

- ***Menu do Sistema*** *(linha do sistema superior da janela)* é a navegação padrão que permite acessar todos os componentes, serviços e recursos do AVG - detalhes >>
- ***Informações do Status de Segurança*** *(seção inferior da janela)* fornece informações sobre o status atual do programa AVG - detalhes >>
- ***Links Rápidos*** *(seção esquerda da janela)* permite acessar rapidamente as tarefas mais importantes e mais utilizadas do AVG - detalhes >>
- ***Visão Geral dos Componentes*** *(seção central da janela)* oferece uma visão geral de todos os componentes AVG instalados - detalhes >>
- ***Estatísticas*** *(seção inferior esquerda da janela)* fornece todos os dados estatísticos referentes à operação dos programas - detalhes >>
- ***Ícone da Bandeja do Sistema*** *(canto inferior direito do monitor, na bandeja do sistema)* indica o status atual do AVG - detalhes >>

6.1. Menu do sistema

O ***Menu do sistema*** é a navegação padrão usada em todos os aplicativos Windows. Está localizado horizontalmente, na parte superior da janela principal do AVG Email Server Edition 2011**.** Use o menu do sistema para acessar os componentes específicos do AVG, recursos e serviços.

O menu do sistema é dividido em cinco seções principais:

6.1.1. Arquivo

- ***Sair*** - fecha a interface do usuário do **AVG Email Server Edition 2011**. Entretanto, o aplicativo AVG continuará sendo executado em segundo plano e seu computador continuará protegido.

6.1.2. Componentes

O item ***Componentes*** do menu do sistema inclui links para todos os componentes do AVG instalados, abrindo sua caixa de diálogo padrão na interface do usuário:

- ***Visão geral do sistema*** - muda para a caixa de diálogo da interface padrão do usuário com a visão geral de todos os componentes instalados e seu status
- ***Componentes do servidor*** - exibe os componentes de segurança e a visão geral de seu status - detalhes >>
- ***O Antivírus*** garante que o computador seja protegido de vírus que tentam entrar nele -detalhes >>
- ***Anti-Spyware*** garante que o seu computador esteja protegido contra spyware e adware - detalhes >>
- ***A Proteção Residente*** é executada em segundo plano e verifica os arquivos à medida que eles são copiados, abertos ou salvosdetalhes>>
- ***O Gerenciador de Atualizações*** controla todas as atualizações do AVG - detalhes>>
- ***Licença*** exibe o número da licença, tipo e data de validade - detalhes >>
- ***A Administração Remota*** é exibida apenas caso você tenha especificado durante o processo de instalação que esse componente deveria ser instalado.
- ***O Anti-Rootkit*** detecta programas e tecnologias que tentam camuflar malware - detalhes>>

6.1.3. Histórico

- ***Resultados da verificação*** - alterna para a interface de teste do AVG, especificamente para a caixa de diálogo ***Visão Geral dos Resultados da Verificação***

- ***Detecção da Proteção Residente*** - abre uma caixa de diálogo com uma visão geral das ameaças detectadas pela ***Proteção Residente***

- ***Quarentena de Vírus*** - abre a interface do espaço de quarentena (***Quarentena de Vírus***) no qual o AVG remove todas as infecções detectadas que, por algum motivo, não podem ser resolvidas automaticamente. No espaço de quarentena, os arquivos infectados são isolados e a segurança do computador é preservada, e, ao mesmo tempo, os arquivos infectados são armazenados para possível reparo futuro.

- ***Log de Histórico de Eventos*** - abre a interface do log de eventos com uma visão geral de todas as ações registradas do **AVG Email Server Edition 2011** .

6.1.4. Ferramentas

- ***Verificar computador*** - alterna para a interface de verificação do AVG e inicia a verificação em todo o computador

- ***Verificar pasta selecionada*** - alterna para a interface de verificação do AVG e permite definir, na estrutura de árvore do computador, quais arquivos e pastas devem ser verificados

- ***Verificar arquivo*** - permite executar um teste sob demanda em um único arquivo selecionado na estrutura de árvore do disco

- ***Atualizar*** - inicia automaticamente o processo de atualização **AVG Email Server Edition 2011**

- ***Atualizar a partir do diretório*** - executa o processo de atualização a partir dos arquivos de atualização localizados em uma pasta específica do disco local. Entretanto, esta opção é recomendada somente como emergência, ou seja, em situações em que não há conexão com a Internet (*por exemplo, seu computador está infectado e desconectado da Internet; seu computador está conectado a uma rede sem acesso à Internet, etc.*). Na nova janela aberta, selecione a pasta na qual colocou o arquivo de atualização anteriormente e inicialize o processo de atualização.

- ***Configurações avançadas*** - abre a caixa de diálogo ***Configurações avançadas do AVG***, na qual é possível editar a configuração **AVG Email Server Edition 2011**. Em geral, é recomendável manter as configurações padrão do aplicativo conforme definido pelo fornecedor do software.

6.1.5. Ajuda

- ***Conteúdo*** - abre os arquivos de ajuda do AVG

- ***Obter ajuda on-line*** - abre o site da AVG (http://www.avg.com) na página de suporte técnico ao cliente

- ***Sua Web AVG*** - abre o site da AVG (http://www.avg.com)

- ***Sobre vírus e ameaças*** - abre a ***Enciclopédia de vírus*** on-line, na qual é

possível procurar informações sobre o vírus identificado

- ***Fazer download do AVG Rescue CD*** - abre o navegador da Web apontando para a página de download do AVG Rescue CD.

- ***Reativar*** - abre a caixa de diálogo ***Ativar AVG*** com os dados inseridos na caixa de diálogo ***Personalizar AVG*** do processo de instalação. Nessa caixa de diálogo é possível inserir o número da licença para substituir o número de vendas (*o número com o qual você instalou o AVG*) ou para substituir o número antigo da licença (*por exemplo, durante a atualização de um novo produto AVG*).

- ***Registre-se agora*** - estabelece uma conexão com a página de registro do site da AVG (http://www.avg.com). Informe os dados de registro; somente os clientes que registrarem seus produtos AVG poderão receber suporte técnico gratuito.

Observação*: Se estiver utilizando a versão de teste do* **AVG Email Server Edition 2011***, os dois últimos itens aparecem como* ***Comprar agora*** *e* ***Ativar****, permitindo que você compre a versão completa do programa imediatamente. Para* **AVG Email Server Edition 2011** *instalado com um número de vendas, o itens são exibidos como****Registrar*** *e* ***Ativar****. Para obter mais informações, visite a seção Licença deste documento.*

- ***Sobre o AVG*** - abre a caixa de diálogo ***Informações*** com cinco guias que fornecem dados sobre o nome do programa, versão do programa e do banco de dados de vírus, informações do sistema, contrato de licença e informações de contato da ***AVG Technologies CZ***.

6.2. Informações sobre status de segurança

A seção ***Informações sobre status de segurança*** está localizada na parte superior da janela principal do AVG. Nessa seção, você encontrará informações sobre o status de segurança atual do **AVG Email Server Edition 2011.** Observe uma visão geral dos ícones possivelmente ocultos dessa seção e seus significados:

 - O ícone verde indica que o AVG está totalmente funcional. Seu computador está totalmente protegido, atualizado e todos os componentes instalados estão funcionando corretamente.

 O ícone laranja avisa que um ou mais componentes estão configurados incorretamente e você deverá prestar atenção às propriedades e configurações respectivas. Não há problema crítico no AVG e você provavelmente decidiu desativar alguns componentes por algum motivo. Você ainda está protegido pelo AVG. Entretanto, preste atenção às configurações do componente com problema! Seu nome será fornecido na seção ***Informações sobre*** o status de segurança.

Esse ícone também aparece se, por alguma razão, você decidiu ignorar o status de erro de um componente (a opção *"Ignorar estado do componente" está disponível no menu de contexto aberto clicando-se com o botão direito sobre o ícone do componente em questão na visão geral do componente na janela principal do AVG*). Você pode precisar usar esta opção em uma determinada situação; porém, recomendamos que a opção "***Ignorar estado do componente***" seja desligada o mais rápido possível.

 - O ícone vermelho indica que o AVG está com status crítico! Um ou mais componentes não estão funcionando adequadamente e o AVG não poderá proteger o seu computador. Preste atenção para reparar imediatamente o problema relatado. Se você não conseguir reparar o erro por conta própria, entre em contato com o Suporte técnico da AVG .

No caso de o AVG não ser ajustado para o desempenho ideal, um novo botão denominado Corrigir (ou Corrigir tudo, se o problema envolver mais de um componente) aparecerá perto das informações do status de segurança. Pressione o botão para iniciar um processo automático de Clique com o botão direito no ícone AVG da verificação em execução para abrir um menu de contexto, onde você pode escolher pausar ou até interromper a verificação e configuração do programa. Essa é uma forma fácil de ajustar o AVG para o desempenho ideal e alcançar o nível de segurança máximo!

É altamente recomendável prestar atenção nas Informações sobre status de segurança e, caso o relatório indique algum problema, tentar resolvê-lo imediatamente. Caso contrário, seu computador estará sob risco!

Observação: *as informações sobre o status do AVG também podem ser obtidas a qualquer momento no ícone da bandeja do sistema.*

6.3. Links rápidos

Os links rápidos *(na seção esquerda da Interface do usuário do AVG)* permitem acessar imediatamente os recursos mais importantes e usados com mais frequência no AVG:

- ***Visão geral*** - use este link para passar de qualquer interface do AVG aberta no momento para a interface padrão, com uma visão geral de todos os componentes. Consulte o capítulo ***Visão geral dos componentes >>***

- ***Verificar agora*** - por padrão, o botão fornece informações (*tipo de verificação, data da última verificação*) sobre a última verificação feita. Você pode executar o comando ***Verificar agora*** para iniciar a mesma verificação novamente ou seguir o link ***Verificador do computador*** para abrir a interface de verificação do AVG, onde é possível realizar verificações, programar verificações ou editar seus parâmetros - consulte o capítulo ***Verificação do AVG >>***

- ***Atualizar agora*** - o link fornece a data da última execução do processo de atualização. Pressione o botão para abrir a interface de atualização e executar o processo de atualização do AVG - consulte o capítulo ***Atualizações do AVG >>***

- ***Componentes do servidor*** - esse link o leva até a ***Visão geral dos componentes do servidor***.

Esses links podem ser acessados da interface do usuário a qualquer momento. Quando você usar um link rápido para executar um processo específico, a GUI será alterada para uma nova caixa de diálogo, mas os links rápidos permanecerão disponíveis. Além disso, o processo de execução será representado graficamente.

6.4. Visão geral dos componentes

A seção ***Visão geral dos componentes*** está localizada na parte central da Interface do usuário do AVG. A seção é dividida em duas partes:

- Visão Geral de todos os componentes instalados, consistindo em um painel com o ícone do componente e as informações indicando se o respectivo componente está ativo ou inativo.

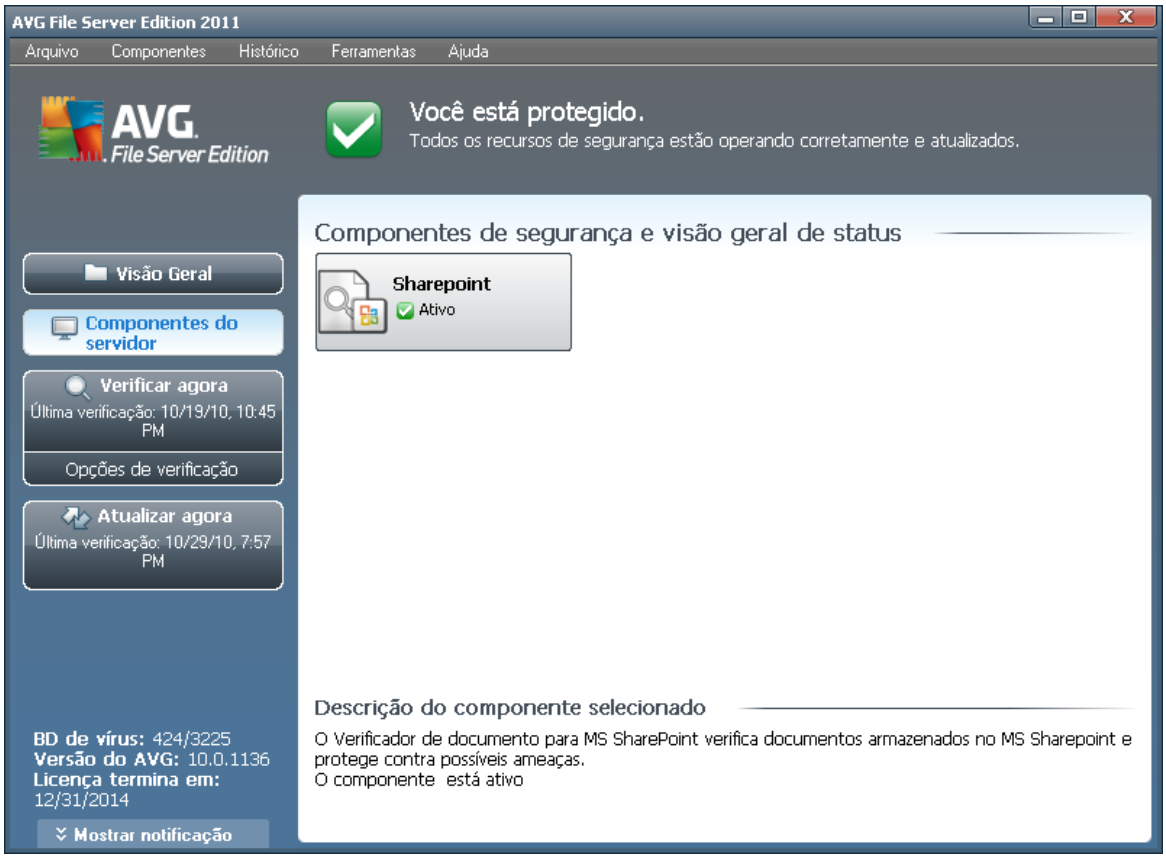
- Descrição de um componente selecionado

No**AVG Email Server Edition 2011**a seção***Visão geral dos componentes*** contém informações sobre os seguintes componentes:

- ***O Antivírus*** garante que o computador seja protegido de vírus que tentam entrar nele -detalhes >>

- ***Anti-Spyware*** garante que o seu computador esteja protegido contra spyware e adware - detalhes >>

6.5. Componentes do servidor



A seção ***Componentes do servidor*** está localizada na parte central da Interface do usuário do AVG. A seção é dividida em duas partes:

- Visão Geral de todos os componentes instalados, consistindo em um painel com o ícone do componente e as informações indicando se o respectivo componente está ativo ou inativo.
- Descrição de um componente selecionado

No **AVG Email Server Edition 2011** a seção ***Componentes do servidor*** inclui informações sobre os seguintes componentes:

- ***O SharePoint*** verifica documentos armazenados no MS SharePoint e protege contra possíveis ameaças - detalhes >>

Clique no ícone de qualquer um dos componentes para realçá-lo na visão geral dos componentes. Ao mesmo tempo, a descrição da funcionalidade básica do componente será exibida na parte inferior da interface do usuário. Clique duas vezes no ícone para abrir a interface dos componentes com uma lista de dados estatísticos básicos.

Clique com o botão direito no ícone de um componente para expandir um menu de

contexto: além de abrir a interface gráfica do componente, você ainda pode selecionar ***Ignorar estado do componente***. Selecione esta opção para informar que você está ciente do estado de erro do componente mas que, por alguma razão, deseja continuar com o AVG e não quer avisado da alteração pelo ícone da bandeja do sistema.

6.6. Estatísticas

A seção ***Estatísticas***se localiza na parte inferior esquerda da ***Interface do usuário do AVG***. Ela oferece uma lista de informações relativas à operação do programa:

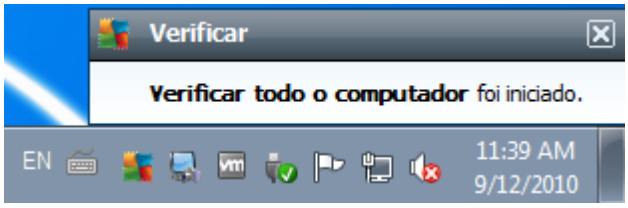
- ***Banco de Dados de Vírus*** - informa sobre a versão do banco de dados de vírus instalada no momento
- ***Versão do AVG*** - informa sobre a versão do AVG instalada *(o número está na forma de 10.0.xxxx, onde 10.0 é a versão da linha do produto, e xxxx indica o número da compilação)*
- ***Vencimento da licença*** - fornece a data de vencimento da licença do AVG

6.7. Ícone da bandeja do sistema

O Ícone da bandeja do sistema (*na barra de tarefas do Windows*) indica o status atual doAVG Email Server Edition 2011. Ele fica visível sempre na bandeja do sistema, independentemente de a janela principal do AVG estar aberta ou fechada:

Se colorido, o ***Ícone da bandeja do sistema*** indica que todos os componentes do AVG estão ativos e completamente funcionais. Da mesma forma, o ícone AVG na bandeja do sistema pode ser exibido em sua cor normal caso o AVG esteja em estado de erro mas que você esteja completamente ciente desta situação e tenha deliberadamente decidido ***Ignorar o estado do componente***. Um ícone com um sinal de exclamação indica um problema (*componente inativo, status de erro, etc.*). Clique duas vezes no ***Ícone da bandeja do sistema*** para abrir a tela principal e editar um componente.

O ícone da bandeja do sistema também informa sobre atividades atuais do AVG e possíveis mudanças de status no programa (*por ex., início automático de uma verificação ou atualização agendada, alteração do status do componente, ocorrência de status de erro, ...*) por uma janela pop-up aberta pelo ícone AVG na bandeja do sistema:



O ***Ícone da bandeja do sistema*** também pode ser usado como um link rápido para acessar uma janela principal do AVG a qualquer momento (basta clicar duas vezes no ícone). Ao clicar com o botão direito do mouse no ***Ícone da bandeja do sistema*** , você abre um menu de contexto breve com as opções a seguir:

- ***Abrir Interface do Usuário do AVG*** - clique para abrir a Interface do Usuário do AVG
- ***Verificações*** - clique para abrir o menu de contexto das verificações predefinidas (*Verificar todo o computador*, *Verificar arquivos ou pastas específicos*, *Verificação Anti-Rootkit*) e selecione a verificação necessária. Ela será iniciada imediatamente
- ***Executando verificações*** - este item será exibido apenas se uma verificação estiver atualmente em execução no computador. Para essa verificação, você pode definir sua prioridade ou, como segunda opção, interromper ou pausar a verificação em execução. Além disso, as seguintes ações estão acessíveis: *Definir prioridade para todas as verificações, Pausar todas as verificações* ou *Interromper todas as verificações*.
- ***Atualizar agora*** - inicia uma atualização imediata
- ***Ajuda*** - abre o arquivo de ajuda da página de inicialização

7. Componentes do AVG

7.1. Antivírus

7.1.1. Princípios do Antivírus

O mecanismo de verificação do software antivírus verifica se há vírus conhecidos em todos os arquivos e atividades de arquivo (abertura/fechamento de arquivos, etc.) . Todo e qualquer vírus detectado será bloqueado e não poderá executar nenhuma ação. Ele também será limpado e colocado em quarentena. A maioria dos softwares antivírus usa a verificação heurística, em que os arquivos são verificados no que diz respeito às características normais de vírus, as chamadas assinaturas virais. Isso significa que o verificador antivírus pode detectar um vírus novo e desconhecido se este contiver algumas características típicas dos vírus existentes.

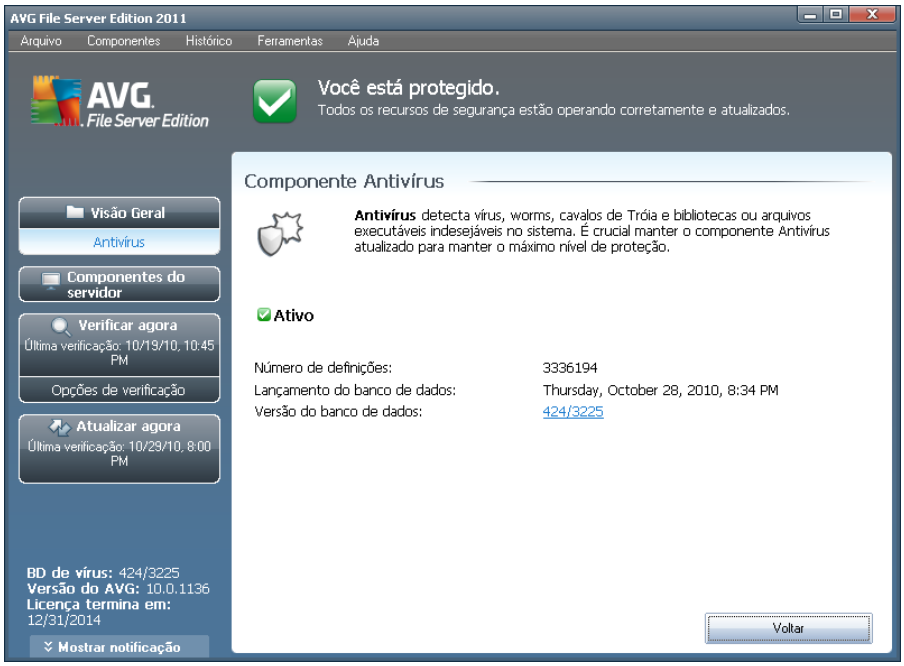
O recurso importante da proteção antivírus é que nenhum vírus conhecido pode ser executado no computador!

Nas situações em que uma única tecnologia poderia falhar na detecção ou identificação de um vírus, o ***Antivírus*** combina várias tecnologias para assegurar que o computador fique protegido:

- Verificação - procura seqüências de caracteres típicas de um determinado vírus.
- Análise heurística - emulação dinâmica das instruções do objeto verificado em um ambiente de computador virtual
- Detecção genérica - detecção de instruções características de um determinado vírus ou grupo de vírus

O AVG também é capaz de analisar e detectar aplicativos executáveis ou bibliotecas DLL potencialmente indesejáveis no sistema. Chamamos essas ameaças de Programas Potencialmente Indesejáveis (vários tipos de spyware, adware, etc). Além disso, o AVG verifica o registro do sistema em busca de entradas suspeitas, arquivos temporários da Internet e cookies de rastreamento, além de permitir o tratamento de todos os itens potencialmente prejudiciais como qualquer outra infecção.

7.1.2. Interface do Antivírus



A interface do componente do ***Antivírus*** apresenta informações básicas sobre a funcionalidade do componente, informações sobre o status atual do componente (*O Antivírus está ativo.*) e uma breve visão geral das ***estatísticas do*** Antivírus:

- ***Número de definições de spyware*** - o número fornece a contagem de vírus definidos na versão atualizada do banco de dados de vírus.
- ***Lançamento de banco de dados*** - especifica quando e a que horas o banco de dados de vírus foi atualizado pela última vez
- ***Versão do banco de dados*** - define o número da versão do banco de dados de vírus atualmente instalada. Esse número aumenta a cada atualização da base de vírus

Existe apenas um botão de operação disponível na interface deste componente (***Voltar***) - pressione o botão para retornar à interface do usuário do AVGpadrão (*visão geral dos componentes*).

7.2. Anti-Spyware

7.2.1. Princípios do Anti-Spyware

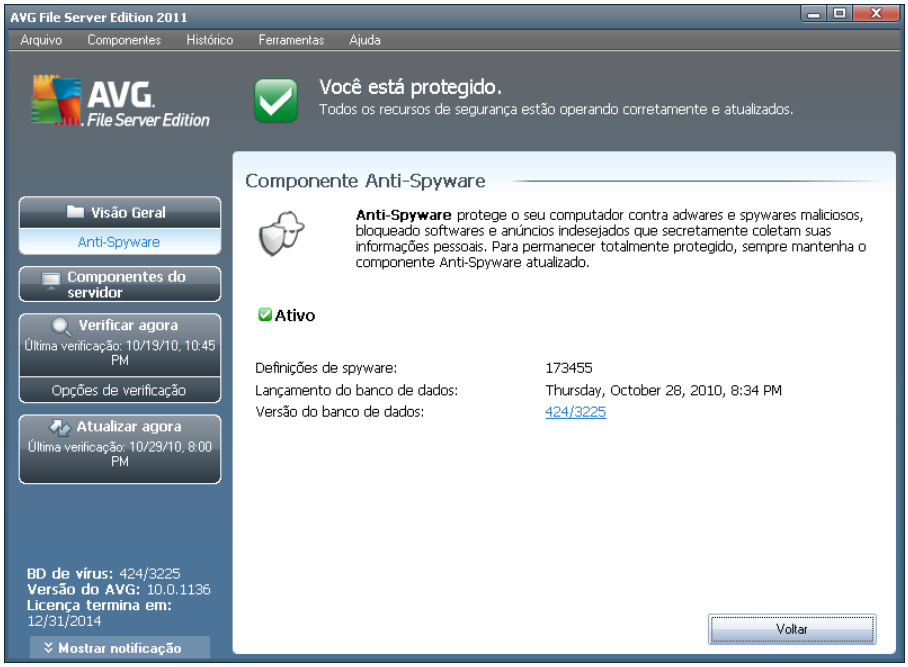
Normalmente, o spyware é definido como um tipo de malware, ou seja, software que coleta informações a partir do computador do usuário sem o conhecimento ou consentimento dele. Alguns aplicativos de spyware também podem ser instalados propositalmente e, em geral, contêm anúncios, janelas pop-up ou tipos diferentes de

softwares inoportunos.

Atualmente, a fonte mais comum de infecção são sites com conteúdo potencialmente perigoso. Outros métodos de transmissão, como e-mail ou worms e vírus, são também predominantes. A proteção mais importante é o uso de um verificador de segundo plano sempre ativo, o ***Anti-Spyware***, que funciona como uma proteção residente e verifica seus aplicativos em segundo plano, à medida que são executados.

Também é possível que algum malware tenha sido transmitido ao seu computador antes da instalação do AVG ou que você tenha esquecido de baixar as últimasAVG Email Server Edition 2011 atualizações de banco de dados e programas . Por essa razão, o AVG permite verificar totalmente o computador em busca de malware ou spyware, usando o recurso de verificação. Ele também detecta malwares inativos e não perigosos, ou seja, baixados mas ainda não ativados.

7.2.2. Interface do Anti-Spyware



A interface do componente ***Anti-Spyware*** fornece uma breve visão geral da funcionalidade do componente, informações sobre o status atual do componente e algumas estatísticas de ***Anti-Spyware***:

- ***Definições de spyware*** - o número fornece a contagem de amostras de spyware definidas na versão do banco de dados de spyware mais recente.
- ***Lançamento de banco de dados*** - especifica quando e a que horas o banco de dados do spyware foi atualizado
- ***Versão do banco de dados*** - define o número da versão mais recente do spyware. Esse número aumenta a cada atualização da base de vírus.

Existe apenas um botão de operação disponível na interface deste componente (***Voltar***) - pressione o botão para retornar à interface do usuário do AVGpadrão (*visão geral dos componentes*).

7.3. Proteção Residente

7.3.1. Princípios da Proteção Residente

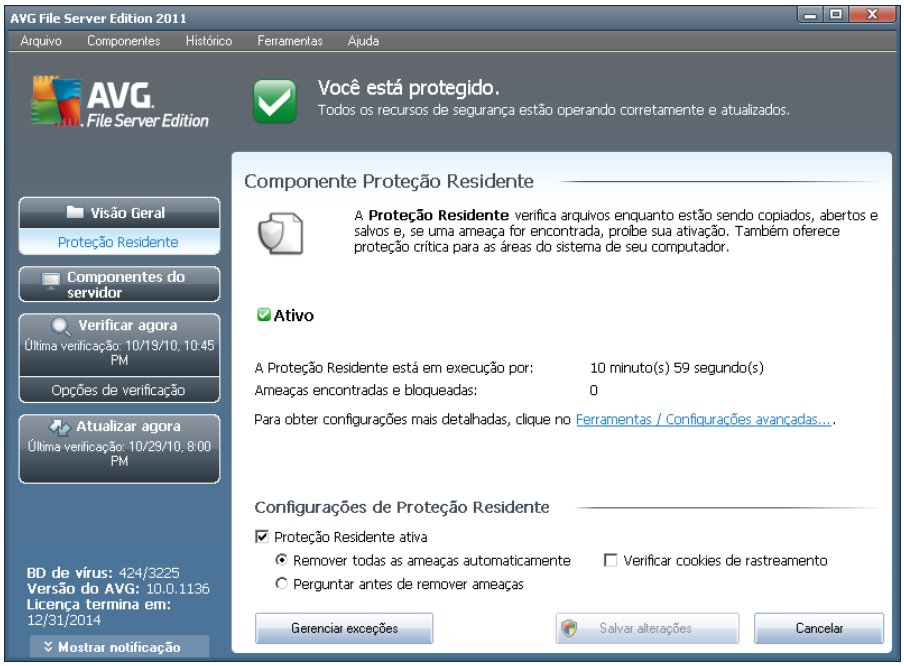
O componente ***Proteção Residente*** oferece proteção contínua a seu computador. Ele verifica todos os arquivos que estão sendo abertos, salvos ou copiados e protege as áreas de sistema do computador. Quando a ***Proteção Residente*** descobre um vírus em um arquivo acessado, ela pára as operações em execução no momento e não permite que o vírus seja ativado. Normalmente, você sequer nota o processo, pois ele acontece "em segundo plano", e você só é notificado quando são encontradas ameaças; ao mesmo tempo, a ***Proteção Residente*** evita que as ameaças sejam ativadas e as remove. A ***Proteção Residente*** está sendo carregada na memória do computador durante a inicialização.

O que a Proteção Residente pode fazer:

- Verificar tipos específicos de possíveis ameaças
- Verificar mídia removível (*disco flash etc.*)
- Verificar arquivos com extensões específicas ou sem nenhuma extensão
- Permitir exceções de verificação – especificar arquivos ou pastas que nunca devem ser verificados

Aviso: a Proteção Residente é carregada na memória do computador durante a inicialização e é vital que você a mantenha ativada todo o tempo!

7.3.2. Interface da Proteção Residente



Além de uma visão geral da funcionalidade ***Proteção Residente*** e das informações sobre o status do componente, a interface da ***Proteção Residente*** oferecerá também alguns dados estatísticos:

- ***A Proteção Residente esteve ativa em*** - fornece a hora desde a última inicialização do componente
- ***Ameaças detectadas e bloqueadas*** - número de infecções detectadas e impedidas de serem executadas/abertas ((*se necessário, este valor pode ser redefinido, por exemplo, para fins estatísticos - Redefinir valor*)

Configurações da Proteção Residente

Na parte inferior da caixa de diálogo, você encontrará a seção chamada ***Configurações da Proteção Residente***, na qual é possível editar algumas configurações básicas da funcionalidade do componente (*a configuração detalhada, como nos demais componentes, está disponível por meio do item Ferramentas/ Configurações avançadas do menu do sistema*).

A opção ***Proteção Residente está ativa*** permite ativar/desativar facilmente a proteção residente. Por padrão, a função está ativa. Com a proteção residente ativa, é possível decidir como as infecções possivelmente detectadas devem ser tratadas (removidas):

- automaticamente (***Remover todas as ameaças automaticamente***)
- ou somente após a aprovação do usuário (***Perguntar antes de remover***

ameaças)

Esta opção não afeta o nível de segurança e se reflete apenas em suas preferências.

Nos dois casos, você ainda pode selecionar se deseja ***Verificar cookies de rastreamento***. Em casos específicos, você pode ativar esta opção para obter níveis de segurança máximos, mas ela fica desativada por padrão. (*cookies = parcelas de texto enviadas por um servidor a um navegador da Web e em seguida enviadas de volta inalteradas pelo navegador sempre que ele acessa esse servidor. Cookies HTTP são usados para autenticar, controlar e manter informações específicas sobre usuários, como preferências de site ou o conteúdo de suas compras eletrônicas*).

Observação: o *fornecedor do software configurou todos os componentes do AVG para propiciar um desempenho ideal. A menos que você tenha um motivo real para isso, não mude as configurações do AVG. Alterações nas configurações devem ser realizadas somente por um usuário experiente. Se você precisar alterar a configuração do AVG, selecione o item de menu do sistema****Ferramentas/ Configurações avançadas*** *e edite a configuração do AVG na caixa de diálogo Configurações avançadas do AVG recém-aberta.*

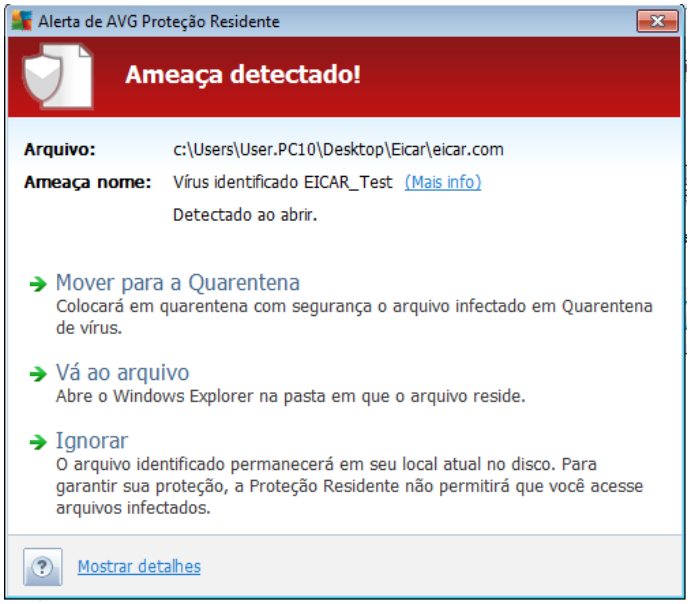
Botões de controle

Estes são os botões de controle disponíveis na interface da ***Proteção Residente***:

- ***Gerenciar exceções*** - abre a caixa de diálogo ***Proteção Residente - Itens Excluídos*** , em que é possível definir as pastas que devem ser excluídas da verificação do ***Proteção Residente***
- ***Salvar alterações*** - pressione este botão para salvar e aplicar quaisquer alterações feitas na caixa de diálogo
- ***Cancelar*** - pressione este botão para retornar à ***interface do usuário do AVG*** padrão (*visão geral dos componentes*)

7.3.3. Detecção da Proteção Residente

A Proteção Residente verifica os arquivos à medida que são copiados, abertos ou salvos. Quando um vírus ou qualquer tipo de ameaça é detectado, você é alertado imediatamente por meio da seguinte caixa de diálogo:



Nessa caixa de diálogo de aviso, você encontrará dados sobre o arquivo detectado e considerado infectado (*Nome do arquivo*), o nome da infecção reconhecida (*Nome da ameaça*) e um link para a ***Enciclopédia de vírus***, na qual você pode encontrar informações detalhadas sobre a infecção detectada, se conhecida (*Mais informações*).

Além disso, você precisa decidir qual ação deve ser executada agora - as seguintes opções estão disponíveis:

Observe que, em condições específicas (o tipo de arquivo infectado e sua localização), nem todas as opções estarão sempre disponíveis!

- ***Remover ameaça como Usuário avançado*** – marque a caixa se supor que pode não ter direitos suficientes para remover a ameaça como um usuário comum. Usuários avançados possuem direitos de acesso amplos e se a ameaça estiver localizada em uma certa pasta do sistema, você pode precisar usar essa caixa de seleção para removê-la com sucesso.

- ***Reparar*** - este botão será exibido apenas se a infecção detectada puder ser reparada. Em seguida, ela é removida do arquivo e restaura o estado original do arquivo. Se o próprio arquivo for um vírus, use esta função para excluí-lo (*por exemplo, removido para a* ***Quarentena***)

- ***Mover para Quarentena*** - o vírus será movido para a ***Quarentena de vírus do AVG***

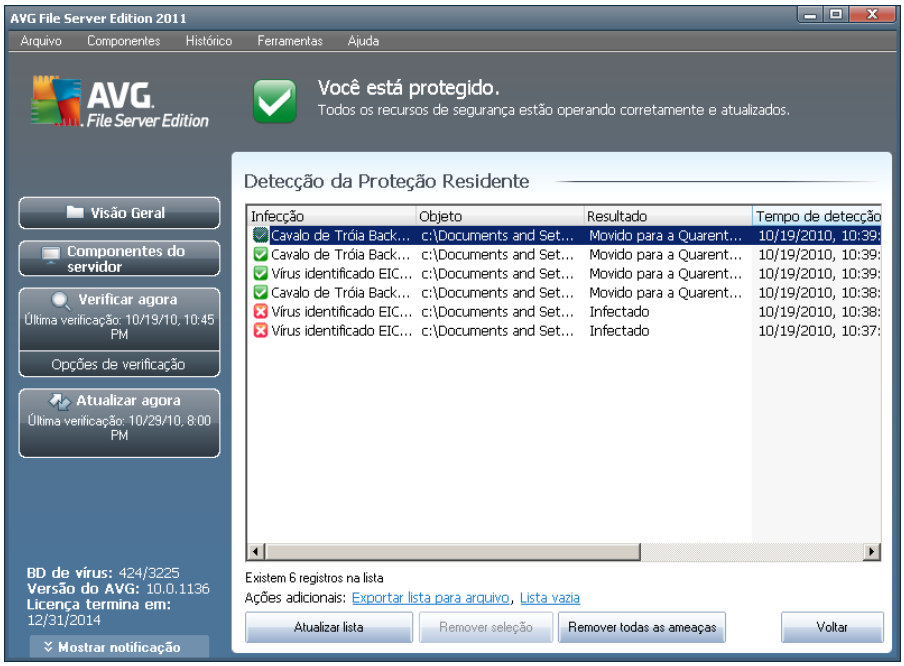
- ***Ir para o arquivo*** - essa opção redireciona o usuário ao local exato do objeto suspeito (*abre a nova janela do Windows Explorer*)

- ***Ignorar*** - NÃO recomendamos o uso desta opção, a não ser que exista um bom motivo!

Na seção inferior da caixa de diálogo, você encontrará o link ***Mostrar detalhes*** -

clique nele para abrir uma janela popup com informações detalhadas sobre o processo em execução enquanto a infecção foi detectada e a identificação do processo.

A visão geral completa de todas as ameaças detectadas pela ***Proteção Residente*** está disponível na caixa de diálogo ***Detecção da Proteção Residente***, acessível por meio da opção de menu do sistema ***Histórico/detecção da Proteção Residente***:



A ***detecção da Proteção Residente*** oferece uma visão geral dos objetos detectados pela ***Proteção Residente***, avaliados como perigosos e recuperados ou movidos para a ***Quarentena de vírus***. Em cada objeto detectado, são fornecidas as seguintes informações:

- ***Infecção*** - descrição (possivelmente até o nome) do objeto detectado
- ***Objeto*** - localização do objeto
- ***Resultado*** - ação executada pelo objeto detectado
- ***Hora da detecção*** - data e hora em que o objeto foi detectado
- ***Tipo de Objeto*** - tipo de objeto detectado
- ***Processo*** - qual ação foi executada para ativar o objeto potencialmente perigoso de modo a permitir que fosse detectado

Na parte inferior da caixa de diálogo, na lista, você encontrará informações sobre o total de objetos detectados listados em cima. Além disso você pode exportar a lista inteira de objetos detectados em um arquivo (***Exportar lista para arquivo***) e excluir todas as entradas de objetos detectados (***Lista vazia***). O botão ***Atualizar lista*** atualizará a lista de detecções feitas pela ***Proteção Residente***. O botão ***Voltar*** leva

você de volta à interface do usuário do AVG padrão _ *(visão geral dos componentes*).

7.4. Gerenciador de atualizações

7.4.1. Princípios do Gerenciador de Atualizações

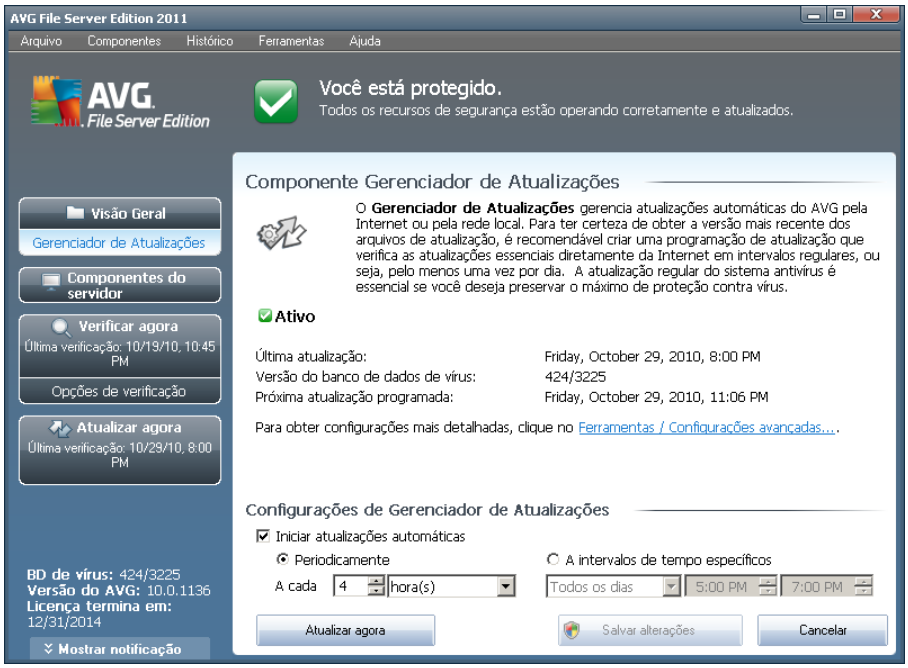
Nenhum software de segurança pode garantir proteção real de vários tipos de ameaças se não for regularmente atualizado! Os criadores de vírus estão sempre em busca de novas brechas que possam explorar em softwares e sistemas operacionais. Novos vírus, novos malwares, novos ataques de hackers surgem diariamente. Por esse motivo, os fornecedores de software estão continuamente emitindo atualizações e patches de segurança para corrigir qualquer brecha de segurança que seja descoberta.

É fundamental atualizar o AVG regularmente!

O ***Gerenciador de atualizações*** ajuda a controlar a atualização regularmente. Nesse componente você pode programar downloads automáticos de arquivos de atualização da Internet ou da rede local. As atualizações das definições de vírus essenciais devem ser feitas diariamente, se possível. Atualizações de programas menos urgentes podem ser feitas semanalmente.

Observação: *consulte o capítulo Atualizações do AVG para obter mais informações sobre os tipos e níveis de atualização!*

7.4.2. Interface do Gerenciador de atualizações



A interface do ***Gerenciador de Atualizações***exibe informações sobre a funcionalidade do componente e seu status atual e fornece os dados estatísticos relevantes:

- ***Atualização mais recente*** - especifica quando e a que horas o banco de dados foi atualizado
- ***Versão do banco de dados de vírus*** - define o número da versão do banco de dados de vírus atualmente instalada. Esse número aumenta a cada atualização da base de vírus
- ***Próxima atualização programada*** - especifica quando e em que horário o banco de dados está programado para uma nova atualização

Configurações de Gerenciador de Atualizações

Na parte inferior da caixa de diálogo, você encontrará a seção ***Configurações do Gerenciador de Atualizações*** , onde é possível realizar algumas alterações nas regras de inicialização do processo de atualização. Você pode definir se deseja que os arquivos de atualização sejam baixados automaticamente (***Iniciar atualizações automáticas***) ou apenas sob demanda. Por padrão, a opção ***Iniciar atualizações automáticas*** é ativada e recomendamos mantê-la dessa forma. O download regular dos arquivos de atualização mais recentes é crucial para a funcionalidade adequada de um software de segurança.

Além disso, você pode definir quando a atualização será iniciada:

- ***Periodicamente*** - define o intervalo de tempo
- ***Em um intervalo de tempo específico*** - defina a hora do dia exata que a atualização deve ser feita

Por padrão, a atualização é definida para a cada 4 horas. É altamente recomendável manter essa configuração, a menos que você tenha um motivo real para alterá-la.

Nota: o *fornecedor do software configurou todos os componentes do AVG para propiciar um desempenho ideal. A menos que você tenha um motivo real para isso, não mude as configurações do AVG. Alterações nas configurações devem ser realizadas somente por um usuário experiente. Se você precisar alterar a configuração do AVG, selecione o item de menu do sistema****Ferramentas/ Configurações avançadas*** *e edite a configuração do AVG na caixa de diálogo Configurações avançadas do AVG recém-aberta.*

Botões de controle

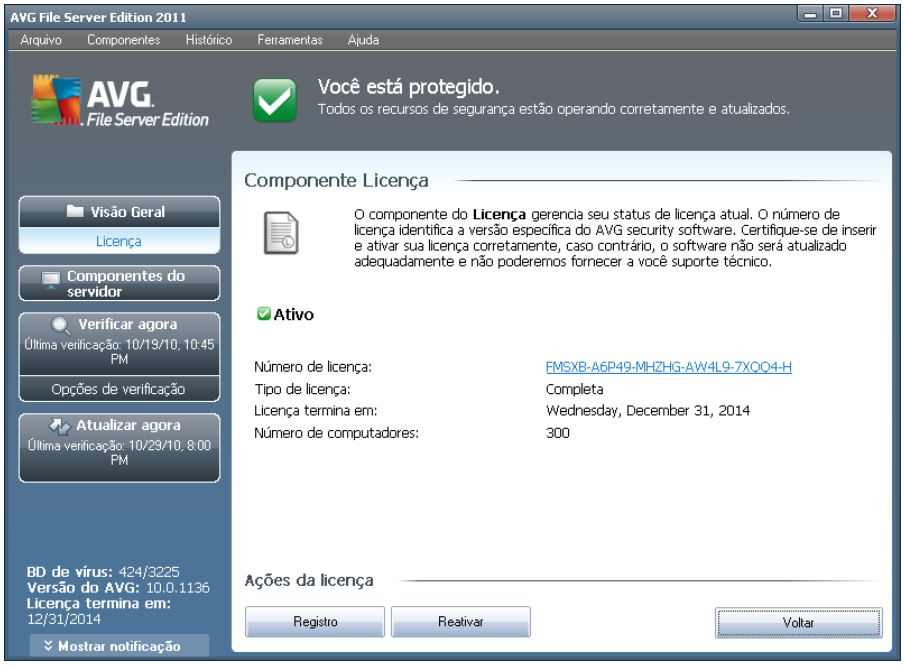
Os botões de controle disponíveis na interface do ***Gerenciador de Atualizações*** são os seguintes:

- ***Atualizar agora*** - inicializa uma atualização imediata sob demanda.

- ***Salvar alterações*** - pressione este botão para salvar e aplicar quaisquer alterações feitas na caixa de diálogo

- ***Cancelar*** - pressione este botão para retornar à ***interface do usuário do AVG*** padrão (*visão geral dos componentes*)

7.5. Licença



Na interface do componente ***Licença***, você encontrará um texto curto descrevendo a funcionalidade do componente, informações sobre seu status atual e as seguintes informações:

- ***Número da licença*** - apresenta a forma reduzida do número da licença (*por motivos de segurança, os últimos quatro símbolos estão faltando*). Ao digitar o número da licença, você deve ser totalmente preciso e inseri-lo como mostrado. Portanto, convém sempre usar o método "copiar e colar" para qualquer manipulação com o número da licença.

- ***Tipo de licença*** - especifica o tipo de produto instalado.

- ***Vencimento da licença*** - essa data determina o período de validade da licença. Se quiser continuar usando o **AVG Email Server Edition 2011** depois dessa data, terá que renovar a licença. A renovação da licença pode ser realizada online, no site da AVG.

- ***Número de computadores*** - a quantidade de estações de trabalho em que você tem permissão para instalar o **AVG Email Server Edition 2011**.

Botões de controle

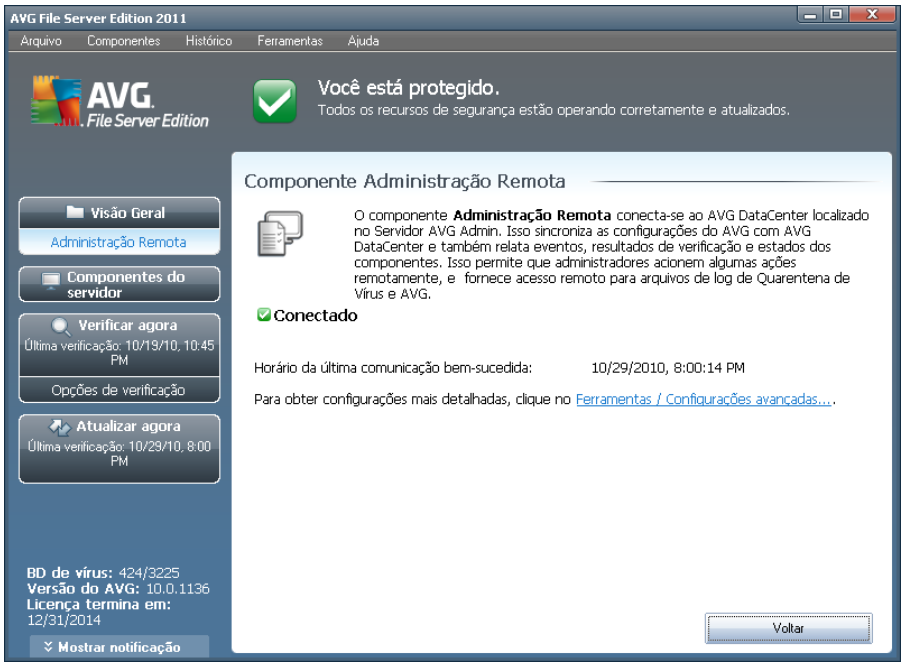
- ***Registre-se*** - estabelece uma conexão com a página de registro do site da AVG (http://www.avg.com). Informe os dados de registro; somente os clientes que registrarem seus produtos AVG poderão receber suporte técnico gratuito.

- ***Reativar*** - abre a caixa de diálogo ***Ativar AVG*** com os dados inseridos na caixa de diálogo ***Personalizar AVG*** do processo de instalação. Nessa caixa de diálogo é possível inserir o número da licença para substituir o número de vendas (*o número com o qual você instalou o AVG*) ou para substituir o número antigo da licença (*por exemplo, durante a atualização de um novo produto AVG*).

Observação: Se estiver utilizando a versão do *AVG Email Server Edition 2011*, **os botões aparecem como** *Comprar agora* **e** *Ativar, permitindo que você compre a versão completa do programa imediatamente. Para* **AVG Email Server Edition 2011** *instalado com um número de vendas, os botões são exibidos como* ***Registrar*** *e* ***Ativar****.*

- ***Voltar*** - pressione esse botão para voltar para a ***interface do usuário do AVG padrão*** (*visão geral dos componentes*).

7.6. Administração Remota



O componente ***Administração Remota*** aparece apenas na interface do usuário do **AVG Email Server Edition 2011** no caso de você ter instalado a edição de rede do produto (*veja o componente* ***Licença***). Na caixa de diálogo ***Administração Remota***, você pode encontrar informações relativas ao componente, ou seja, se ele está ativo

e conectado ao servidor. Todas as configurações do componente ***Administração Remota*** devem ser feitas em ***Configurações Avançadas/Administração Remota***.

Para uma descrição detalhada das opções e da funcionalidade do componente no sistema Administração Remota do AVG, consulte a documentação específica dedicada a esse tópico exclusivamente. Esta documentação está disponível para download no Site do AVG (www.avg.com), na seção ***Centro de suporte/Download/ Documentação***.

Botões de controle

- ***Voltar*** - pressione esse botão para voltar para a interface do usuário do AVG padrão (*visão geral dos componentes*).

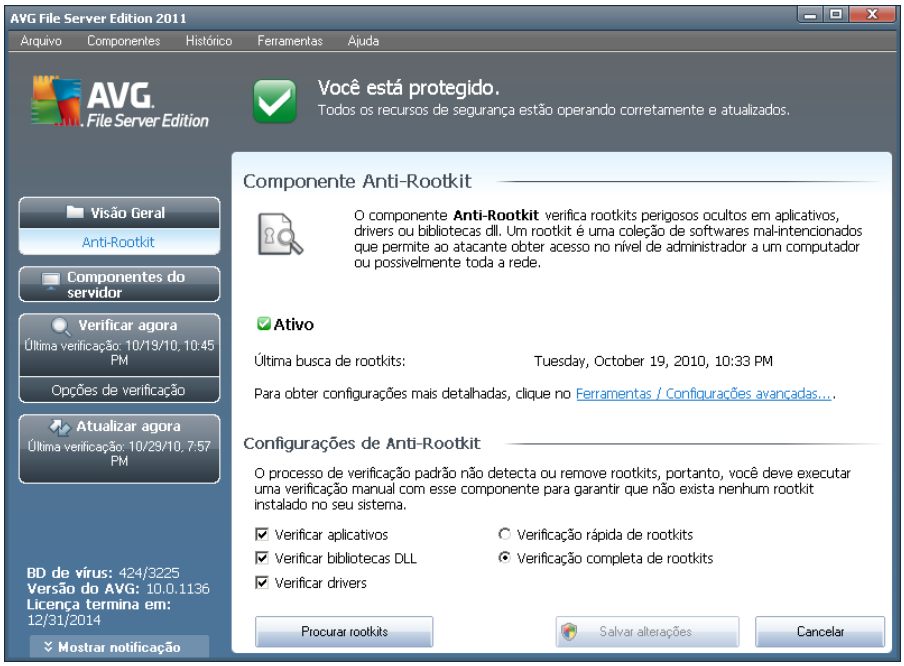
7.7. Anti-Rootkit

Um rootkit é um programa criado para assumir o controle fundamental de um sistema de computador, sem autorização dos proprietários do sistema e gerentes legítimos. O acesso ao hardware é realmente necessário, pois um rootkit tem o objetivo de executar o controle do sistema operacional executado no hardware. Geralmente, os rootkits atuam para obscurecer sua presença no sistema por meio de subversão ou evasão de mecanismos de segurança padrão do sistema operacional. Freqüentemente, eles também são cavalos-de-tróia, levando os usuários a acreditarem que é confiável executá-los no sistema. As técnicas usadas para conseguir isso podem incluir ocultar processos em execução de programas de monitoramento ou ocultar arquivos ou dados do sistema operacional.

7.7.1. Princípios do Anti-Rootkit

O AVG Anti-Rootkit é uma ferramenta especializada para detectar e remover efetivamente rootkits perigosos, isto é, programas e tecnologias que podem camuflar a presença de software malicioso no seu computador. O ***AVG Anti-Rootkit*** é capaz de detectar rootkits com base em um conjunto de regras predefinidas. Observe que são detectados todos os rootkits (*não apenas os infectados*). Se o ***AVG Anti-Rootkit*** encontrar um rootkit, isso não quer dizer necessariamente que esse rootkit está infectado. Algumas vezes os rootkits são usados como drivers ou fazem parte de aplicativos corretos.

7.7.2. Interface do Anti-Rootkit



A interface do usuário do ***Anti-Rootkit*** fornece uma breve descrição da funcionalidade do componente, informa o status atual do componente e também traz informações sobre a última vez que o teste do ***Anti-Rootkit*** foi iniciado (***Última pesquisa do rootkit***). A caixa de diálogo ***Anti-Rootkit*** apresenta também o link ***Ferramentas/ Configurações Avançadas***. Use o link para ser redirecionado ao ambiente de configuração avançada do componente ***Anti-Rootkit***.

Nota: *o fornecedor do software configurou todos os componentes do AVG para proporcionar um desempenho ideal. A menos que você tenha um motivo real para isso, não mude as configurações do AVG. Alterações nas configurações devem ser realizadas somente por um usuário experiente.*

Configurações de Anti-Rootkit

Na parte inferior da caixa de diálogo, você localizará a seção ***Configurações do Anti-Rootkit*** , onde é possível configurar funções elementares da verificação de presença do rootkit. Primeiro, marque as respectivas caixas de seleção para especificar objetos que devem ser verificados:

- ***Verificar aplicativos***
- ***Verificar bibliotecas DLL***
- ***Verificar drivers***

Em seguida, você pode selecionar o modo de verificação do rootkit:

- ***Verificação rápida do rootkit*** - verifica todos os processos em execução, unidades carregadas e pasta do sistema (*tipicamente c:\Windows*)

- ***Verificação completa do rootkit*** - verifica todos os processos em execução, unidades carregadas, a pasta do sistema (*tipicamente c:\Windows*além de todos os discos locais (*incluindo o disco flash, mas excluindo as unidades de CD/disquete*)

Botões de controle

- ***Pesquisar rootkits*** - como a verificação do rootkit não é parte implícita de ***Verificar todo o computador*** , você pode executar a verificação do rootkit diretamente da interface do ***Anti-Rootkit*** usando esse botão.

- ***Salvar alterações*** - pressione este botão para salvar todas as alterações feitas nessa interface e voltar para a ***interface do usuário do AVG padrão*** (*visão geral dos componentes*)

- ***Cancelar*** - pressione este botão para voltar para a ***interface do usuário AVG padrão*** (*visão geral dos componentes*) sem salvar as alterações feitas

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/AVG 2011/Gerenciador de Configurações do AVG

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

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

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

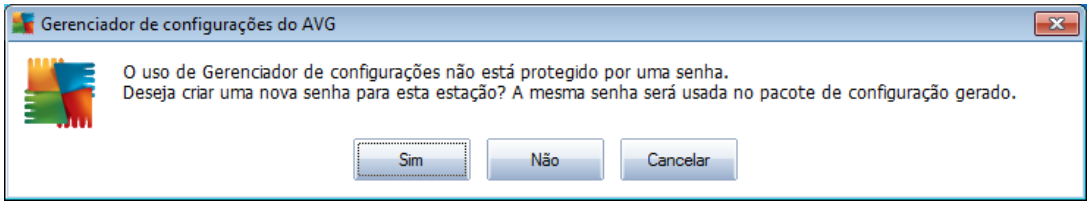
  Se você já possui um arquivo de configuração do AVG (.pck), use este botão para abri-lo e editá-lo. Quando você confirmar as modificações com o botão ***OK*** ou ***Aplicar***, o arquivo será substituído pelas novas configurações!

- ***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 (.pck) da instalação local do AVG. Se não tiver configurado uma senha para as Ações permitidas, pode ser exibida a seguinte caixa de diálogo:



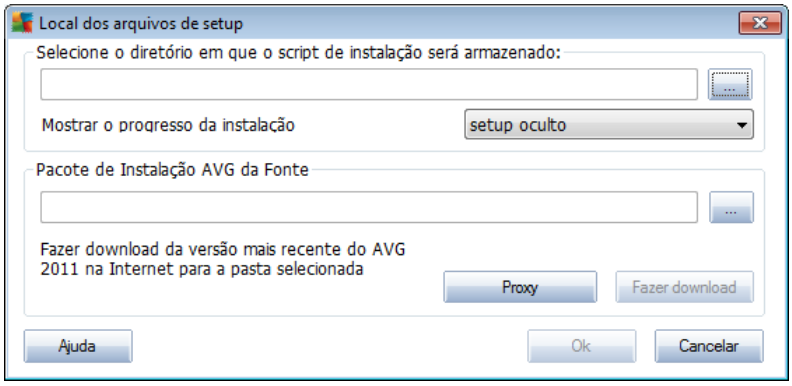
Responder ***Sim*** se desejar configurar a senha para acesso para Itens permitidos agora, preencha as informações solicitadas e confirme sua escolha. Responder ***Não*** para ignorar a criação de senha e continuar para salvar a configuração do AVG local para um arquivo.

- ***Clonar instalação do AVG***

Esta opção permite que você faça uma cópia do local de instalação do AVG criando um pacote de instalação com opções do consumidor. O clone inclui muitas das configurações do AVG, com exceção das seguintes:

- Configurações de idioma
- Configurações de som
- Configuração de firewall
- Lista de exceções de programas permitidos e potencialmente indesejáveis do componente de proteção da identidade.

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*** para fazer download do pacote de instalação do AVG mais recente disponível diretamente do site do AVG para a pasta selecionada ou coloque manualmente o pacote de instalação do AVG nesta pasta.

Você pode usar o botão ***Proxy*** para definir as configurações do servidor proxy se sua rede exigir isso para uma conexão bem-sucedida.

Clicando em ***OK***, o processo de clonagem será iniciado e deverá terminar rapidamente. Também pode aparecer uma caixa de diálogo solicitando a senha de configuração para os itens Permitidos (veja acima). Assim que terminar, o ***AvgSetup.bat*** deverá 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. Componentes de servidor do AVG

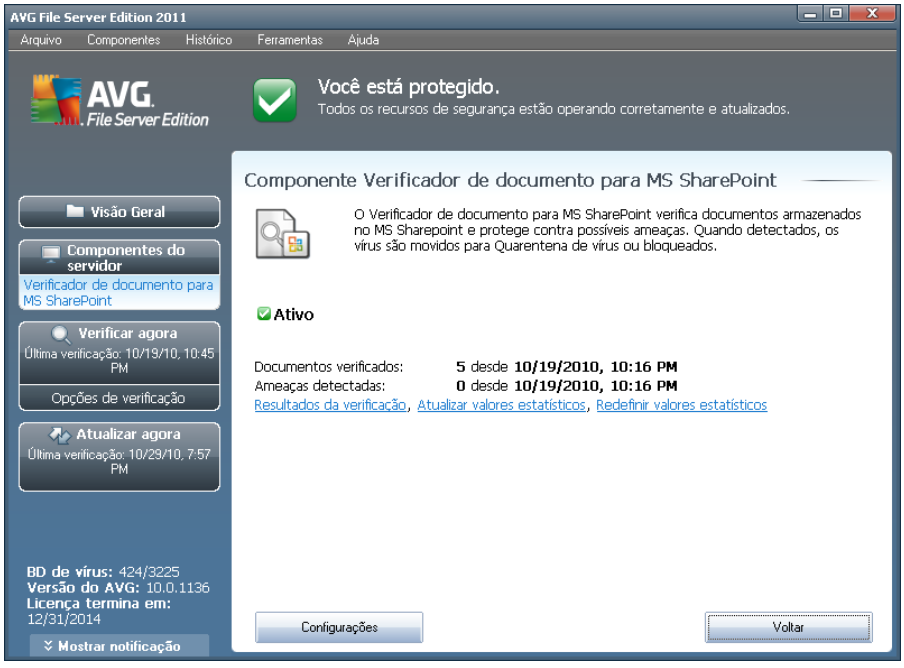
9.1. Verificador de Documentos para MS SharePoint

9.1.1. Princípios do Verificador de Documentos

A finalidade do componente de servidor ***Verificador de Documentos para MS SharePoint*** é verificar documentos armazenados no MS SharePoint. Se forem detectados vírus, eles serão movidos para a Quarentena de vírus ou totalmente removidos.

O Microsoft SharePoint é um conjunto de produtos e elementos de software que inclui, entre uma seleção cada vez maior de componentes, funções de colaboração do Explorer, módulos de gerenciamento de processo, módulos de pesquisa e uma plataforma de gerenciamento de documentos. O SharePoint pode ser usado para hospedar sites que acessam espaços de trabalho compartilhados, e armazena informações e documentos.

9.1.2. Interface do Verificador de Documentos



Além de uma visão geral dos dados estatísticos mais importantes e as informações sobre o status atual do componente (*Componente está ativo*), a interface ***Verificador de Documentos para MS SharePoint*** oferece uma visão geral resumida das estatísticas do componente :

- ***Documentos verificados*** - número de documentos verificados a partir de uma determinada data

- ***Ameaças detectadas*** - número de infecções detectadas a partir de uma determinada data

Você pode atualizar estas estatísticas a qualquer momento clicando no link ***Atualizar valores estatísticos***. Os novos dados aparecerão quase que imediatamente. Se você quiser definir todos os valores estatísticos para zero, clique no link ***Redefinir valores estatísticos***. Clicar no link ***Verificar resultados*** vai abrir uma nova caixa de diálogo contendo uma lista de verificação de resultados. Classifique os dados na lista usando os botões de rádio e/ou separadores.

Botões de controle

Os botões de controle disponíveis na interface ***Verificador de Documentos para MS SharePoint*** são:

- ***Configurações*** - abre uma nova caixa de diálogo na qual é possível ajustar diversos parâmetros relacionados ao desempenho de verificação de vírus de documentos do ***Verificador de Documentos para MS SharePoint*** (para obter mais informações sobre essa caixa de diálogo, leia o capítulo ***Configurações avançadas para o Verificador de Documentos para MS SharePoint*** e/ou ***Ações de detecção***).

- ***Voltar*** - pressione este botão para retornar à ***Interface de componentes do servidor*** padrão.

10. AVG para SharePoint Portal Server

Este capítulo trata da manutenção do AVG no ***MS SharePoint Portal Server***, que pode ser considerado um tipo especial de servidor de arquivos.

10.1. Manutenção do programa

O **<%AVG_FOR_SHAREPOINT_SERVER%>** usa a interface de verificação de vírus do Microsoft SP VSAPI 1.4 para a proteção do servidor contra possível infecção de vírus. Os objetos no servidor são testados em relação à presença de malware quando baixados e/ou enviados do servidor ou no servidor por seus usuários. A configuração da proteção antivírus pode ser definida usando a interface da ***Administração Central*** do seu SharePoint Portal Server. Na ***Administração Central***, é possível exibir e gerenciar o arquivo de log do **<%AVG_FOR_SHAREPOINT_SERVER%>**.

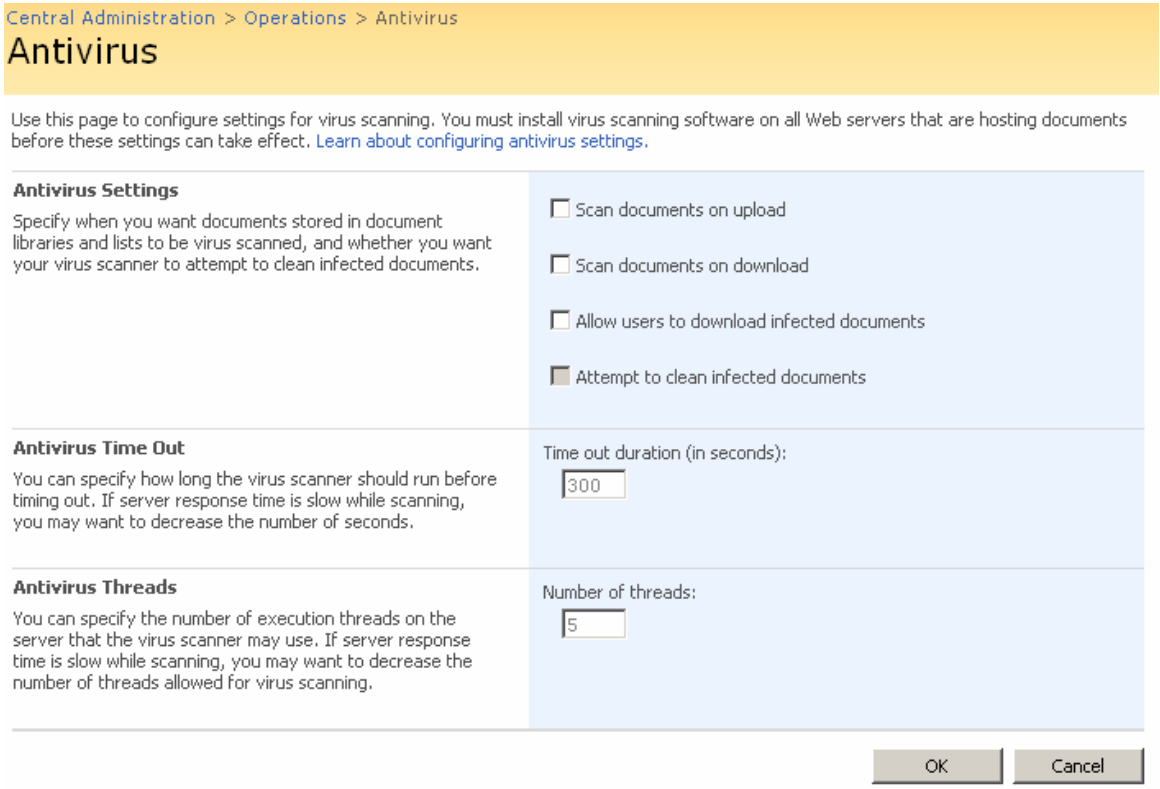
Você pode iniciar a ***Administração Central do SharePoint Portal Server*** quando conectado ao computador em que seu servidor estiver sendo executado. A interface do administrador é baseada na Web (*bem como a interface do usuário do SharePoint Portal Server*) e você pode abri-la usando a opção ***Administração Central do SharePoint*** na pasta ***Programas/Servidor Microsoft Office*** (dependendo da sua versão do ***SharePoint Portal Server***) no menu ***Iniciar*** do Windows ou navegando até as ***Ferramentas administrativas*** e selecionando ***Administração Central do Sharepoint***.

Você também pode acessar remotamente a página da Web da ***Administração Central do SharePoint Portal Server*** usando os direitos de acesso e URL apropriados.

10.2. AVG para Configuração SPPS - SharePoint 2007

Na interface da ***Administração Central do SharePoint 3.0***, você pode configurar com facilidade as ações e parâmetros de desempenho do verificador do **<% AVG_FOR_SHAREPOINT_SERVER%>**. Selecione a opção ***Operações*** na seção ***Administração Central***. Uma nova caixa de diálogo será exibida. Selecione o item ***Anti-vírus***na parte***Configuração de segurança***.

Em seguida, esta janela será exibida:

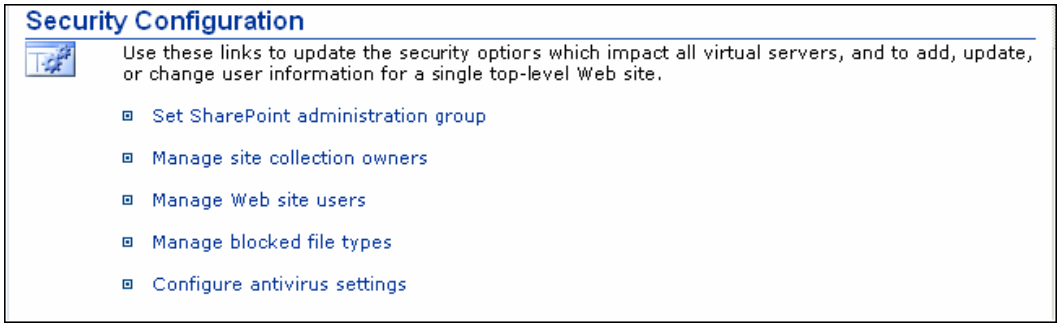


Você pode configurar várias ações de verificação de antivírus e recursos de desempenho do **<%AVG_FOR_SHAREPOINT_SERVER%>** aqui:

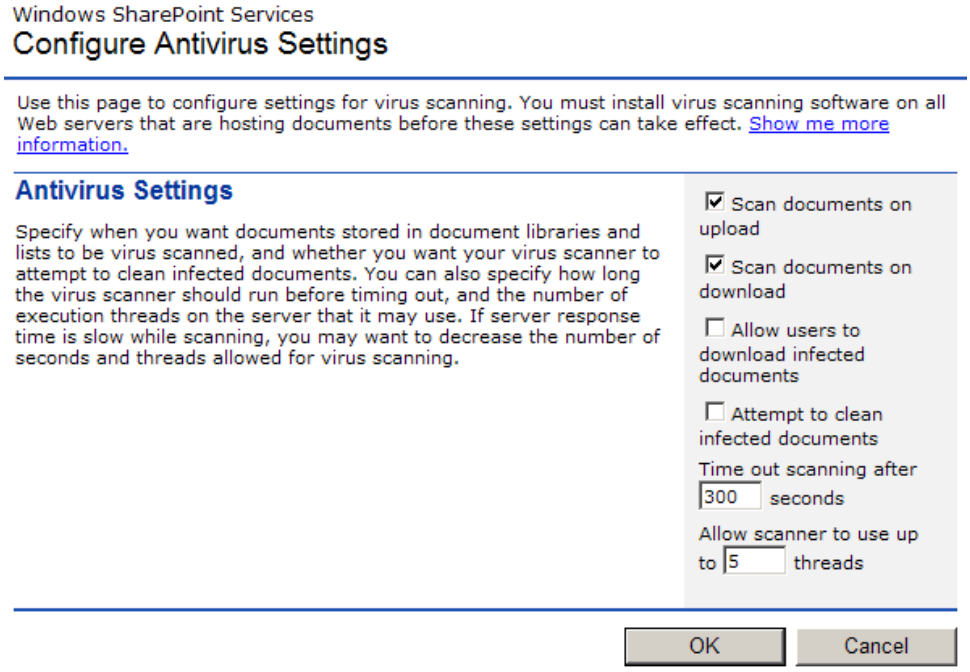
- ***Verificar documentos no envio*** – ativa/desativa a verificação de documentos que estão sendo enviados
- ***Verificar documentos no download*** – ativa/desativa a verificação de documentos que estão sendo baixados
- ***Permitir que usuários façam download de documentos infectados*** – permite/impede que usuários façam download de documentos infectados
- ***Tentar limpar documentos infectados*** – ativa/desativa a reparação automática de documentos infectados)
- ***Duração de tempo limite*** (*em segundos*) – o número máximo de segundos durante o qual o processo de verificação de vírus será executado após a inicialização simples (diminuir o valor quando a resposta do servidor parecer lenta durante a verificação de documentos)
- ***Número de processos*** – você pode especificar o número de processos de verificação de vírus que podem ser executados simultaneamente; aumentar o número pode agilizar a velocidade da verificação devido ao nível de paralelismo mais alto; por outro lado, pode aumentar o tempo de resposta do servidor

10.3. AVG para Configuração SPPS - SharePoint 2003

Na interface do ***Administração Central do SharePoint Portal Server***, é possível configurar com facilidade as ações e parâmetros de desempenho do verificador do **<%AVG_FOR_SHAREPOINT_SERVER%>**. Selecione a opção ***Configuração de ações do antivírus*** na seção ***Configuração de segurança***:



Em seguida, esta janela será exibida:



Você pode configurar várias ações de verificação de antivírus e recursos de desempenho do **<%AVG_FOR_SHAREPOINT_SERVER%>** aqui:

- ***Verificar documentos no envio*** – ativa/desativa a verificação de documentos que estão sendo enviados
- ***Verificar documentos no download*** – ativa/desativa a verificação de documentos que estão sendo baixados

- ***Permitir que usuários façam download de documentos infectados*** – permite/impede que usuários façam download de documentos infectados

- ***Tentar limpar documentos infectados*** – ativa/desativa a reparação automática de documentos infectados)

- ***Tempo limite de verificação*** – o número máximo de segundos em que o processo de verificação de vírus será executado após a inicialização simples (*diminui o valor quando a resposta do servidor parecer lenta durante a verificação de documentos*)

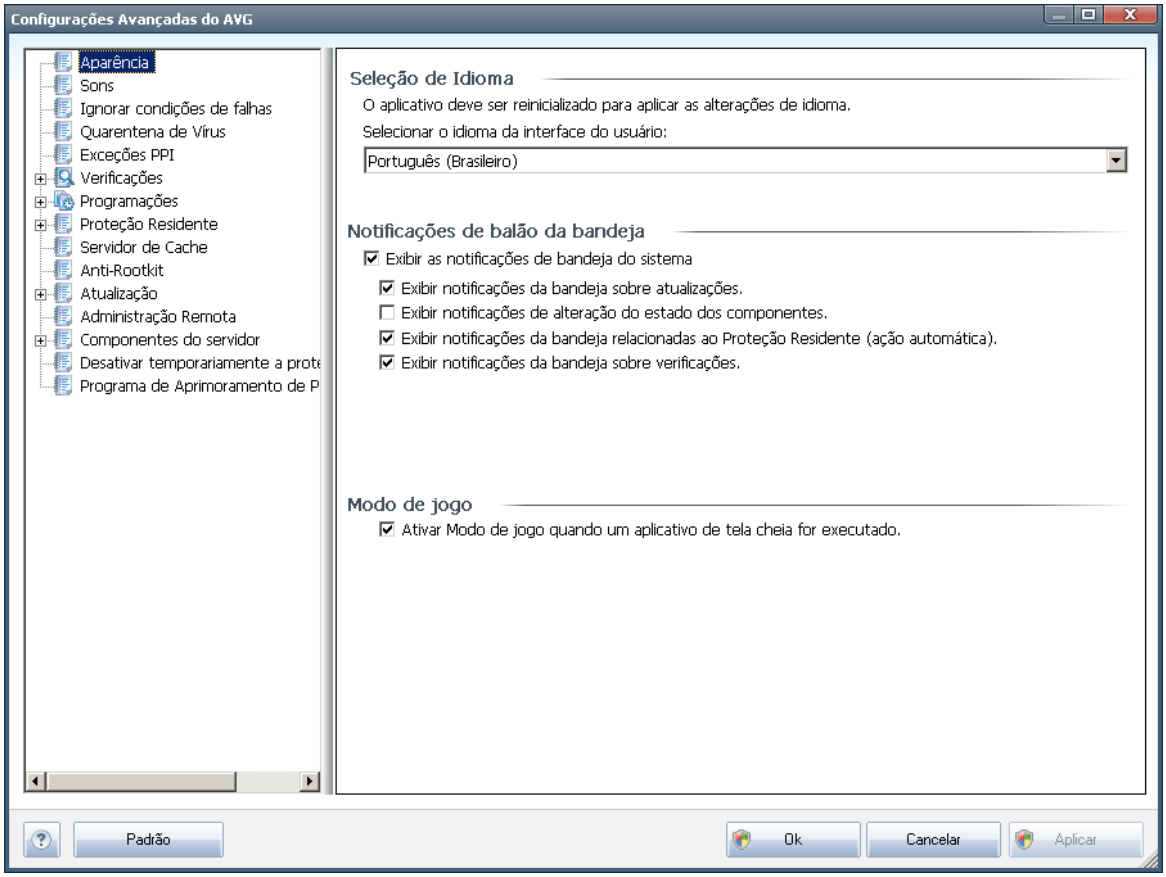
- ***Máx. uso Subprocessos X durante a verificação de documentos*** – X especifica o número de processos de verificação de vírus que podem ser executados simultaneamente; aumentar o número pode agilizar a velocidade da verificação devido ao nível mais alto de paralelismo; por outro lado, pode aumentar o tempo de resposta do servidor

11. Configurações avançadas do AVG

A caixa de diálogo de configuração avançada do **AVG Email Server Edition 2011** é aberta em uma nova janela denominada ***Configurações Avançadas do AVG***. A janela é dividida em duas seções: a parte da esquerda oferece uma navegação organizada em árvore para as opções de configuração do programa. Selecione o componente do qual deseja alterar a configuração do (*ou sua parte específica*) para abrir a caixa de edição na seção à direita da janela.

11.1. Aparência

O primeiro item na árvore de navegação, ***Aparência***, refere-se às configurações gerais dainterface de usuário do AVG e algumas opções básicas do comportamento do aplicativo:

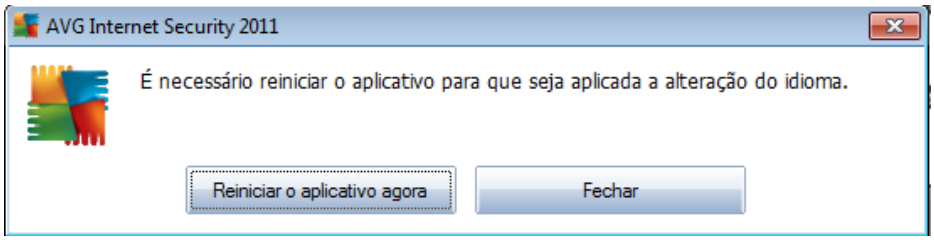


Seleção de idioma

Na seção ***Seleção de idioma***, você pode escolher o idioma desejado no menu suspenso; o idioma será usado em toda a interface de usuário do AVG. O menu suspenso só oferece os idiomas selecionados anteriormente para serem usados durante o processo de instalação (*consulte o capítulo Opção Personalizada*), além do inglês (*que vem instalado por padrão*). Entretanto, para concluir a alteração do aplicativo

para outro idioma, é necessário reiniciar a interface do usuário. Siga estas etapas:

- Selecione o idioma desejado para o aplicativo e confirme a seleção pressionando o botão ***Aplicar*** (canto inferior direito)
- Pressione o botão ***OK*** para confirmar
- É exibida uma nova janela de diálogo pop-up informando que a alteração de idioma da interface do usuário do AVG exige a reinicialização do aplicativo:



Notificações de balão da bandeja

Nesta seção, você poderá suprimir a exibição das notificações de balão da bandeja no status do aplicativo. Por padrão, as notificações de balão podem ser exibidas e é recomendável manter essa configuração! As notificações de balão geralmente informam sobre alguma alteração de status do componente do AVG e você deve prestar atenção nelas.

Entretanto, se por alguma razão você optar por não exibir essas notificações ou se desejar a exibição de apenas algumas notificações (relacionadas a um componente do AVG específico), poderá definir e especificar suas preferências selecionando/ cancelando a seleção das seguintes opções:

- ***Exibir notificações da bandeja do sistema*** - por padrão, este item fica marcado (*como ativado*) e as notificações são exibidas. Desmarque este item para desativar completamente a exibição de todas as notificações de balão. Quanto ativado, é possível selecionar quais notificações específicas devem ser exibidas:
  - ***Exibir notificações da bandeja sobre atualizações*** - defina se as informações referentes ao início, andamento ou finalização do processo do de atualização do AVG devem ser exibidas;
  - ***Exibir notificações de mudança de estado de componentes*** - decidir se informações relativas à atividade/inatividade de componentes ou seu possível problema devem ser exibidas. Ao relatar o status de falha de um componente, esta opção se iguala à função informativa do ícone da bandeja do sistema (mudança de cor) relatando um problema em quaisquer componentes da AVG;
  - ***Exibir notificações referentes a Proteção Residente (ação automática)*** - decida se as informações relativas a salvar, copiar e abrir

processos devem ser exibidas ou omitidas (*esta configuração apenas demonstra se a opção Reparo automático de Proteção Residente está ativada*);

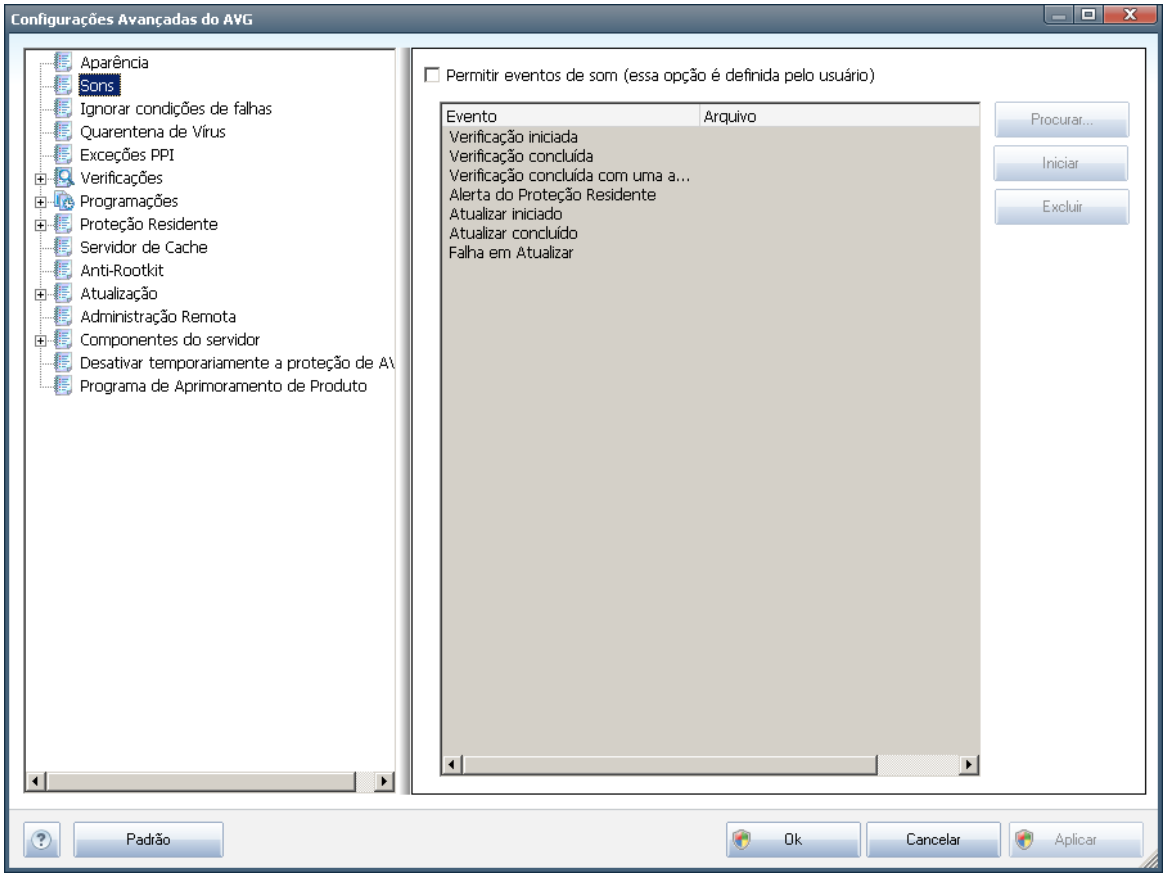
- ***Exibir notificações sobre verificação*** - decida se as informações sobre início automático da verificação agendada, seu andamento e resultados devem ser exibidos;

Modo de jogo

Esta função do AVG foi desenvolvida para aplicativos de tela inteira em que possíveis balões de informação do AVG (*exibidos, por exemplo, quando uma verificação programada é iniciada*) poderiam gerar problemas (*podem minimizar o aplicativo ou corromper seus gráficos*). Para evitar essa situação, mantenha marcada a caixa de seleção referente à opção ***Ativar modo de jogo quando um aplicativo de tela inteira for executado*** (*configuração padrão*).

11.2. Sons

Na caixa de diálogo ***Sons***, você pode especificar se deseja receber informações sobre ações especificas do AVG via notificação sonora. Em caso positivo, marque a opção ***Ativar eventos sonoros*** (*desativada por padrão*) para ativar a lista de ações do AVG:

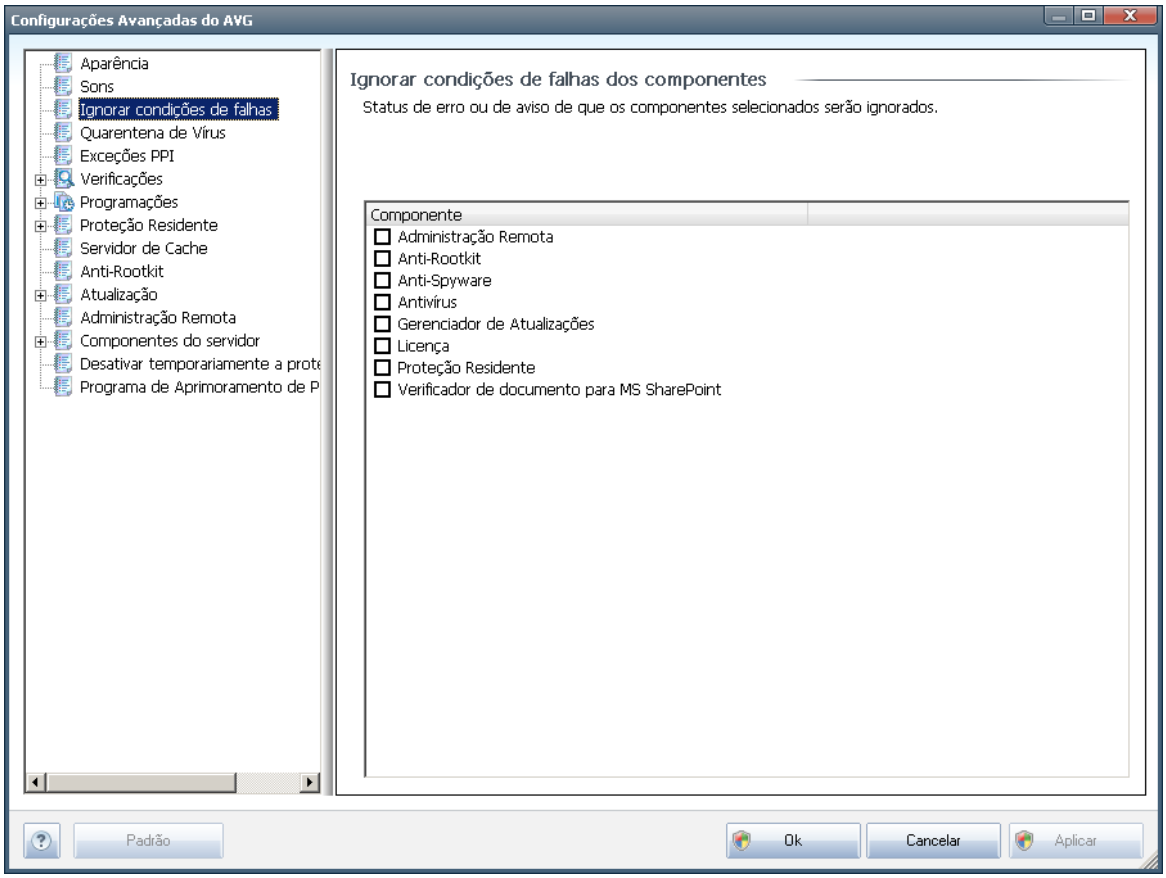


Em seguida, selecione o respectivo evento na lista e procure (usando a opção ***Procurar***) um som apropriado no disco rígido que deseja atribuir a esse evento. Para ouvir o som selecionado, realce o evento na lista e pressione o botão ***Reproduzir***. Use o botão ***Excluir*** para remover o som atribuído a um evento específico.

Observação: *apenas sons *.wav podem ser usados!*

11.3. Ignorar condições de falhas

Na caixa de diálogo ***Ignorar condições de falhas dos componentes*** você pode marcar aqueles componentes sobre os quais não deseja obter informações:



Por padrão, não há componentes selecionados nesta lista. Isto significa que, caso qualquer componente receba um status de erro, você será informado sobre isso imediatamente via:

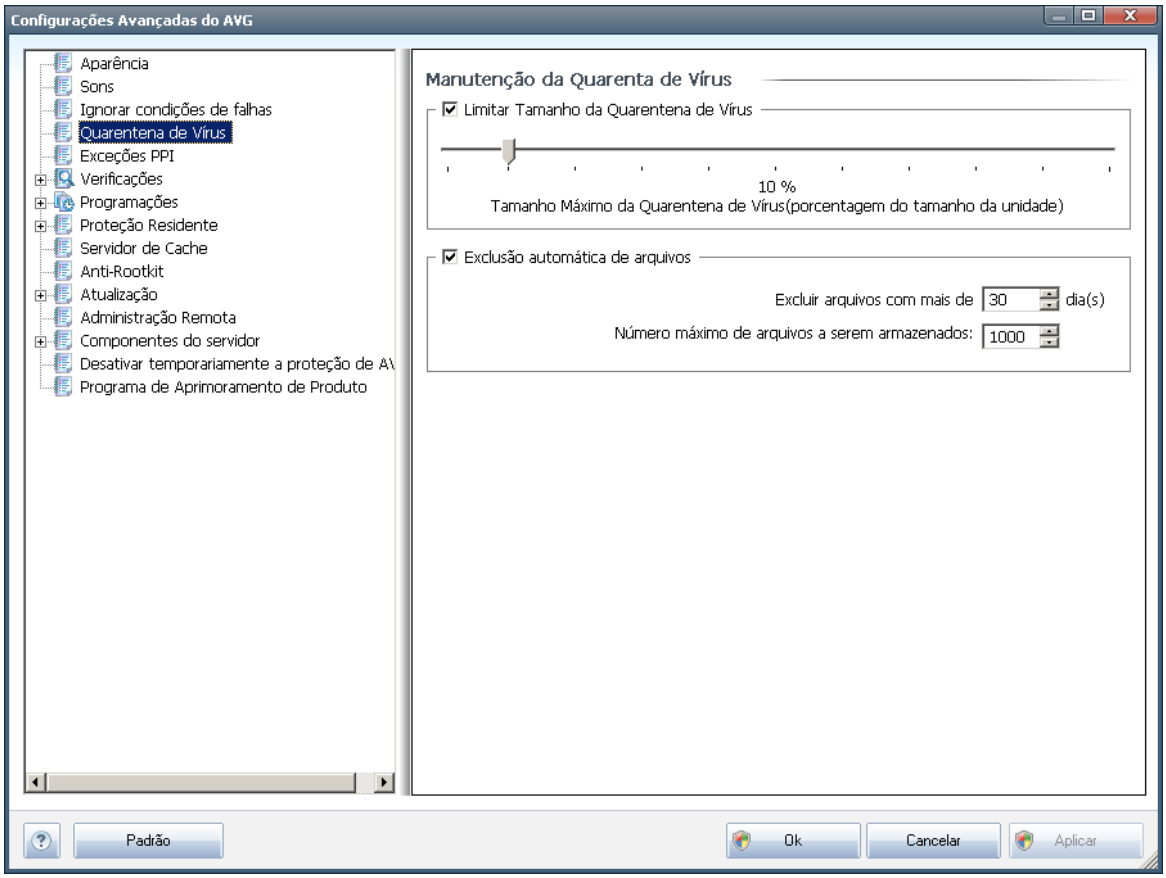
- ***ícone da bandeja do sistema*** - enquanto todos os componentes do AVG estão funcionando adequadamente, o ícone é exibido em quatro cores; entretanto, se ocorrer um erro, os ícones aparecem com um ponto de exclamação amarelo,
- descrição textual do problema na seção ***Informações sobre Status de Segurança*** na janela principal do AVG

Pode acontecer que, por alguma razão, você precise desligar um componente por certo tempo (*não é recomendável, você deve tentar manter todos os componentes sempre ligados e em sua configuração padrão, mas pode acontecer*). Neste caso, o ícone da bandeja do sistema relata automaticamente o status de erro do componente. Entretanto, neste caso em particular, não se pode falar de um erro, pois você deliberadamente o induziu, e está ciente do provável risco. Ao mesmo tempo, assim

que é exibido em cinza, o ícone não pode relatar qualquer outro erro que possa aparecer.

Neste caso, na caixa de diálogo acima você pode selecionar componentes que podem estar com status de erro (*ou desligados*) e sobre os quais você não deseja receber informações. A mesma opção ***Ignorando o estado do componente*** também está disponível para componentes específicos diretamente da visão geral dos componentes na janela principal do AVG.

11.4. Quarentena de vírus



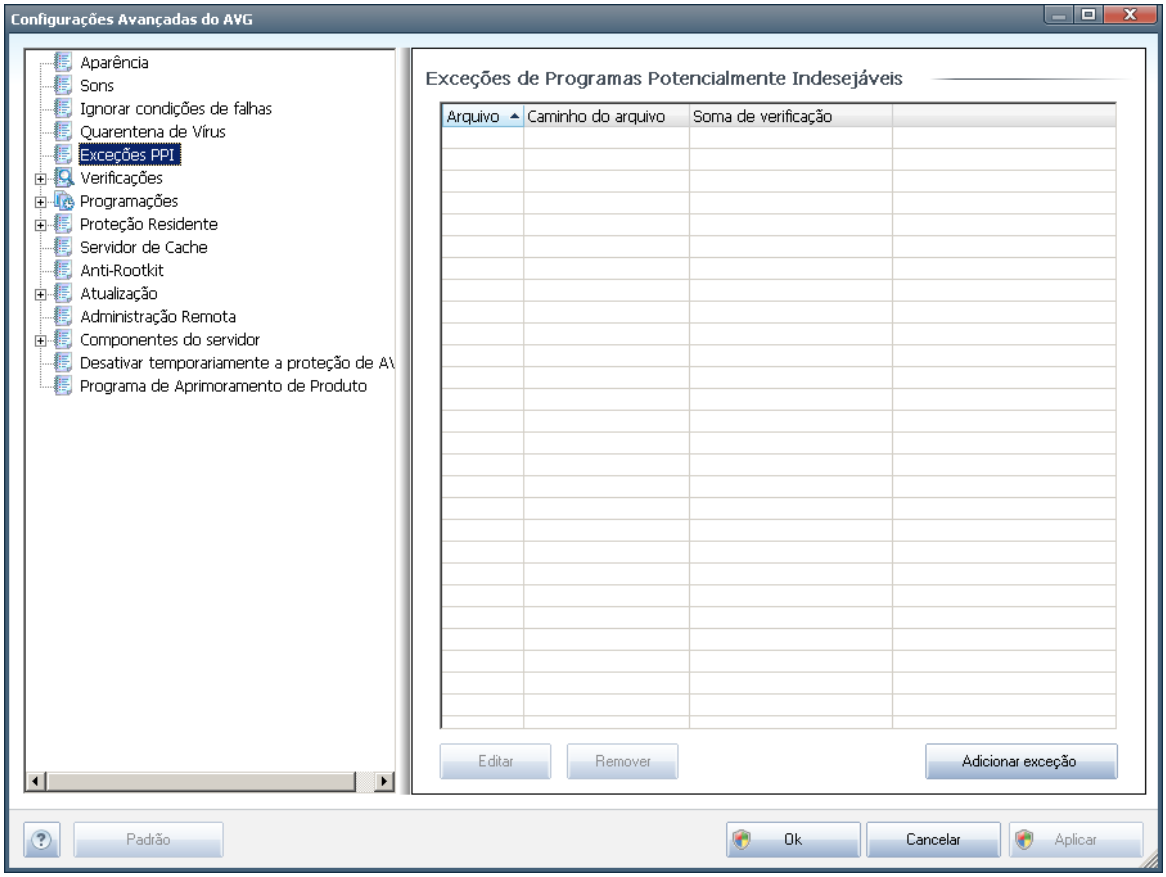
A caixa de diálogo ***Manutenção da quarentena*** permite definir vários parâmetros relativos à administração de objetos armazenados na ***Quarentena***:

- ***Limitar tamanho da Quarentena de vírus*** - use o controle deslizante para definir o tamanho máximo da ***Quarentena de vírus***. O tamanho é especificado proporcionalmente ao tamanho do seu disco rígido local.

- ***Exclusão automática de arquivo*** - nessa seção, defina a duração máxima de armazenamento dos objetos na ***Quarentena*** (***Excluir arquivos mais antigos que...***) e o número máximo de arquivos a serem armazenados na ***Quarentena*** (***Número máximo de arquivos a serem armazenados***).

11.5. Exceções PPI

O AVG Email Server Edition 2011 é capaz de analisar e detectar aplicativos executáveis ou bibliotecas DLL que possam ser potencialmente indesejáveis no sistema. Pode ser que o usuário deseje manter, em alguns casos, determinados programas indesejáveis no computador (*programas instalados propositalmente*). Alguns programas, especialmente os gratuitos, incluem adware. Esse adware pode ser detectado e reportado pelo AVG como um ***programa potencialmente indesejável***. Se desejar manter esse programa no computador, você poderá defini-lo como uma exceção de programa potencialmente indesejável:



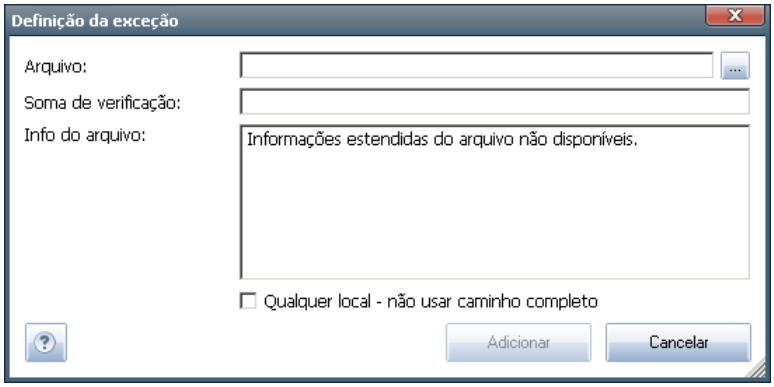
A caixa de diálogo ***Exceções de programa potencialmente indesejável*** exibe uma lista das exceções definidas e válidas atualmente dos programas não desejados. É possível editar a lista, excluir itens existentes ou adicionar novas exceções. As informações a seguir podem ser encontradas na lista para cada exceção:

- ***Arquivo*** - fornece o nome do respectivo aplicativo
- ***Caminho do arquivo*** - mostra a localização do aplicativo
- ***Soma de Verificação*** - exibe a 'assinatura' exclusiva do arquivo selecionado. Essa Soma de verificação é uma string de caracteres gerados automaticamente, que permite ao AVG diferenciar inequivocamente o arquivo

escolhido dos outros arquivos. A Soma de verificação é gerada e exibida após a adição bem-sucedida do arquivo.

Botões de controle

- ***Editar*** - abre uma caixa de diálogo de edição (*idêntica à da definição de exceção; veja abaixo*) de uma exceção já definida, na qual é possível alterar os parâmetros de exceção
- ***Remover*** - exclui o item selecionado da lista de exceções
- ***Adicionar exceção*** - abre uma caixa de diálogo de exceção na qual é possível definir os parâmetros da nova exceção a ser criada:



  - ***Arquivo*** - digite o caminho completo para o arquivo que deseja marcar como uma exceção
  - ***Soma de verificação*** - exibe a 'assinatura' exclusiva do arquivo selecionado. Essa Soma de verificação é uma string de caracteres gerados automaticamente, que permite ao AVG diferenciar inequivocamente o arquivo escolhido dos outros arquivos. A Soma de verificação é gerada e exibida após a adição bem-sucedida do arquivo.
  - ***Informações do arquivo*** - exibe outras informações disponíveis sobre o arquivo (*informações de licença/versão etc.*)
  - ***Qualquer local - não use caminhos completos*** - se quiser definir o arquivo como uma exceção apenas no local específico, deixe a caixa de seleção desmarcada. Se a caixa de seleção estiver marcada, o arquivo especificado será definido como uma exceção, não importa onde esteja (*entretanto, você precisa especificar o caminho completo para o arquivo específico de qualquer forma; o arquivo será usado como um exemplo exclusivo para a possibilidade de que dois arquivos com o mesmo nome apareçam no sistema*).

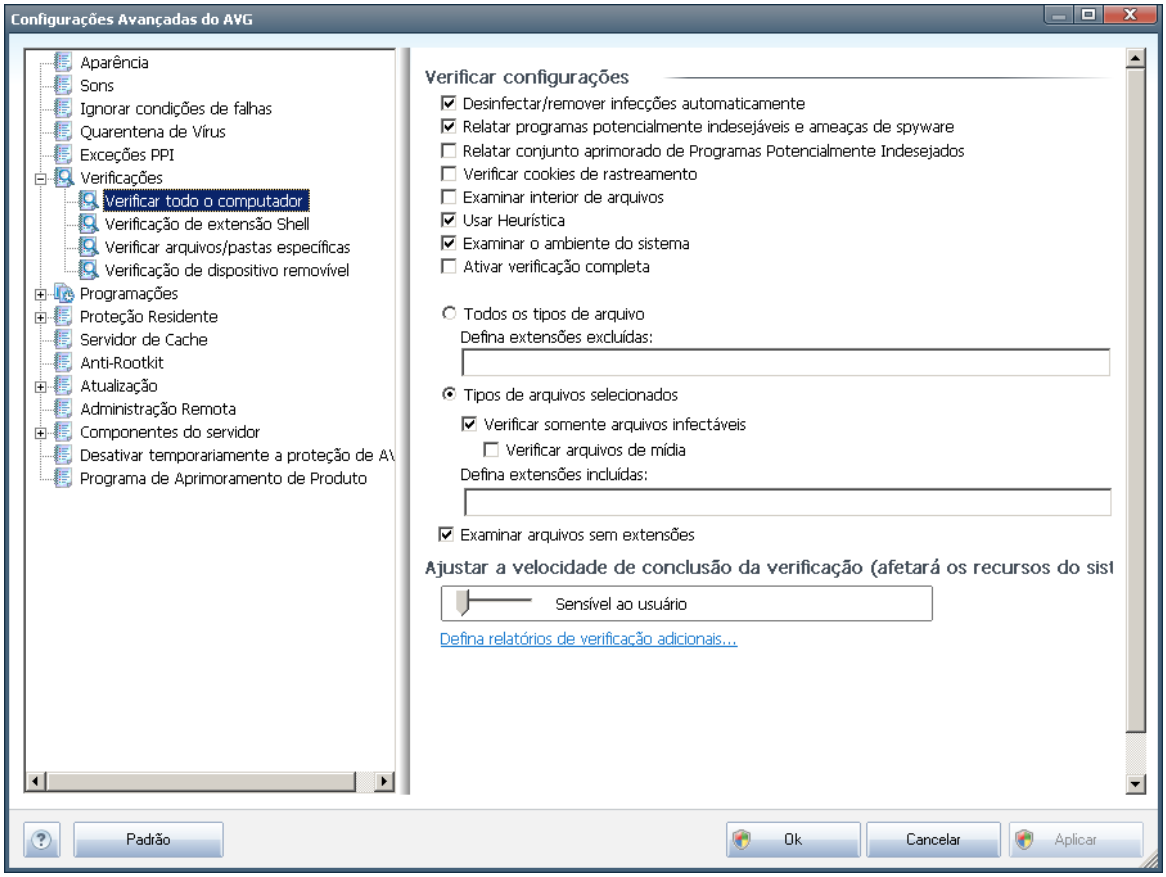
11.6. Verificações

As configurações de verificação avançadas estão divididas em três categorias referentes a tipos específicos de verificação, conforme definido pelo fornecedor do software:

- ***Verificar todo o computador*** - verificação padrão predefinida de todo o computador
- ***Verificação de extensão Shell*** - verificação específica de um objeto selecionado diretamente do ambiente do Windows Explorer
- ***Verificar arquivos ou pastas específicos*** - verificação padrão predefinida de áreas selecionadas do computador
- ***Verificação de dispositivos removíveis*** - verificação específica de dispositivos removíveis conectados ao computador

11.6.1. Verificar todo o computador

A opção ***Verificar todo o computador*** permite editar parâmetros de uma das verificações predefinidas pelo fornecedor do software, ***Verificar todo o computador***:



Configurações da verificação

Na guia ***Configurações da verificação*** , você encontrará uma lista de parâmetros de verificação que podem ser ativados ou desativados.

- ***Reparar ou remover vírus automaticamente*** (*ativada por padrão*) - se um vírus for identificado durante a verificação, ele pode ser reparado automaticamente, se houver solução disponível. Se o arquivo infectado não puder ser reparado automaticamente, o objeto infectado será movido para a ***Quarentena de Vírus***.

- ***Informar programas potencialmente indesejáveis e ameaças de spyware*** (*ativada por padrão*) - marque para ativar o mecanismo ***Anti-Spyware*** e verificar spyware, bem como vírus. Spyware representa uma categoria de malware questionável: embora ele geralmente represente um risco de segurança, alguns desses programas pode ser instalado intencionalmente. Recomendamos manter esse recurso ativado, pois aumenta a segurança do computador.

- ***Informar conjunto avançado de programas potencialmente indesejáveis*** (*desativada por padrão*) - marque para detectar o pacote estendido de spyware: programas que estão perfeitamente ok e são inofensivos quando adquiridos do fabricante diretamente, mas podem ser mal-utilizados para finalidades mal-intencionadas posteriormente. Esta é uma medida adicional que aumenta ainda mais a segurança de seu computador; no entanto, pode eventualmente bloquear programas legais, e, portanto, é desativada por padrão.

- ***Verificar cookies de rastreamento*** (*desativada por padrão*) - este parâmetro do componente Anti-Spyware define que os cookies devem ser detectados; (*cookies HTTP são usados para autenticar, controlar e manter informações específicas sobre usuários, como preferências de sites ou conteúdo de carrinhos de compras eletrônicas*)

- ***Verificar dentro dos arquivos*** (*desativada por padrão*) - esse parâmetro define que a verificação deve ocorrer em todos os arquivos armazenados dentro de arquivos, como ZIP, RAR etc.

- ***Usar Heurística*** (*ativada por padrão*) - a análise heurística (*emulação dinâmica das instruções do objeto verificado, em um ambiente de computador virtual*) será um dos métodos usados para detecção de vírus durante a verificação;

- ***Verificar ambiente do sistema*** (*ativada por padrão*) - a verificação também atuará nas áreas do sistema do seu computador.

- ***Ativar verificação completa*** (*desativada por padrão*) - em situações específicas (*suspeita de que seu computador foi infectado*), é possível marcar esta opção para ativar a maioria dos algoritmos de verificação completos que verificarão até mesmo as áreas do computador que dificilmente são infectadas,

só para ter a absoluta certeza. Entretanto, lembre-se de que esse método consome bastante tempo.

Além disso, você deve decidir se deseja verificar

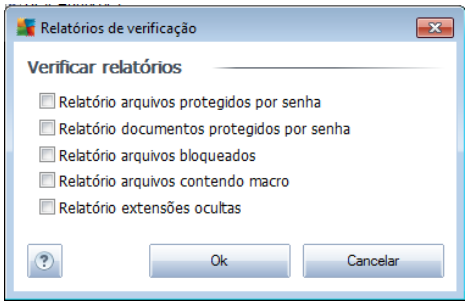
- ***Todos os tipos de arquivos*** com a possibilidade de definirem exceções a partir da verificação, fornecendo uma lista de extensões de arquivo separadas por vírgula (sendo salvas, as vírgulas mudam para ponto-e-vírgulas) que não devem ser verificadas;
- ***Tipos de arquivos selecionados*** - você pode especificar que deseja verificar apenas os arquivos possivelmente infectáveis (*arquivos que não podem ser infectados não serão verificados; por exemplo, alguns arquivos de texto simples ou outros arquivos não executáveis*), incluindo arquivos de mídia (*arquivos de áudio e vídeo - se você deixar essa caixa desmarcada, o tempo de verificação será ainda menor, pois esses arquivos costumam ser grandes, e é muito improvável que eles sejam infectados por vírus*). Mais uma vez, é possível especificar por extensões quais são os arquivos que sempre devem ser verificados.
- Opcionalmente, você pode optar por ***Verificar arquivos sem extensão*** - essa opção está ativada por padrão, e convém mantê-la nesse estado, a não ser que você tenha um motivo concreto para alterá-la. Arquivos sem extensão são relativamente suspeitos e devem ser verificados sempre.

Ajustar a velocidade de conclusão da verificação

Na seção ***Ajustar a velocidade de conclusão da verificação***, você poderá especificar a velocidade de verificação desejada, dependendo do uso do recurso do sistema. Por padrão, esse valor de opção é definido no nível *Sensível ao usuário* de uso automático do recurso. A verificação poderá ser acelerada, mas a utilização de recursos do sistema será bem maior durante sua execução e as outras atividades do PC terão o desempenho reduzido (*essa opção pode ser usada quando o computador está ligado, mas ninguém está trabalhando nele*). Por outro lado, você pode diminuir a utilização dos recursos do sistema ampliando a duração da verificação.

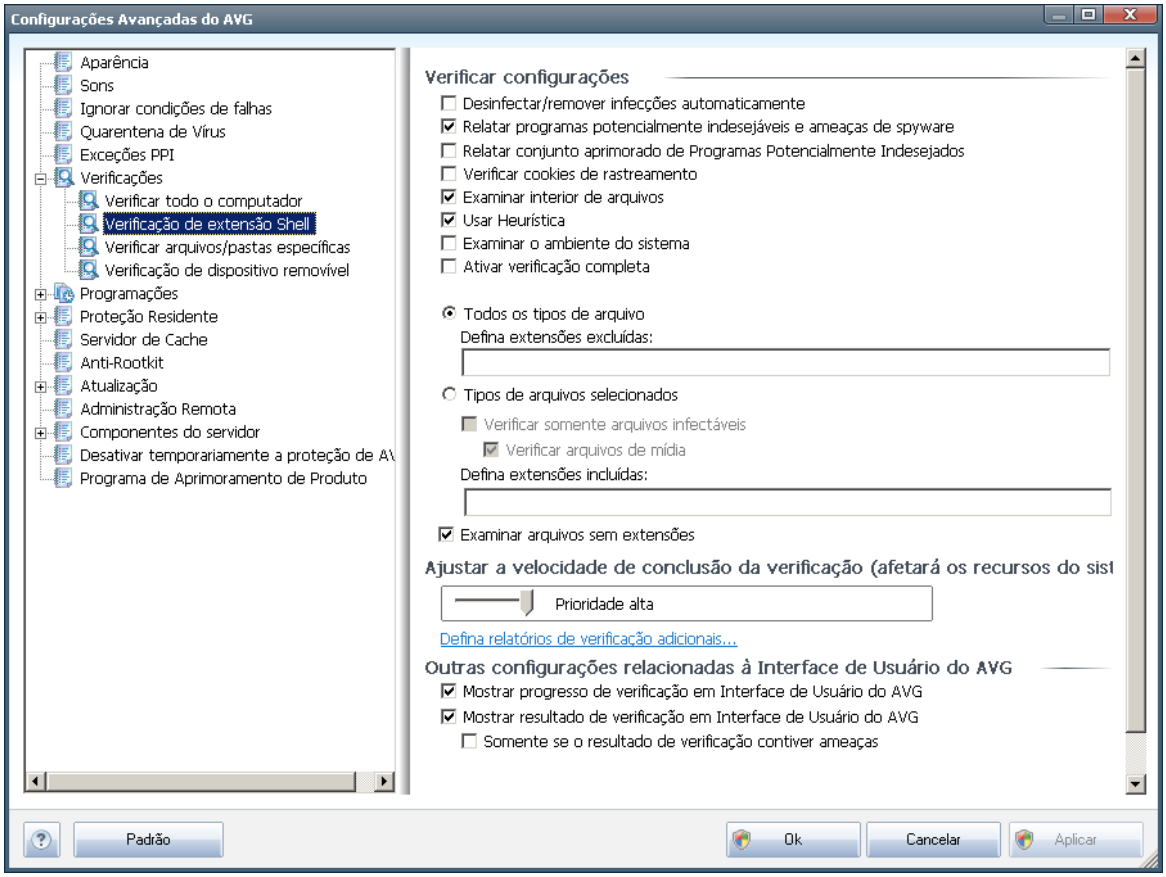
Defina relatórios de verificação adicionais...

Clique no link ***Definir relatórios de verificação adicionais...*** para abrir uma janela independente da caixa de diálogo chamada ***Verificar relatórios*** na qual você pode marcar vários itens para definir quais localizações da verificação devem ser relatadas:



11.6.2. Verificação da extensão shell

Da mesma forma que o item anterior, ***Verificar todo o computador*** , este item, denominado ***Verificação da extensão shell*** também oferece várias opções para editar a verificação predefinida pelo fornecedor do software. Dessa vez a configuração é relacionada à verificação de objetos específicos inicializados diretamente no ambiente do Windows Explorer (*extensão shell*). Consulte o capítulo ***Verificação do Windows Explorer***:



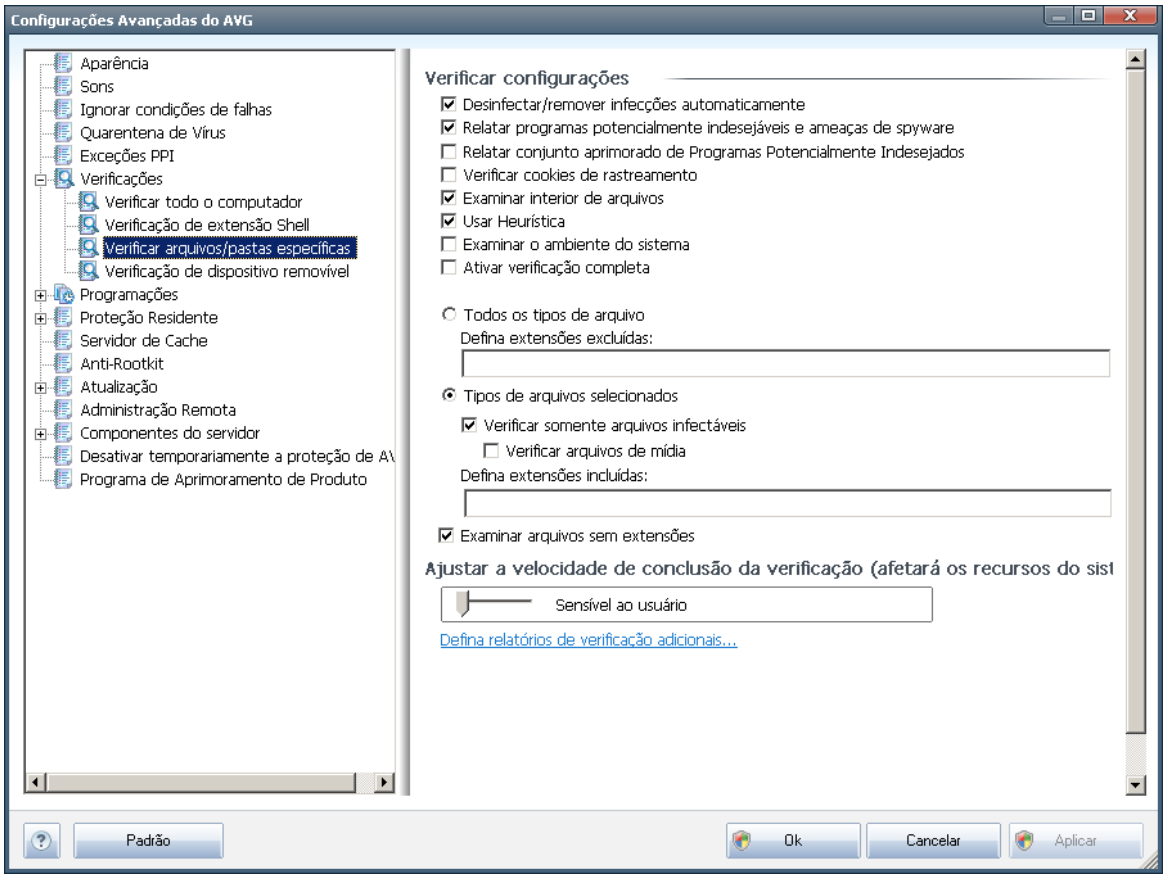
A lista de parâmetros é idêntica à disponível para ***Verificar todo o computador***. Entretanto, as configurações padrão são diferentes (*por exemplo, Verificar todo o computador, por padrão, não verifica os arquivos, mas verifica o ambiente de sistema, ao passo que com a Verificação da Extensão Shell, é ao contrário*).

Observação:*para obter uma descrição dos parâmetros específicos, consulte o capítulo* ***Configurações avançadas do AVG/Verificações/Verificar todo o computador****.*

Em comparação com a caixa de diálogo ***Verificar todo o computador*** , a caixa de diálogo ***Verificação da extensão shell*** também possui uma seção denominada ***Outras configurações relacionadas à interface do usuário do AVG***, onde você pode especificar se deseja que o progresso da verificação e os resultados da verificação estejam acessíveis na interface do usuário do AVG. Além disso, você pode definir que o resultado da verificação seja exibido apenas se uma infecção for detectada durante a verificação.

11.6.3. Verificar arquivos ou pastas específicos

A interface de edição de ***Verificar arquivos ou pastas específicos*** é idêntica à caixa de diálogo de edição ***Verificar todo o computador***. Todas as opções de configuração são as mesmas, porém as configurações padrão são mais rigorosas em ***Verificar todo o computador*** .

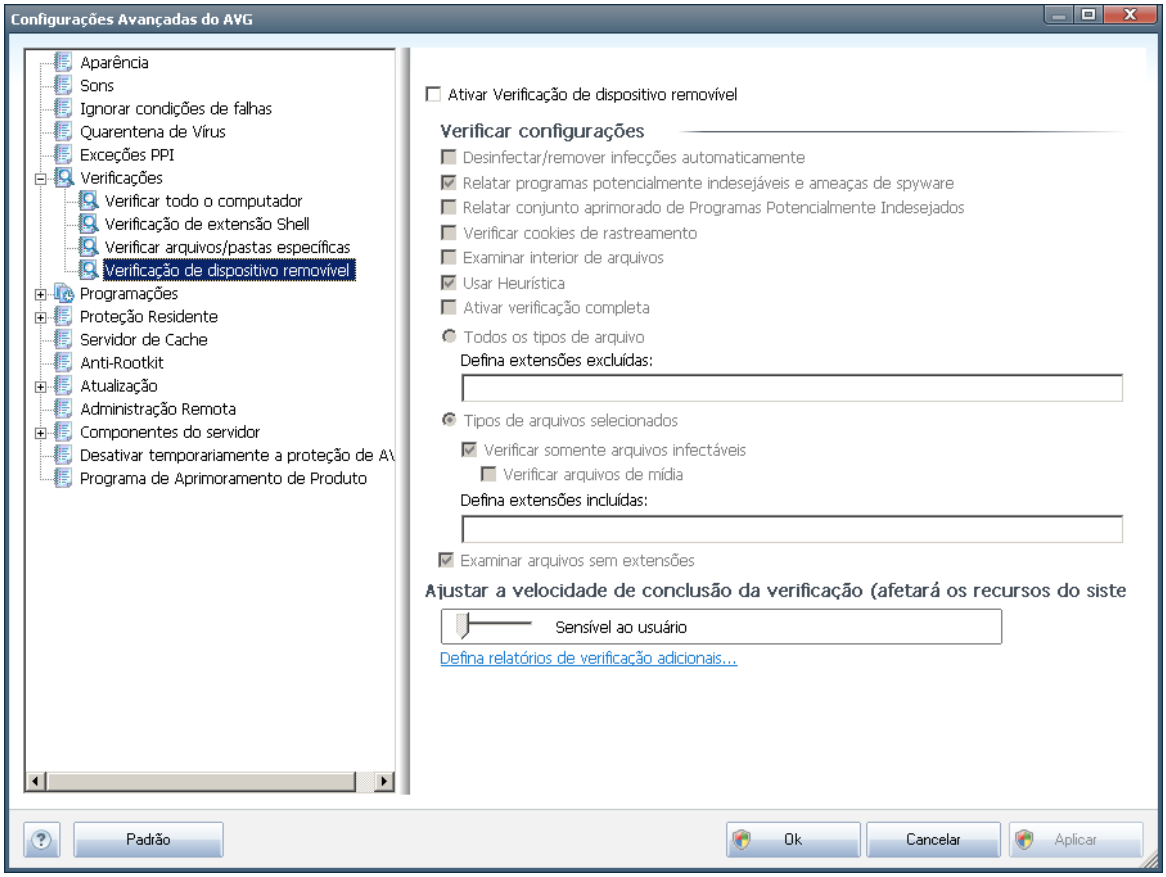


Todo os parâmetros definidos nesta caixa de diálogo de configuração são válidos somente para as áreas selecionadas para verificação com a ***Verificação de arquivos ou pastas específicos***!

Observação:*para obter uma descrição dos parâmetros específicos, consulte o capítulo* ***Configurações avançadas do AVG/Verificações/Verificar todo o computador****.*

11.6.4. Verificação de dispositivo removível

A interface de edição de ***Verificação de dispositivo removível*** também é muito semelhante à caixa de diálogo de edição ***Verificar todo o computador***:



A ***Verificação de dispositivo removível*** é ativada automaticamente quando você conecta um dispositivo removível ao computador. Por padrão, essa verificação está desativada. No entanto, é essencial verificar dispositivos removíveis em busca de ameaças potenciais, pois são uma das fontes principais de infecção. Para que a verificação esteja pronta e seja iniciada quando necessário, marque a opção ***Ativar verificação de dispositivo removível*** .

Observação:*para obter uma descrição dos parâmetros específicos, consulte o capítulo* ***Configurações avançadas do AVG/Verificações/Verificar todo o computador****.*

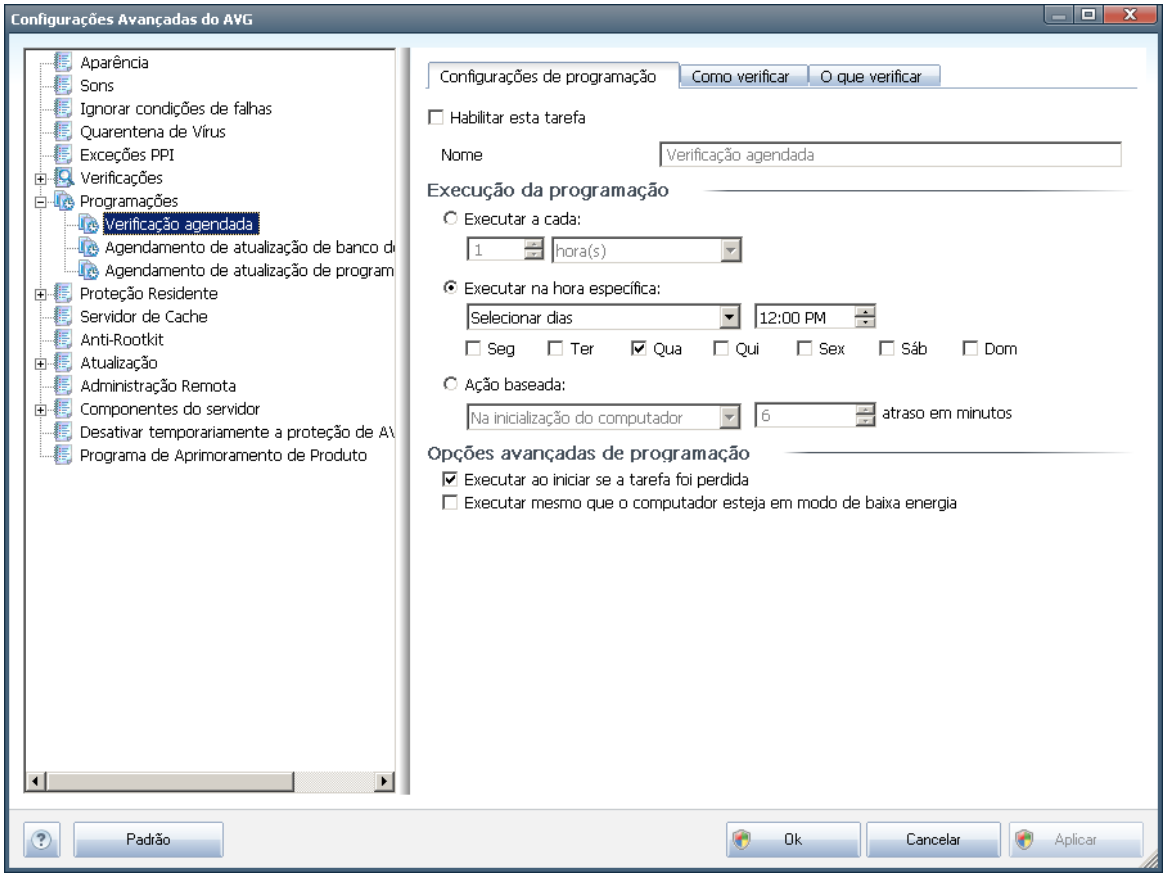
11.7. Programações

Na seção ***Agendamentos***, é possível editar as configurações padrão de:

- Verificação agendada
- Agendamento de atualização de banco de dados de vírus
- Agendamento de atualização de programa

11.7.1. Verificação programada

Os parâmetros da verificação agendada podem ser editados(*ou uma nova configuração de agenda*) em três guias:



Na guia ***Configurações de agendamento***, você pode primeiro marcar/desmarcar o item ***Habilitar esta tarefa*** para simplesmente desativar temporariamente o teste programado e ativá-lo novamente conforme necessário.

Em seguida, no campo de texto denominado ***Nome*** (*desativado para todas as programações padrão*), existe o nome atribuído a essa programação pelo fornecedor

do programa. Para programações recém-adicionadas (*é possível adicionar uma nova programação clicando com o botão direito no item* ***Verificação programada*** *na área de navegação esquerda*), você pode especificar o seu próprio nome e, nesse caso, o campo de texto ficará aberto para edição. Tente sempre usar nomes curtos, descritivos e apropriados para a verificação para tornar seu reconhecimento mais fácil posteriormente.

Exemplo: *não é apropriado denominar a verificação como "Nova verificação" ou "Minha verificação", pois esses nomes não se referem exatamente ao que será verificado. Por outro lado, um exemplo de nome descritivo ideal seria "Verificação de áreas do sistema" etc. Além disso, não é necessário especificar no nome da verificação se ela é uma verificação de todo o computador ou somente uma verificação de pastas ou arquivos selecionados. Suas verificações serão sempre uma versão específica da verificação de arquivos ou pastas selecionados.*

Nessa caixa de diálogo você ainda poderá definir os seguintes parâmetros de verificação:

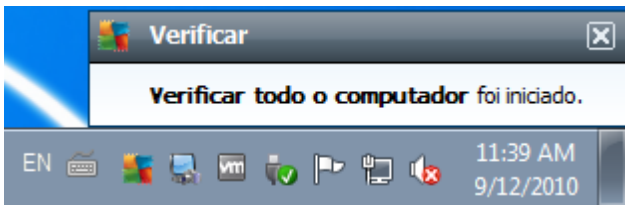
Execução da programação

Aqui, você pode especificar intervalos de tempo para a ativação da verificação recém-programada. O tempo pode ser definido pela repetição da ativação da verificação depois de um determinado período (***Executar a cada ...***), pela definição de uma data e hora exatas (***Executar em uma hora específica...***) ou possivelmente pela definição de um evento ao qual a ativação da verificação deve ser associada (***Ação baseada na inicialização do computador***).

Opções avançadas de programação

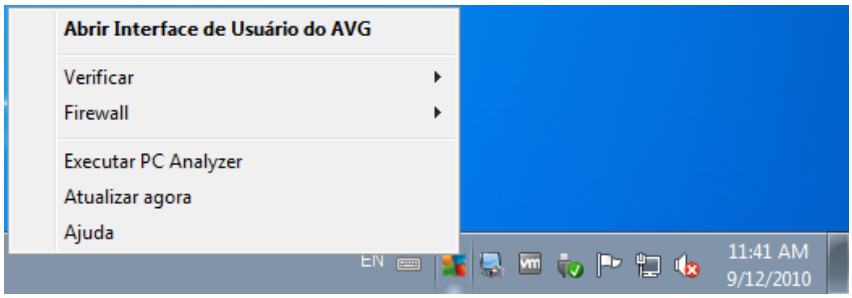
Essa seção permite definir sob quais condições a verificação deverá ou não ser inicializada se o computador estiver no modo de pouca energia ou completamente desligado.

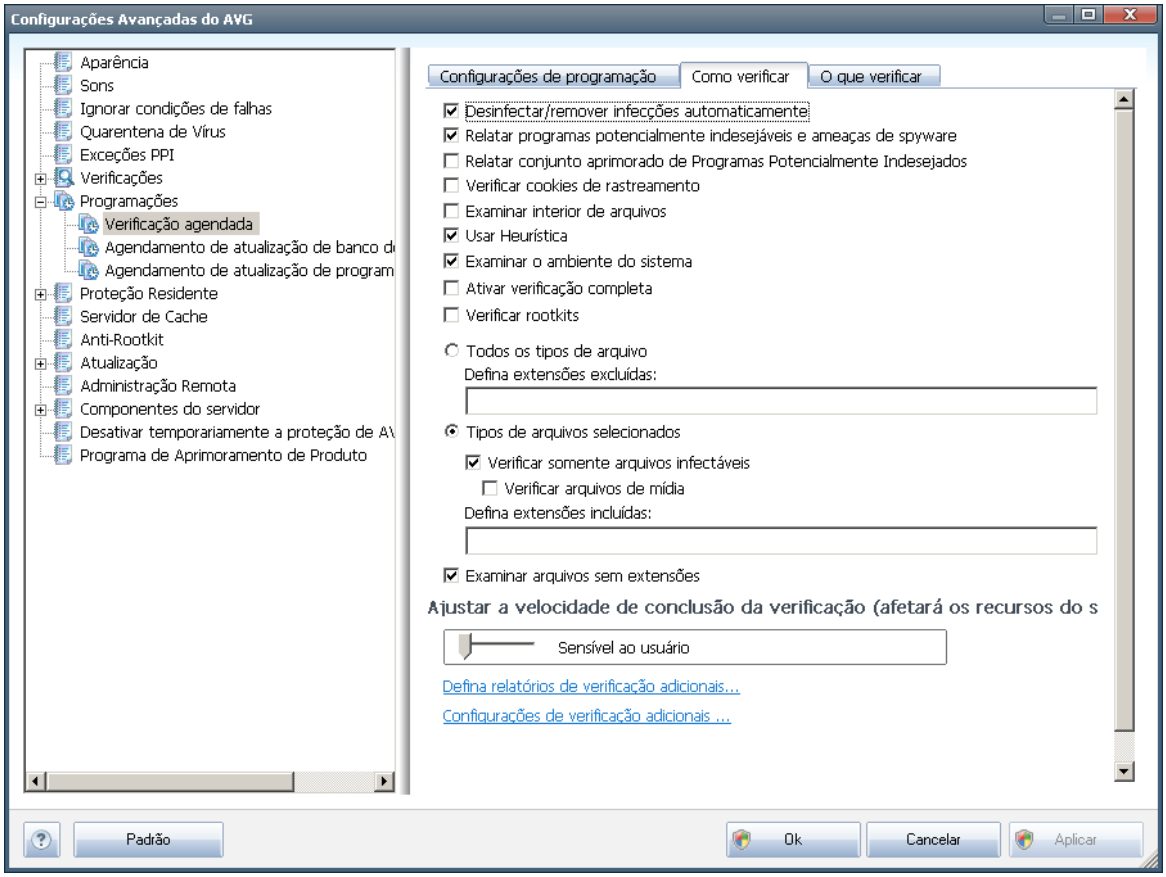
Uma vez que a verificação agendada é iniciada no horário que você especificou, você será informado deste fato por uma janela pop-up aberta sobre o ícone AVG na bandeja do sistema:



Um novo ícone AVG na bandeja do sistema aparece (*em cores e com um holofote*) informando que uma verificação agendada está em execução. Clique com o botão direito do mouse no ícone AVG da verificação em execução para abrir um menu de contexto, onde você pode escolher pausar ou até interromper a verificação e também

alterar a prioridade da verificação em execução:





Na guia ***Como verificar*** , você encontrará uma lista de parâmetros de verificação que podem ser ativados ou desativados. Por padrão, a maioria dos parâmetros é ativada e a funcionalidade será aplicada durante a verificação. A menos que você tenha um motivo válido para alterar as configurações, recomendamos manter a configuração predefinida:

- ***Reparar ou remover vírus automaticamente*** *(ativado por padrão):* se um vírus for identificado durante a verificação, ele poderá ser reparado automaticamente, se houver solução disponível. Se o arquivo infectado não puder ser reparado automaticamente, o objeto infectado será movido para a

Quarentena de Vírus.

- ***Informar programas potencialmente indesejáveis e ameaças de spyware*** *(ativada por padrão):* marque para ativar o mecanismo ***Anti-Spyware*** e verificar se há spyware, bem como vírus. Spyware representa uma categoria de malware questionável: embora ele geralmente represente um risco de segurança, alguns desses programas pode ser instalado intencionalmente. Recomendamos manter esse recurso ativado, pois aumenta a segurança do computador.

- ***Informar conjunto avançado de programas potencialmente indesejáveis*** (*desativada por padrão*): marque para detectar o pacote estendido de spyware: programas que estão perfeitamente ok e são inofensivos quando adquiridos do fabricante diretamente, mas podem ser mal-utilizados para finalidades mal-intencionadas posteriormente. Esta é uma medida adicional que aumenta ainda mais a segurança de seu computador; no entanto, pode eventualmente bloquear programas legais, e, portanto, é desativada por padrão.

- ***Verificar cookies de rastreamento*** (*desativada por padrão*): este parâmetro do componente ***Anti-Spyware*** define que os cookies devem ser detectados durante a verificação; (*cookies HTTP são usados para autenticar, controlar e manter informações específicas sobre usuários, como preferências de sites ou conteúdo de carrinhos de compras eletrônicas*)

- ***Verificar interior dos arquivos*** (*desativada por padrão*): este parâmetro define que a verificação deve atuar em todos os arquivos, mesmo que eles estejam compactados em algum tipo de arquivo, como ZIP, RAR etc.

- ***Usar Heurística*** (*ativada por padrão*): a análise heurística (*emulação dinâmica das instruções do objeto verificado, em um ambiente de computador virtual*) será um dos métodos usados para detecção de vírus durante a verificação;

- ***Verificar ambiente do sistema*** (*ativada por padrão*): a verificação também atuará nas áreas do sistema do seu computador;

- ***Ativar verificação completa*** (*desativada por padrão*) - em situações específicas (*suspeita de que seu computador foi infectado*), é possível marcar esta opção para ativar a maioria dos algoritmos de verificação completos que verificarão até mesmo as áreas do computador que dificilmente são infectadas, só para ter a absoluta certeza. Entretanto, lembre-se de que esse método consome bastante tempo.

- ***Verificar rootkits*** (*desativada por padrão*): marque este item se desejar incluir a detecção de rootkit na verificação de todo o computador. A detecção de rootkit também está disponível por meio do componente ***Anti-Rootkit***;

Além disso, você deve decidir se deseja verificar

- ***Todos os tipos de arquivos*** com a possibilidade de definirem exceções a

partir da verificação, fornecendo uma lista de extensões de arquivo separadas por vírgula (sendo salvas, as vírgulas mudam para ponto-e-vírgulas)

- ***Tipos de arquivos selecionados*** - você pode especificar que deseja verificar apenas os arquivos possivelmente infectáveis (*arquivos que não podem ser infectados não serão verificados; por exemplo, alguns arquivos de texto simples ou outros arquivos não executáveis*), incluindo arquivos de mídia (*arquivos de áudio e vídeo - se você deixar essa caixa desmarcada, o tempo de verificação será ainda menor, pois esses arquivos costumam ser grandes, e é muito improvável que eles sejam infectados por vírus*). Mais uma vez, é possível especificar por extensões quais são os arquivos que sempre devem ser verificados.

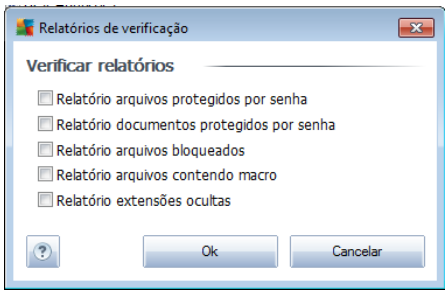
- Opcionalmente, você pode optar por ***Verificar arquivos sem extensão*** - essa opção está ativada por padrão, e convém mantê-la nesse estado, a não ser que você tenha um motivo concreto para alterá-la. Arquivos sem extensão são relativamente suspeitos e devem ser verificados sempre.

Ajustar a velocidade de conclusão da verificação

Na seção ***Ajustar a velocidade de conclusão da verificação***, você poderá especificar a velocidade de verificação desejada, dependendo do uso do recurso do sistema. Por padrão, esse valor de opção é definido no nível *Sensível ao usuário* de uso automático do recurso. A verificação poderá ser acelerada, mas a utilização de recursos do sistema será bem maior durante sua execução e as outras atividades do PC terão o desempenho reduzido (*essa opção pode ser usada quando o computador está ligado, mas ninguém está trabalhando nele*). Por outro lado, você pode diminuir a utilização dos recursos do sistema ampliando a duração da verificação.

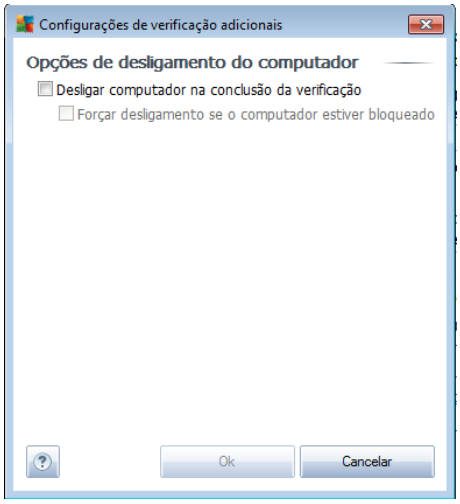
Defina relatórios de verificação adicionais

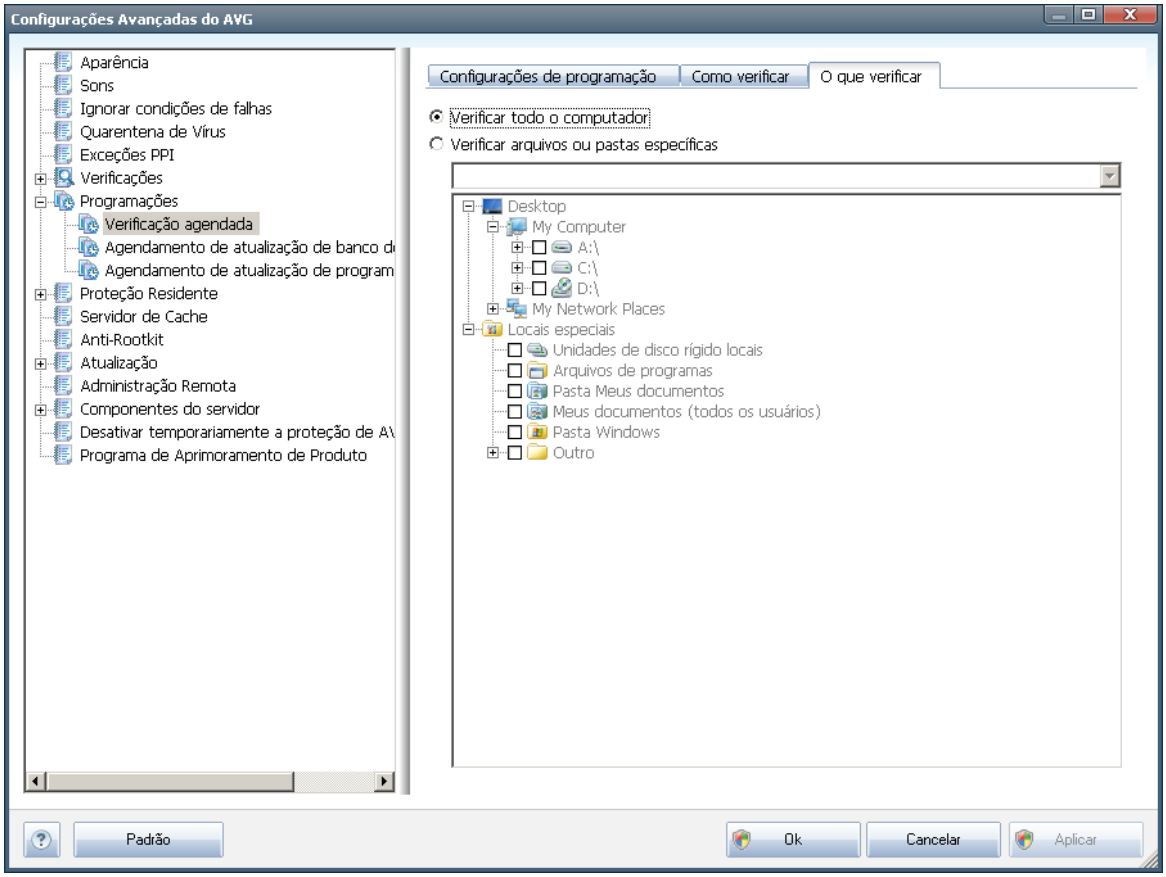
Clique no link ***Definir relatórios de verificação adicionais...*** para abrir uma janela independente da caixa de diálogo chamada ***Verificar relatórios*** na qual você pode marcar vários itens para definir quais localizações da verificação devem ser relatadas:



Configurações de verificação adicionais

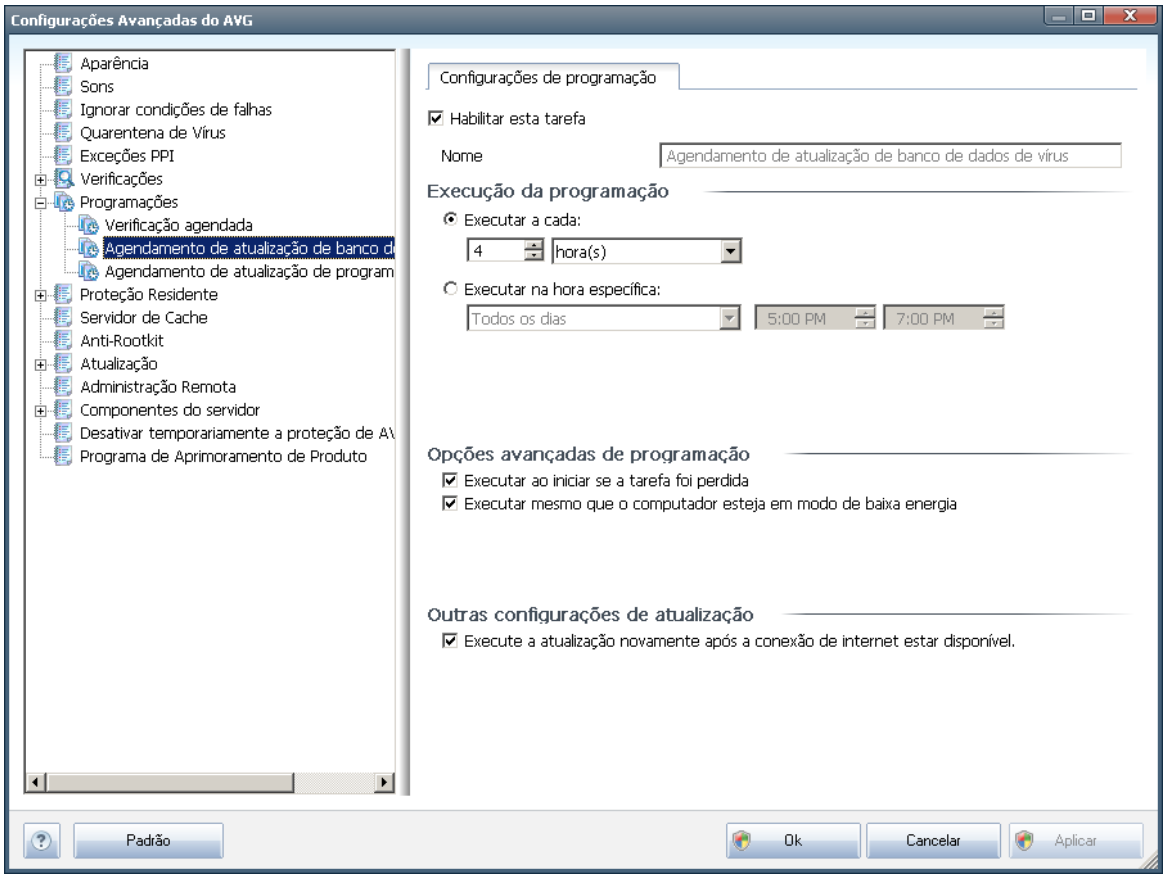
Clique em ***Configurações de verificação adicionais ...*** para abrir uma nova caixa de diálogo ***Opções de desligamento do computador*** que permite decidir se o computador deve ser desligado automaticamente assim que o processo de verificação estiver terminado. Ao confirmar essa opção (***Desligar o computador quando o processo de verificação for concluído***), uma nova opção permitirá que o computador seja desligado mesmo se ele estiver bloqueado (***Forçar desligamento do computador se estiver bloqueado***).





Na guia ***O que verificar***, você pode definir se deseja programar a verificação de todo o computador ou a verificação de arquivos ou pastas específicas***. Se você selecionar a verificação de arquivos ou pastas específicas, na parte inferior dessa caixa de diálogo a estrutura de árvore exibida será ativada e você poderá especificar as pastas para verificação.

11.7.2. Programação de atualização de banco de dados de vírus



Na guia ***Configurações de agendamento***, você pode primeiro marcar/desmarcar o item ***Habilitar esta tarefa*** para simplesmente desativar temporariamente a atualização do banco de dados de vírus agendada e ativá-la novamente conforme necessário. O banco de dados básico de vírus é coberto no componente ***Gerenciador de Atualização***. Nessa caixa de diálogo, você pode configurar parâmetros detalhados de agendamento de atualização do banco de dados de vírus. No campo de texto denominado ***Nome*** (*desativado para todas as programações padrão*), existe o nome atribuído a essa programação pelo fornecedor do programa.

Execução da programação

Nessa seção, especifique os intervalos de tempo para a inicialização da atualização do banco de dados de vírus recém-agendada. O prazo pode ser definido pelo início repetido de atualização após certo período de tempo (***Executar a cada...***) ou definindo um data e hora exatos (***Executar na hora específica...***).

Opções avançadas de programação

Essa seção permite definir sob quais condições a atualização do banco de dados de

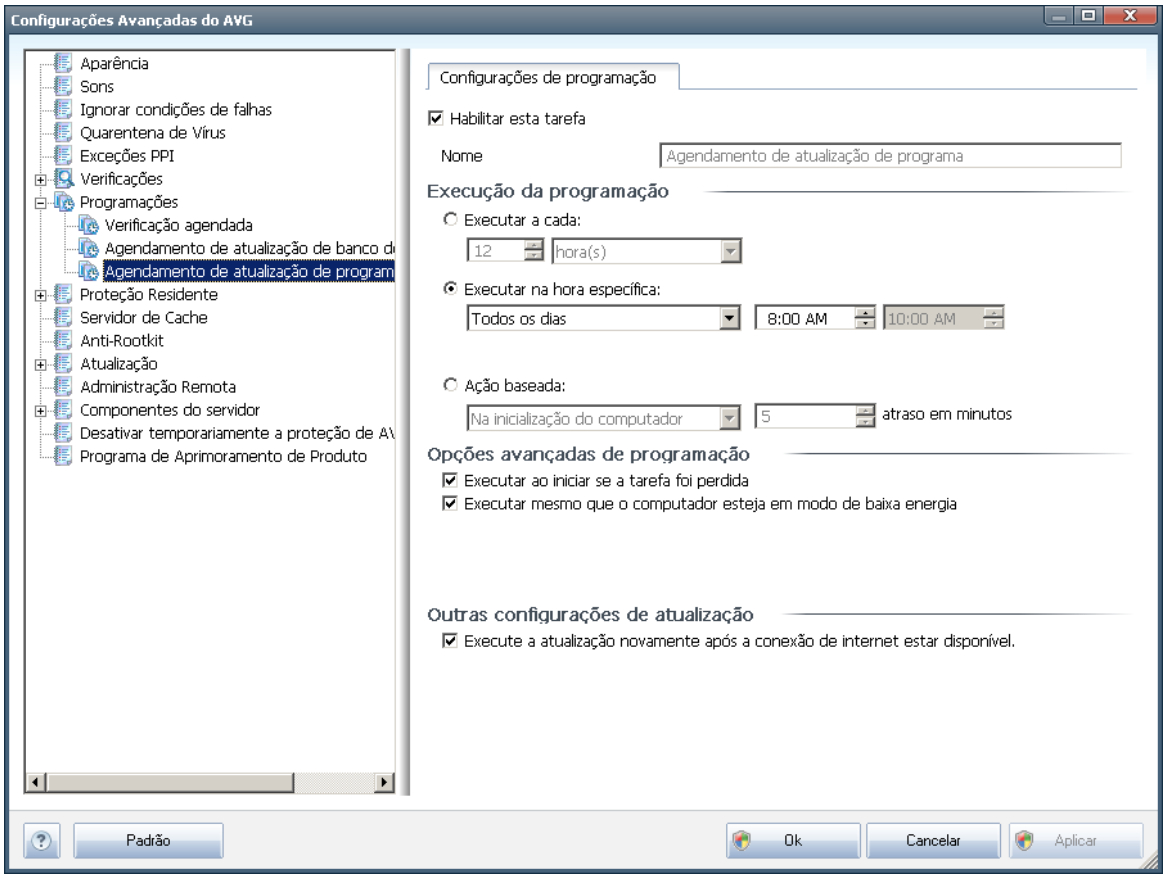
vírus deverá ou não ser inicializada se o computador estiver no modo de pouca energia ou completamente desligado.

Outras configurações de atualização

Por fim, marque a opção ***Executar novamente a atualização assim que uma conexão com a Internet estiver disponível***, para ter certeza de que, se a conexão com a Internet ficar corrompida e o processo de atualização falhar, ele será imediatamente reiniciado quando a conexão com a Internet for restaurada.

Assim que a atualização programada for iniciada na hora especificada, você será informado por uma janela pop-up aberta sobre o ícone AVG na bandeja do sistema (*caso você tenha mantido a configuração padrão da caixa de diálogo* ***Configurações avançadas/Aparência***).

11.7.3. Programação de atualização de programa



Na guia ***Configurações de agendamento***, você pode primeiro marcar/desmarcar o item ***Habilitar esta tarefa*** para simplesmente desativar temporariamente a atualização do programa agendada e ativá-la novamente conforme necessário. No campo de texto denominado ***Nome*** (*desativado para todas as programações padrão*), existe o nome atribuído a essa programação pelo fornecedor do programa.

Execução da programação

Aqui, especifique os intervalos de tempo para iniciar a atualização do programa recém-programada. O tempo pode ser definido pela repetição da inicialização da atualização depois de um determinado período (***Executar a cada...***), pela definição de uma data e hora exatas (***Executar em uma hora específica...***) ou pela definição de um evento ao qual a inicialização da atualização deve ser associada (***Ação baseada na inicialização do computador***).

Opções avançadas de programação

Essa seção permite definir sob quais condições a atualização do programa deverá ou não ser inicializada se o computador estiver no modo de pouca energia ou completamente desligado.

Outras configurações de atualização

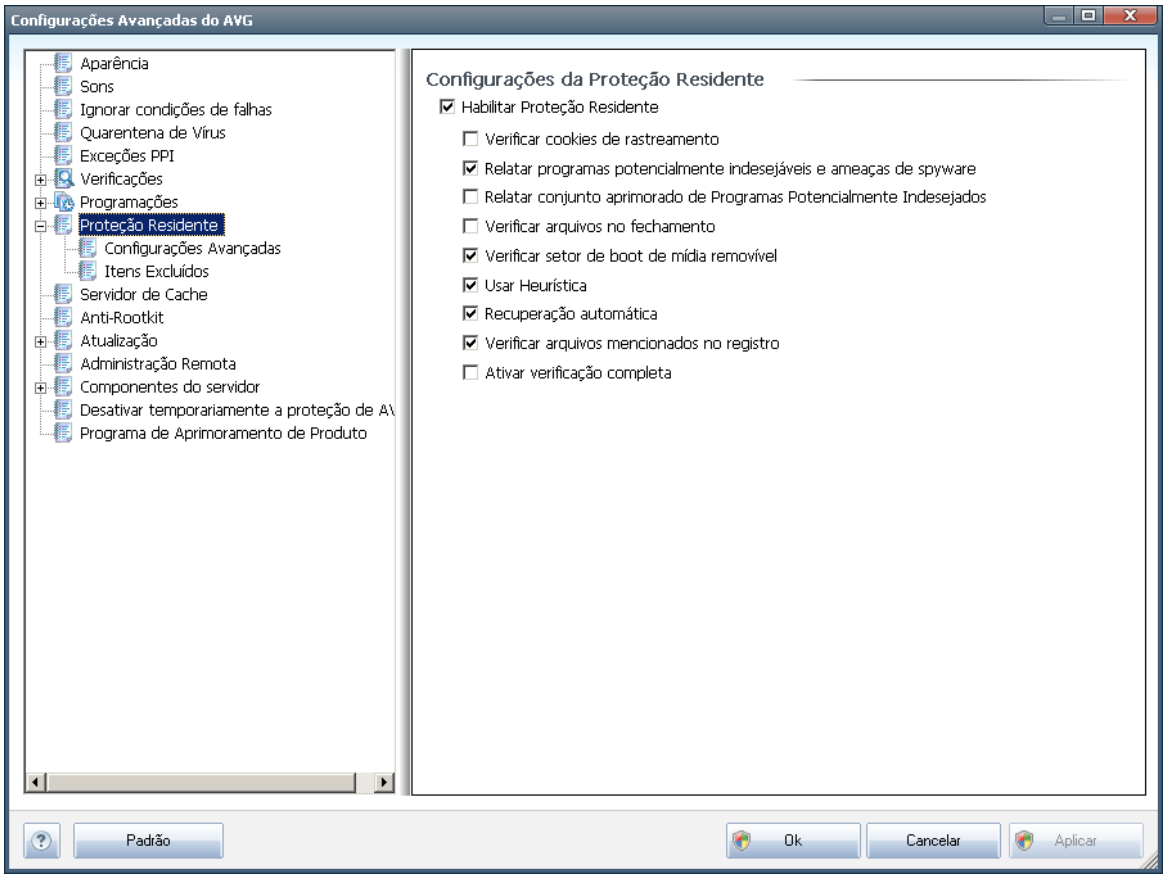
Marque a opção ***Executar novamente a atualização assim que uma conexão com a Internet estiver disponível***, para ter certeza de que, se a conexão com a Internet ficar corrompida e o processo de atualização falhar, ele será imediatamente reiniciado quando a conexão com a Internet for restaurada.

Assim que a atualização programada for iniciada na hora especificada, você será informado por uma janela pop-up aberta sobre o ícone AVG na bandeja do sistema (*caso você tenha mantido a configuração padrão da caixa de diálogo* ***Configurações avançadas/Aparência****)*.

Observação: *se ocorrer uma coincidência de tempo de uma atualização de programa agendada e uma verificação agendada, o processo de atualização terá maior prioridade, e a verificação será interrompida.*

11.8. Proteção Residente

O componente ***Proteção Residente*** realiza a proteção em tempo real contra vírus, spywares e outros malwares em arquivos e pastas.



Na caixa de diálogo ***Configurações da Proteção Residente*** , é possível ativar ou desativar a ***Proteção Residente*** completamente marcando/desmarcando o item ***Ativar Proteção Residente*** (*essa opção é ativada por padrão*). Além disso, você pode selecionar quais recursos da ***Proteção Residente*** devem ser ativados:

- ***Verificar cookies de rastreamento*** (*desativada por padrão*) - esse parâmetro define que os cookies devem ser detectados durante a verificação. (*Cookies HTTP são usados para autenticar, controlar e manter informações específicas sobre usuários, como preferências de site ou o conteúdo de suas compras eletrônicas*)

- ***Informar programas potencialmente indesejáveis e ameaças de spyware –*** marque para ativar o mecanismo ***Anti-Spyware*** ***e verificar spyware, bem como vírus.*** Spyware representa uma categoria de malware questionável: embora ele geralmente represente um risco de segurança, alguns desses programas pode ser instalado intencionalmente. Recomendamos manter esse recurso ativado, pois aumenta a segurança do computador.

- ***Informar conjunto avançado de programas potencialmente indesejáveis*** (*desativada por padrão*) - marque para detectar o pacote estendido de spyware: programas que estão perfeitamente ok e são inofensivos quando adquiridos do fabricante diretamente, mas podem ser mal-utilizados para finalidades mal-intencionadas posteriormente. Esta é uma medida adicional que aumenta ainda mais a segurança de seu computador; no entanto, pode eventualmente bloquear programas legais, e, portanto, é desativada por padrão.

- ***Verificar arquivos no fechamento*** (*desativada por padrão*) - a verificação durante o fechamento garante que o AVG verifique objetos ativos (por exemplo, aplicativos, documentos etc.) quando eles estiverem sendo abertos e também quando estiverem sendo fechados. Esse recurso ajuda a proteger o computador contra alguns tipos de vírus sofisticados

- ***Verificar setor de inicialização de mídia removível*** (*ativada por padrão*)

- ***Usar Heurística*** - (*ativada por padrão*) a análise heurística será usada para detecção (*emulação dinâmica das instruções do objeto verificado em um ambiente de computador virtual*)

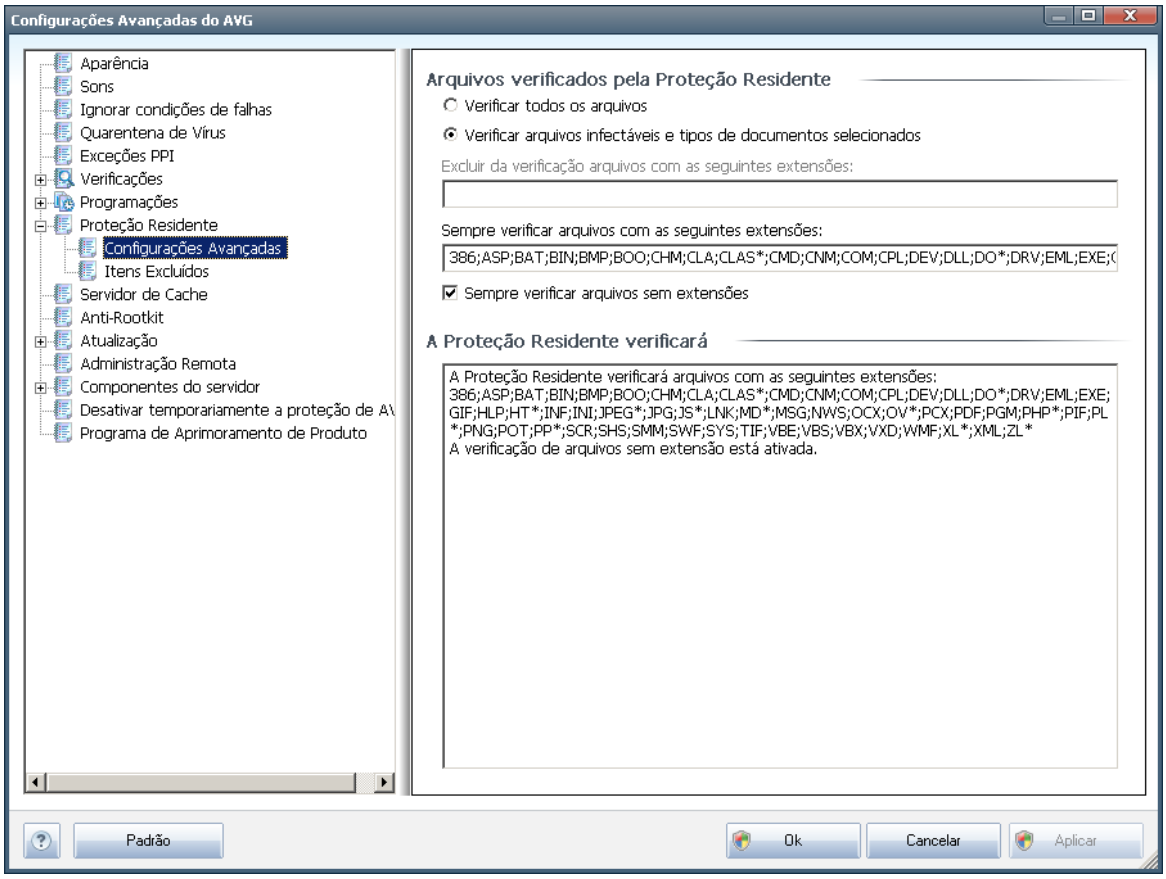
- ***Reparo automático*** (*desativada por padrão*) - todas as infecções detectadas serão reparadas automaticamente, se houver solução disponível, e todas as infecções que não puderem ser solucionadas serão removidas.

- ***Verificar arquivos mencionados no registro*** (*ativada por padrão*) - este parâmetro define que o AVG verificará todos os arquivos executáveis adicionados ao registro de inicialização para evitar que uma infecção conhecida seja executada na próxima inicialização do computador.

- ***Ativar verificação completa*** (*desativada por padrão*) - em situações específicas (*em um estado de extrema emergência*), você pode marcar esta opção para ativar os algoritmos mais completos que verificarão todos os objetos de ameaça possíveis minuciosamente. Entretanto, lembre-se de que esse método consome bastante tempo.

11.8.1. Configurações avançadas

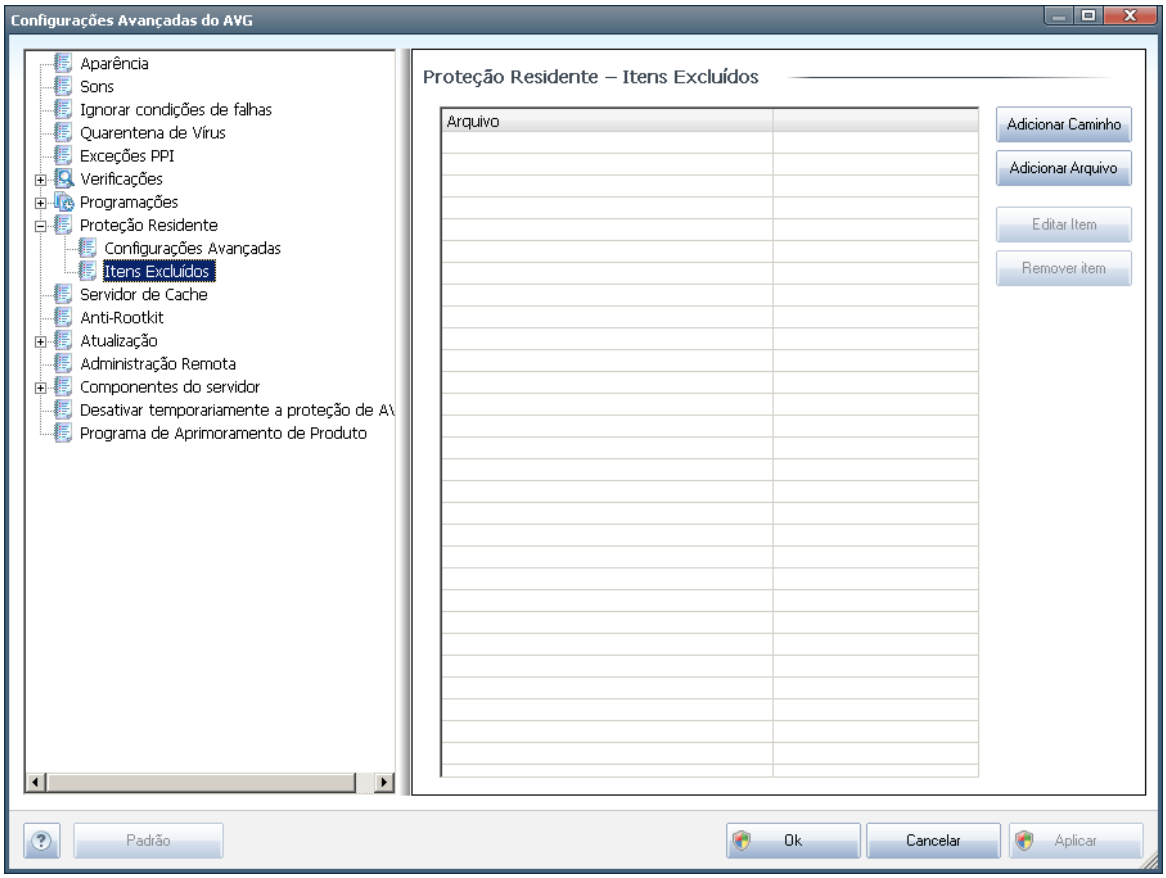
Na caixa de diálogo ***Arquivos verificados pela Proteção Residente***, é possível configurar os arquivos que serão verificados (*por extensão específica*):



Decida se deseja que todos os arquivos sejam verificados ou apenas os infectáveis. Nesse caso, você poderá especificar uma lista de extensões definindo arquivos que devem ser excluídos da verificação, assim como uma lista de extensões de arquivo que definam arquivos que devam ser verificados em todas as circunstâncias.

A seção abaixo denominada ***Proteção Residente vai verificar*** sintetiza as configurações atuais, exibindo uma visão geral detalhada do que a ***Proteção Residente*** irá realmente verificar.

11.8.2. Itens excluídos



A caixa de diálogo ***Proteção Residente - Itens Excluídos*** oferece a possibilidade de definir as pastas e/ou arquivos que devem ser excluídos da verificação da ***Proteção Residente***.

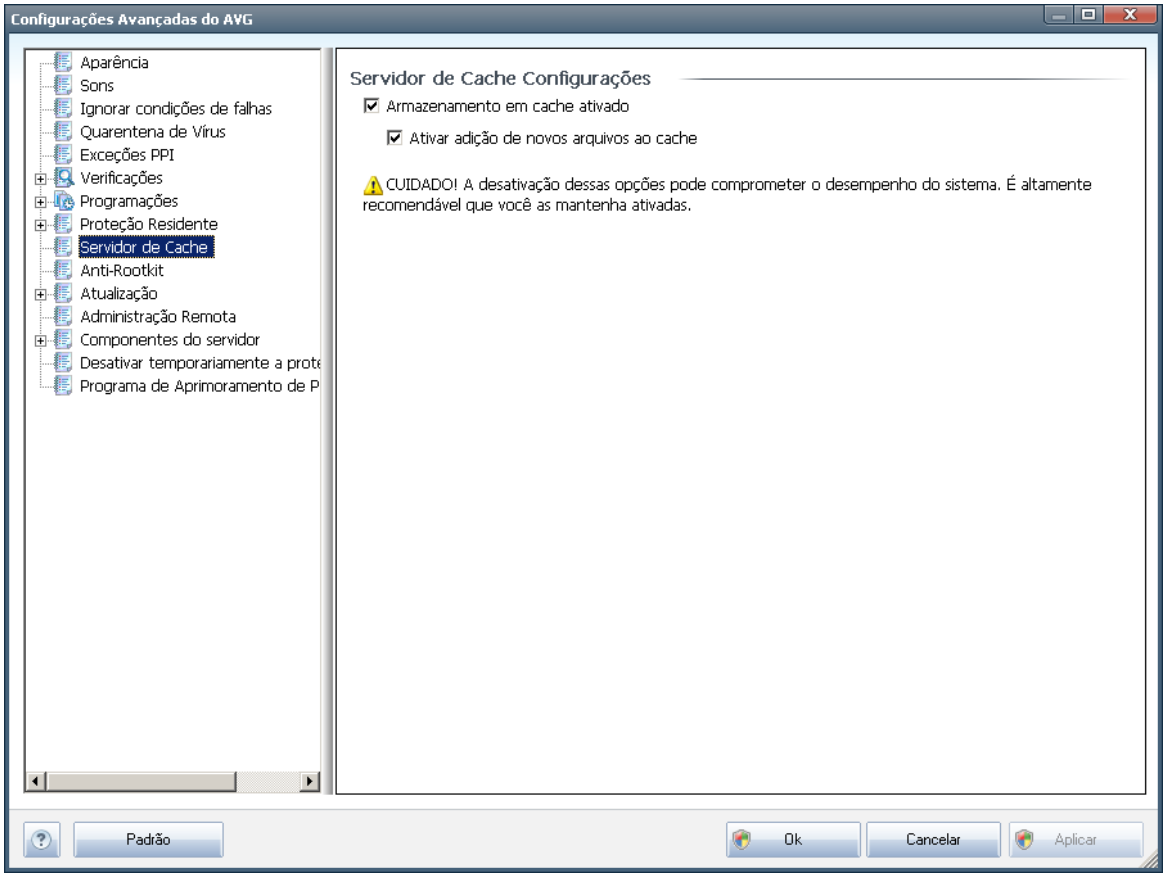
Se isso não for necessário, é altamente recomendável não excluir nenhum item.

Essa caixa de diálogo fornece os seguintes botões de controle:

- ***Adicionar Caminho*** – especifique um diretório (diretórios) a ser excluído da verificação, selecionando-o (um a um, no caso de haver mais de um) na árvore de navegação do disco local
- ***Adicionar Arquivo*** – especifique arquivos a serem excluídos da verificação, selecionando-os um a um na árvore de navegação do disco local
- ***Editar Item*** – permite editar o caminho especificado para um arquivo ou pasta selecionado
- ***Remover Item*** – permite excluir o caminho para um item selecionado da lista

11.9. Servidor de cache

O ***Servidor de cache*** é um processo designado para acelerar qualquer verificação (*verificação sobre demanda, verificação programada total do computador, verificação da Proteção Residente*. Coleta e mantém informações de arquivos confiáveis (*arquivos de sistema com assinatura digital, etc.*): Esses arquivos são ignorados pelo mecanismo de verificação.



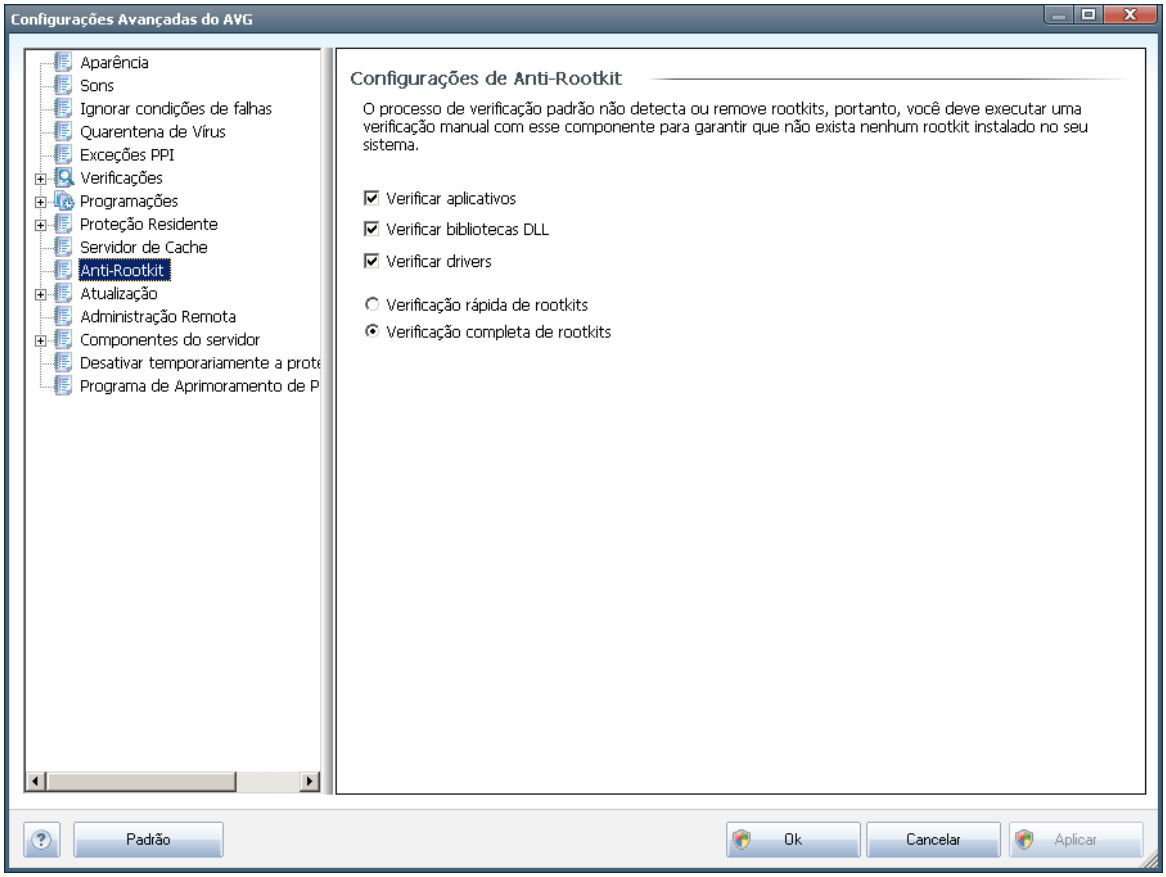
A caixa de diálogo configurações oferece duas opções:

- ***Caching ativado*** (*ativado por padrão*) - desmarque a caixa para desativar o ***Servidor de Cache*** e esvaziar a memória de cache. Observe que a verificação pode desacelerar, e o desempenho global de computador diminuir, conforme é feita a verificação de todos os arquivos únicos em uso procurando primeiro pela existência de vírus e spyware.

- ***Ativar inclusão de novos arquivos em cache*** (*ativado por padrão*) - desmarque a caixa para parar de adicionar mais arquivos na memória cache. Todos os arquivos já armazenados em cache serão mantidos e utilizados até que o cache seja desativado completamente, ou até a próxima atualização do banco de dados de vírus.

11.10. Anti-Rootkit

Nesta caixa de diálogo você pode editar a configuração do componente ***Anti-Rootkit***:



A edição de todas as funções do componente ***Anti-Rootkit***conforme oferecido nesta caixa de diálogo também está acessível diretamente na ***interface do componente Anti-Rootkit***.

Marque as respectivas caixas de seleção para especificar objetos que devem ser verificados:

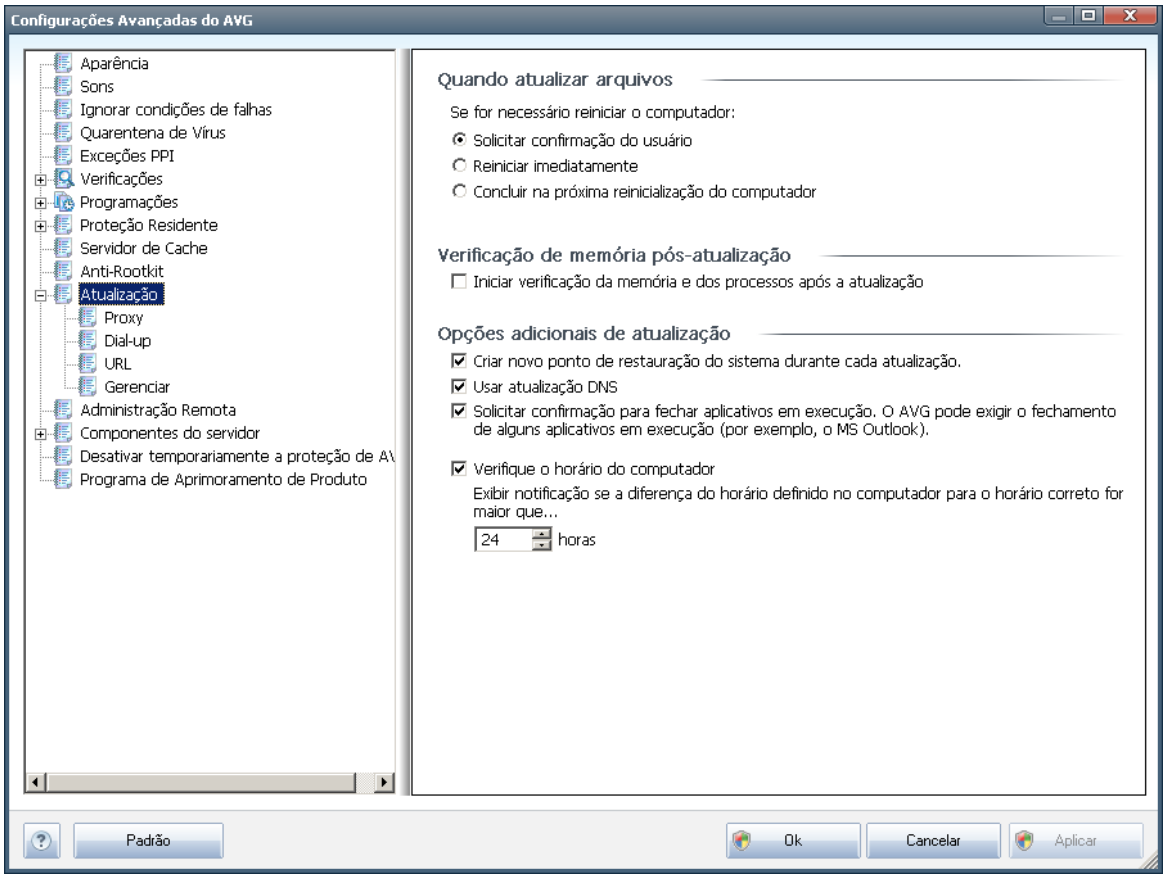
- ***Verificar aplicativos***
- ***Verificar bibliotecas DLL***
- ***Verificar drivers***

Em seguida, você pode selecionar o modo de verificação do rootkit:

- ***Verificação rápida do rootkit*** - verifica todos os processos em execução, unidades carregadas e pasta do sistema (*tipicamente c:\Windows*)
- ***Verificação completa do rootkit*** - verifica todos os processos em execução,

unidades carregadas, a pasta do sistema (*tipicamente c:\Windows*além de todos os discos locais (*incluindo o disco flash, mas excluindo as unidades de CD/disquete*)

11.11. Atualizar



O item de navegação ***Atualizar*** abre uma nova caixa de diálogo na qual é possível especificar parâmetros gerais relativos à atualização do AVG:

Quando atualizar arquivos

Nesta seção você pode selecionar duas alternativas: a atualização pode ser programada para a próxima reinicialização do PC ou você pode iniciar a atualização imediatamente. Por padrão, a opção de atualização imediata é selecionada, pois dessa forma o AVG pode proteger com o nível de segurança máximo. A programação de uma atualização para a próxima reinicialização do PC só pode ser recomendada se você estiver certo de que o computador é reiniciado regularmente, pelo menos diariamente.

Se você decidir manter a configuração padrão e iniciar o processo de atualização imediatamente, poderá especificar as circunstâncias sob as quais uma possível reinicialização necessária será realizada:

- ***Requer confirmação do usuário*** - você será solicitado a aprovar a reinicialização do PC necessária para finalizar o processo de atualização.

- ***Reiniciar imediatamente*** - o computador será reiniciado automaticamente após a conclusão do processo de atualização e sua aprovação não será necessária.

- ***Concluir na próxima reinicialização do computador*** - a finalização do processo de atualização será adiada até a próxima reinicialização do computador. Novamente, tenha em mente que essa opção só é recomendada se você tiver certeza de que o computador será reiniciado regularmente, pelo menos diariamente

Verificação de memória pós-atualização

Marque essa caixa de seleção para definir que deseja iniciar uma nova verificação de memória depois de cada atualização concluída com êxito. A atualização mais atual baixada pode conter novas definições de vírus, e estas devem ser aplicadas à verificação imediatamente.

Opções adicionais de atualização

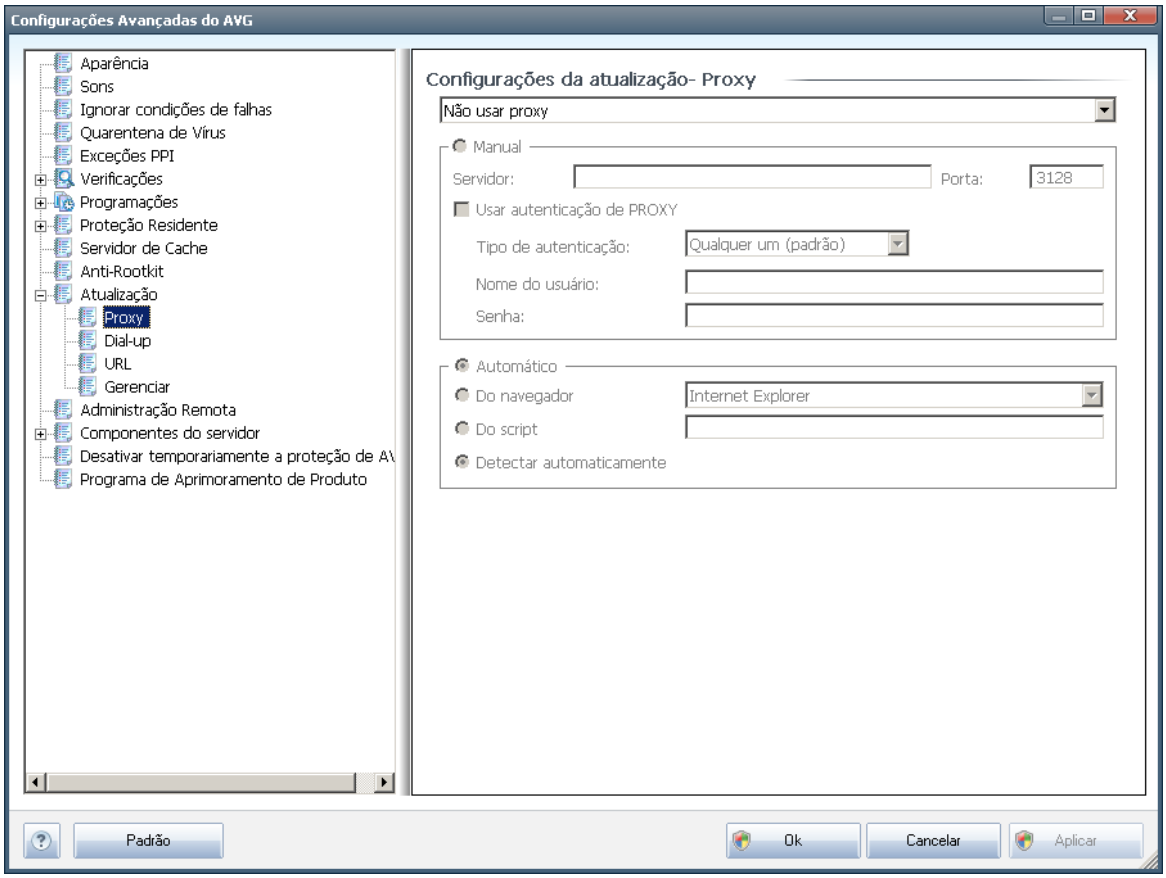
- ***Criar novo ponto de restauração do sistema durante cada atualização do programa*** - antes de cada ativação da atualização do programa AVG, um ponto de restauração do sistema é criado. No caso de falha no processo de atualização e seu sistema operacional, você pode restaurar o seu SO para a configuração original deste ponto. Esta opção está disponível em Iniciar / Todos os Programas / Acessórios / Ferramentas do Sistema / Restauração do Sistema, mas quaisquer alterações podem ser recomendadas apenas para usuários experientes! Mantenha esta caixa de seleção marcada se quiser usar o recurso.

- ***Usar atualização DNS*** - marque esta caixa de seleção para confirmar que você deseja usar o método de detecção de arquivos de atualização que elimina a quantidade de dados transferidos entre o servidor de atualização e o cliente AVG;

- ***Requer confirmação para fechar aplicativos em execução*** (*ativado por padrão*) ajudará você a se certificar de que nenhum aplicativo em execução no momento será fechado sem sua permissão - se necessário para a conclusão do processo de atualização;

- ***Marcar o horário definido do computador*** - marque esta opção para declarar que você deseja que seja exibida uma notificação caso o horário do computador seja diferente do horário correto em um número de horas maior que o especificado.

11.11.1. Proxy



O servidor proxy é um servidor autônomo ou um serviço executado em um PC que garante conexão segura à Internet. De acordo com as regras de rede especificadas, você poderá acessar a Internet diretamente ou por meio do servidor proxy; as duas possibilidades também podem ser permitidas ao mesmo tempo. Em seguida, no primeiro item da caixa de diálogo ***Configurações da Atualização - Proxy*** , você deverá selecionar o menu da caixa de combinação, se desejar:

- ***Usar proxy***
- ***Não usar servidor proxy***- configurações padrão
- ***Tentar conectar usando proxy e, se falhar, conectar diretamente***

Se você selecionar uma opção usando o servidor proxy, terá que especificar alguns outros dados. As configurações do servidor podem ser definidas manualmente ou automaticamente.

Configuração manual

Se você selecionar a configuração manual (selecione a opção *Manual* ***para ativar a***

seção apropriada da caixa de diálogo*)*, terá que especificar os seguintes itens:

- ***Servidor***– especifique o endereço IP do servidor ou o nome do servidor.
- ***Porta*** - especifique o número da porta que permite o acesso à Internet (por padrão, esse número está definido como 3128, mas pode ser definido de forma diferente - *se não tiver certeza, entre em contato com o administrador da rede*).

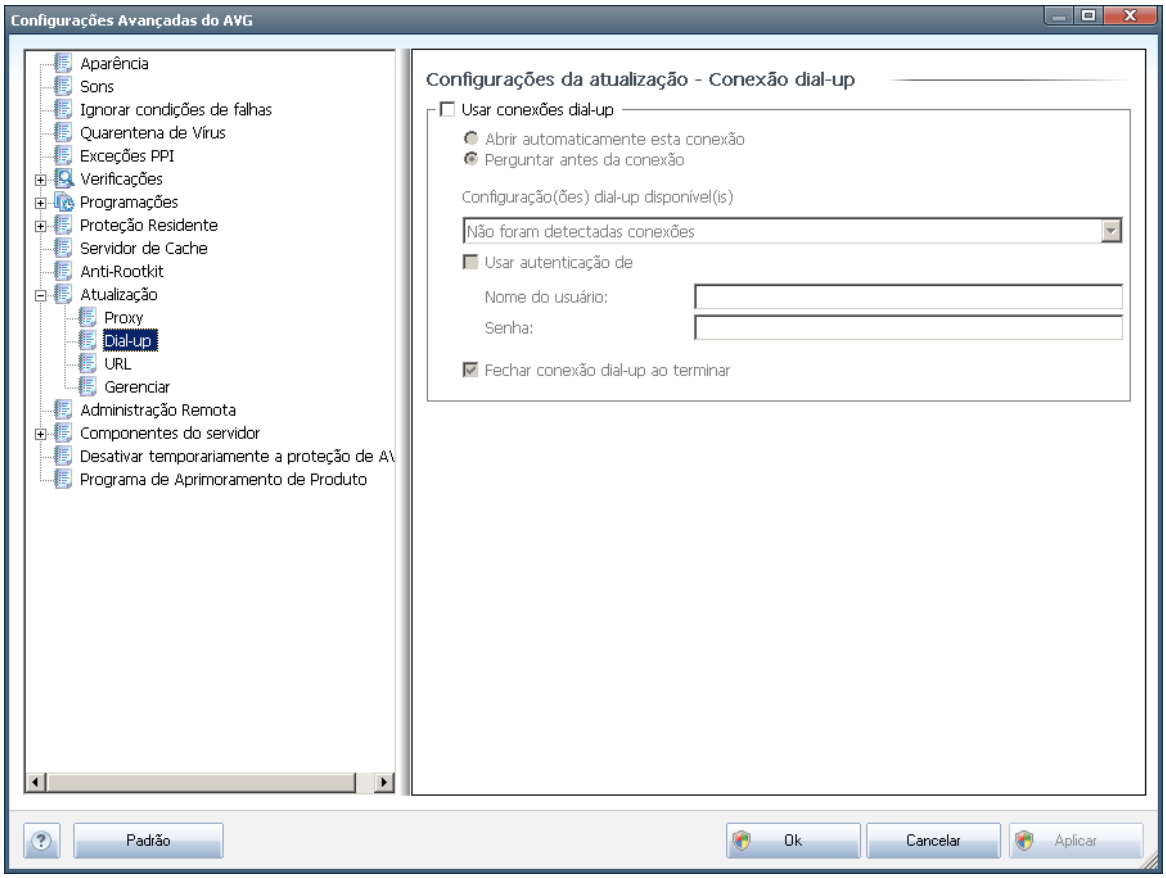
O servidor proxy também pode ter configurado regras especificas para cada usuário. Se o servidor proxy estiver configurado dessa forma, selecione a opção ***Usar autenticação PROXY*** para verificar se o nome de usuário e a senha são válidos para conexão à Internet por meio do servidor proxy.

Configuração automática

Se você selecionar configuração automática (*marque a opção Automática* ***para ativar a seção da caixa de diálogo apropriada****)*, selecione de onde a configuração do proxy deve ser realizada:

- ***A partir do navegador*** - a configuração será lida a partir do navegador da Internet padrão
- ***Do script*** - a configuração será lida de um script de download com a função retornando o endereço proxy
- ***Detecção automática*** - a configuração será detectada de forma automática e direta do servidor proxy

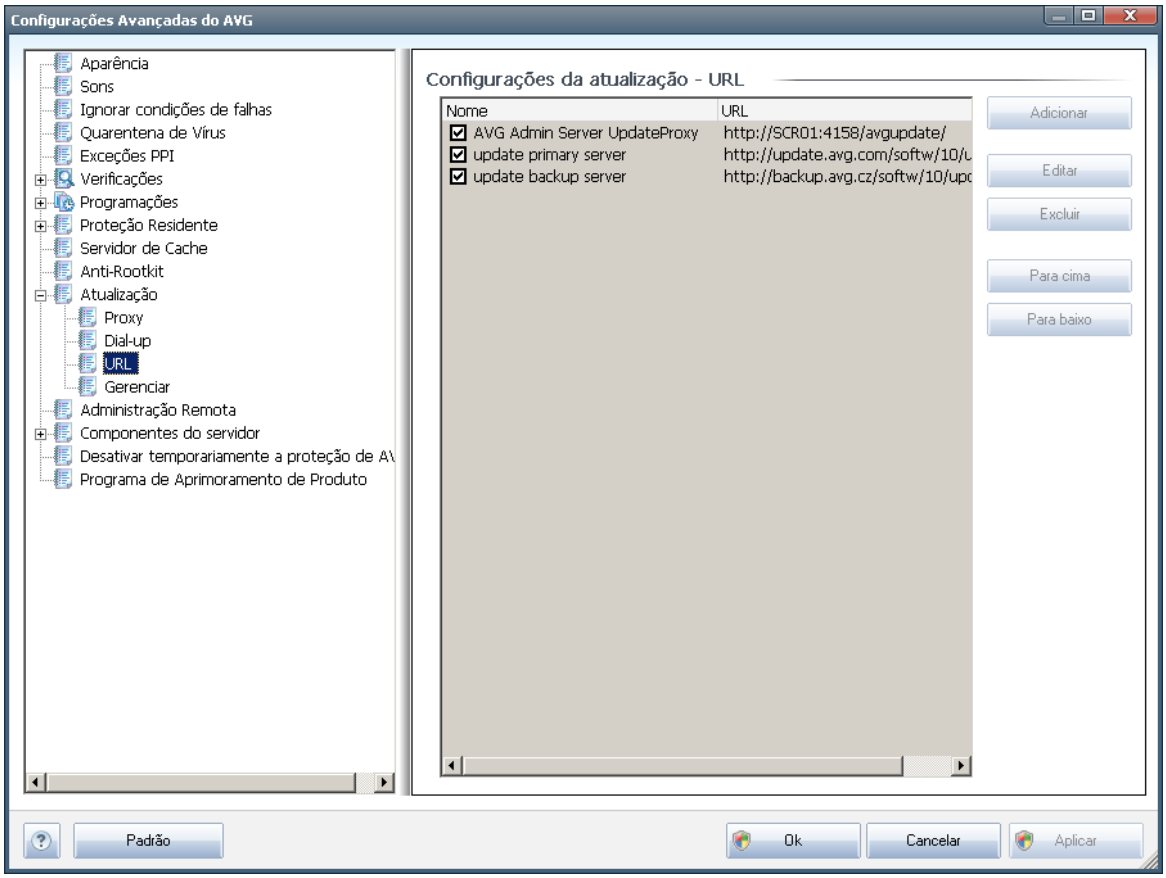
11.11.2. Dial-up



Todos os parâmetros definidos opcionalmente na caixa de diálogo ***Atualizar configurações - Conexão dial-up*** referem-se à conexão discada com a Internet. Os campos da guia estarão inativos até que a opção ***Usar conexões dial-up***, que ativará os campos, esteja marcada.

Especifique se você deseja se conectar à Internet automaticamente (***Abrir esta conexão automaticamente***) ou se deseja confirmar a conexão manualmente, todas as vezes (***Perguntar antes da conexão***). Para conexão automática, você poderá decidir se a conexão deve ser fechada após o término da atualização (***Fechar conexão dial-up ao terminar***).

11.11.3. URL

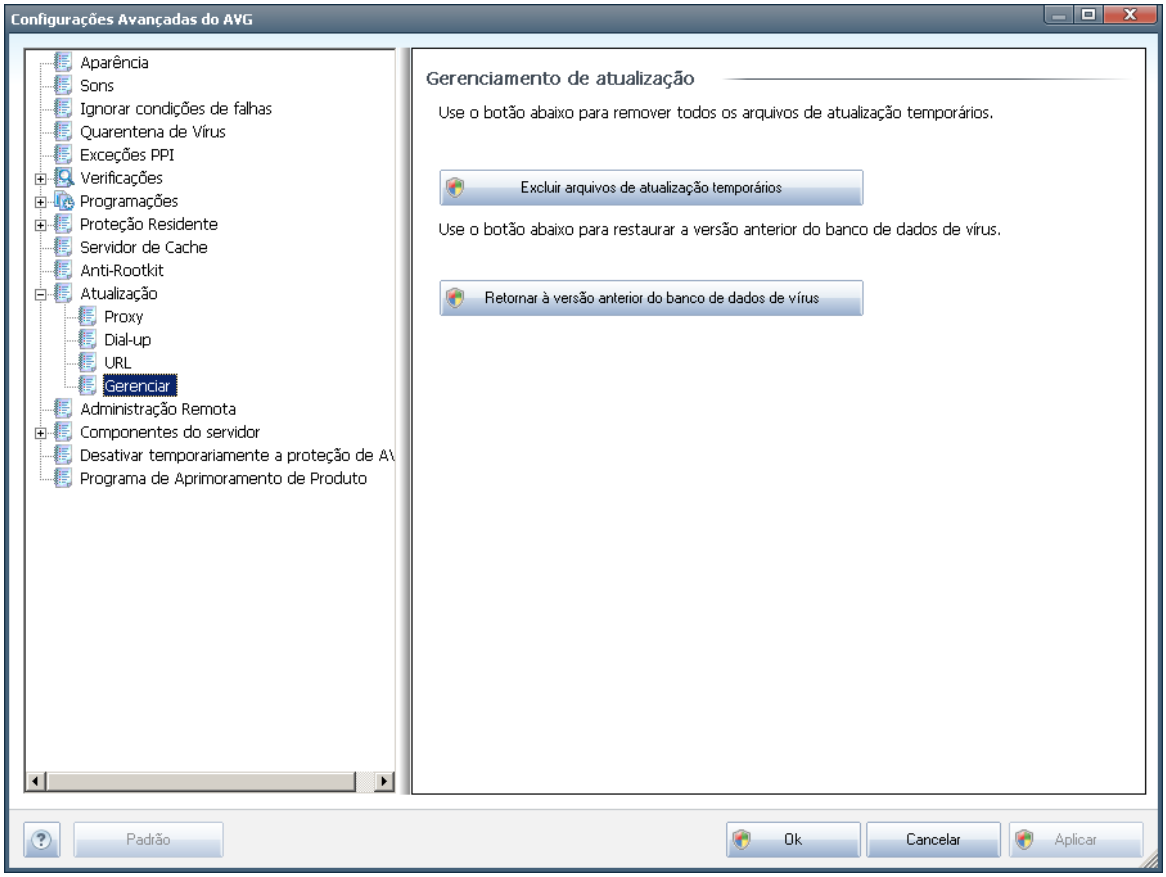


A caixa de diálogo ***URL*** oferece uma lista de endereços da Internet, a partir da qual você poderá baixar os arquivos de atualização. A lista e os itens podem ser modificados por meio dos seguintes botões de controle:

- ***Adicionar***- abre uma caixa de diálogo na qual você especificará a nova URL a ser adicionada à lista
- ***Editar*** – abre uma caixa de diálogo na qual você poderá editar os parâmetros da URL selecionada
- ***Excluir*** - exclui a URL selecionada da lista
- ***Mover para Cima*** -move a URL selecionada uma posição acima na lista
- ***Mover para Baixo*** – move a URL selecionada uma posição abaixo na lista.

11.11.4. Gerenciar

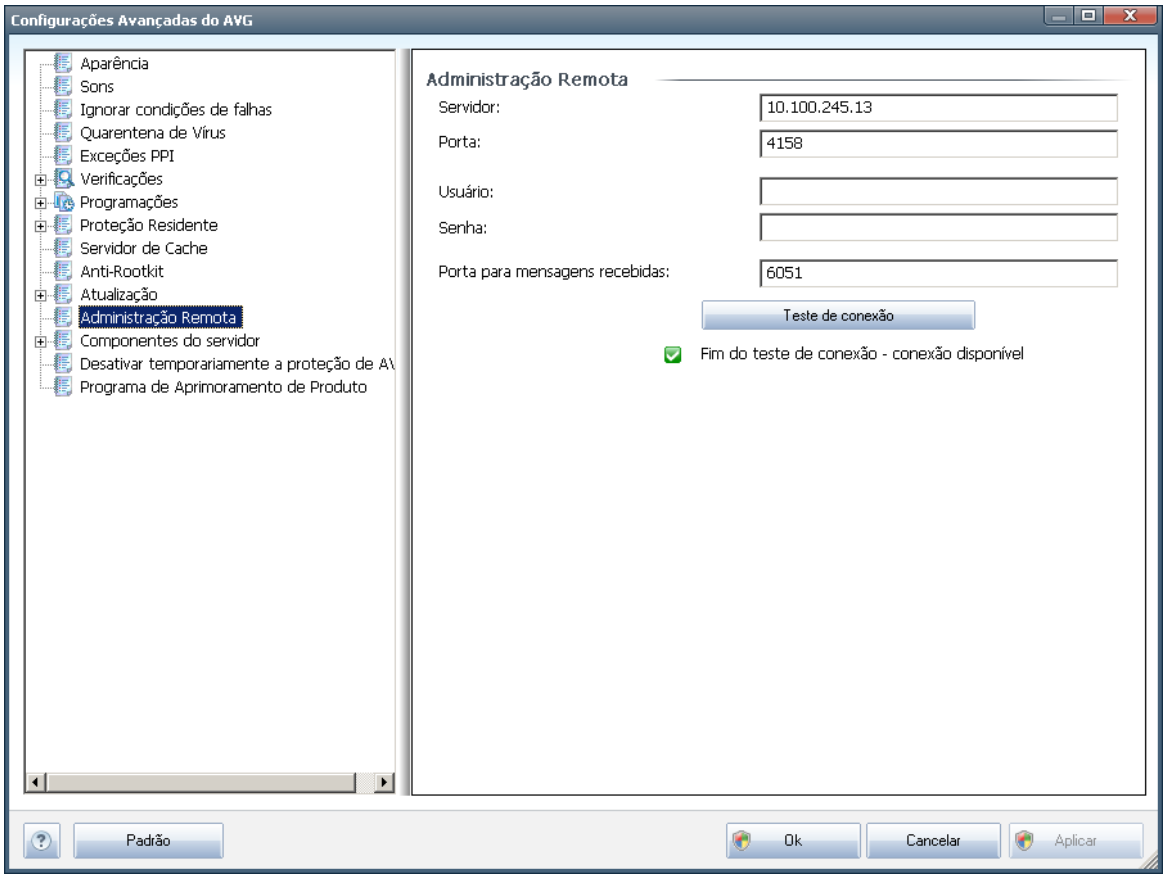
A caixa de diálogo ***Gerenciar*** oferece duas opções acessíveis via dois botões:



- ***Excluir arquivos de atualização temporários*** - pressione este botão para excluir todos os arquivos de atualização redundantes do seu disco rígido (*por padrão, eles são armazenados por 30 dias*)

- ***Retornar banco de dados de vírus para a versão anterior*** –pressione este botão para excluir a versão mais recente da base de vírus do seu disco rígido e retornar à versão salva anteriormente (*a nova versão da base de vírus fará parte da próxima atualização*)

11.12. Administração Remota



A configuração ***Administração Remota*** se refere à conexão da estação do cliente AVG ao sistema de administração remota. Se você planeja conectar a estação apropriada à administração remota, especifique os seguintes parâmetros:

- ***Servidor*** - nome do servidor (ou endereço IP do servidor) em que o AVG Admin Server está instalado
- ***Porta*** - fornece o número da porta em que o cliente do AVG se comunica com o AVG Admin Server (*o número da porta 4158 é considerado padrão. Se você usá-lo, não terá que especificá-lo explicitamente*)
- ***Login*** - se a comunicação entre o cliente AVG e o AVG Admin Server for definida como segura, forneça o nome de usuário ...
- ***Senha*** - ... e a senha
- ***Porta para mensagens recebidas*** - número da porta em que o cliente AVG aceita mensagens recebidas do AVG Admin Server

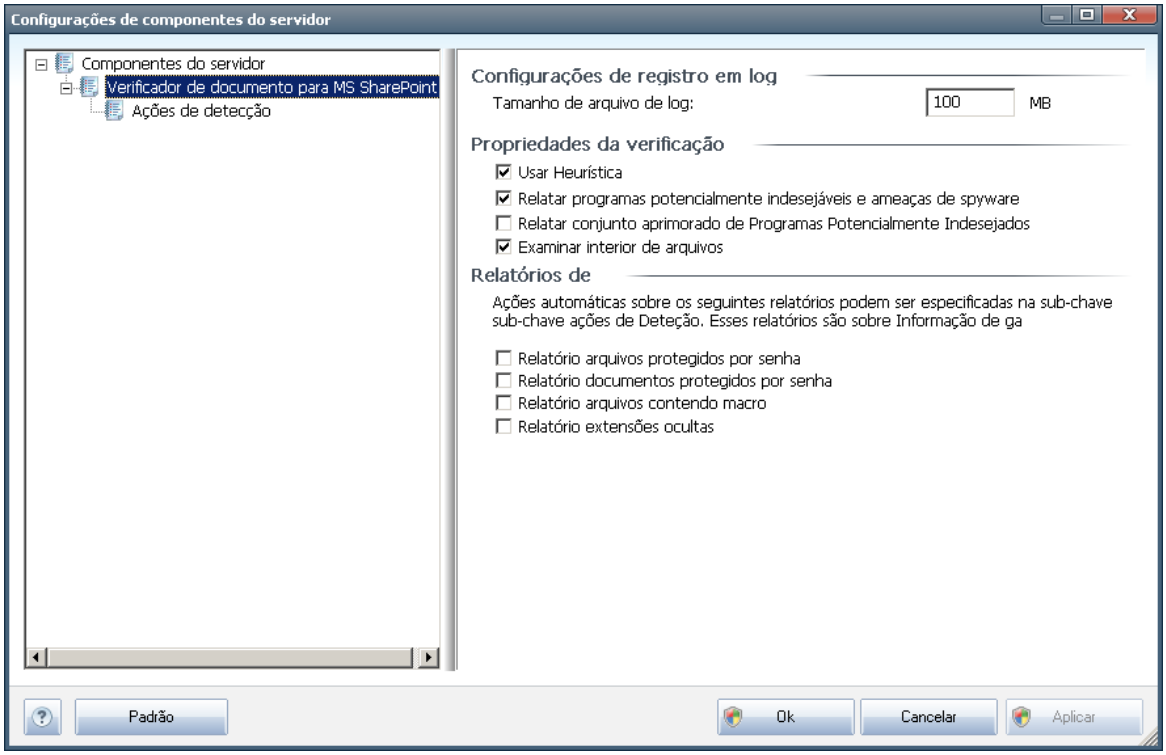
O botão ***Testar conexão*** ajuda a verificar se todos os dados mencionados acima são válidos e podem ser usados para uma conexão bem-sucedida com o DataCenter.

Observação: *para obter uma descrição detalhada sobre a administração remota, consulte a documentação do AVG Business Edition.*

11.13. Componentes do servidor

11.13.1. Verificador de documento para MS SharePoint

Nesta caixa de diálogo, você vai encontrar várias opções predefinidas relacionadas com o desempenho de verificação de vírus em documentos do***Verificador de Documentos para MS SharePoint*** Esta caixa de diálogo divide-se em várias seções:



Configurações de registro em log

Tamanho do arquivo de log – o arquivo de log contém registro de vários eventos relacionados ao ***Verificador de Documentos para MS SharePoint***, como observações sobre carregamento de bibliotecas de programas, eventos de vírus encontrados, avisos de solução de problemas, etc. Use o texto apresentado para definir o tamanho máximo do arquivo.

Propriedades da verificação

- ***Usar análise heurística*** – marque para usar o método de detecção de análise heurística ao verificar documentos. Quando essa opção está ativada, você

pode filtrar documentos não apenas por extensão, mas também o conteúdo real deste será considerado.

- ***Reportar programas potencialmente indesejáveis e ameaças de spyware*** – marque para usar o mecanismo Anti-Spyware, ou seja, detectar e relatar programas suspeitos e potencialmente indesejáveis ao verificar documentos.

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

- ***Verificar dentro de arquivos*** – marque para verificar os conteúdos de arquivos.

Relatórios

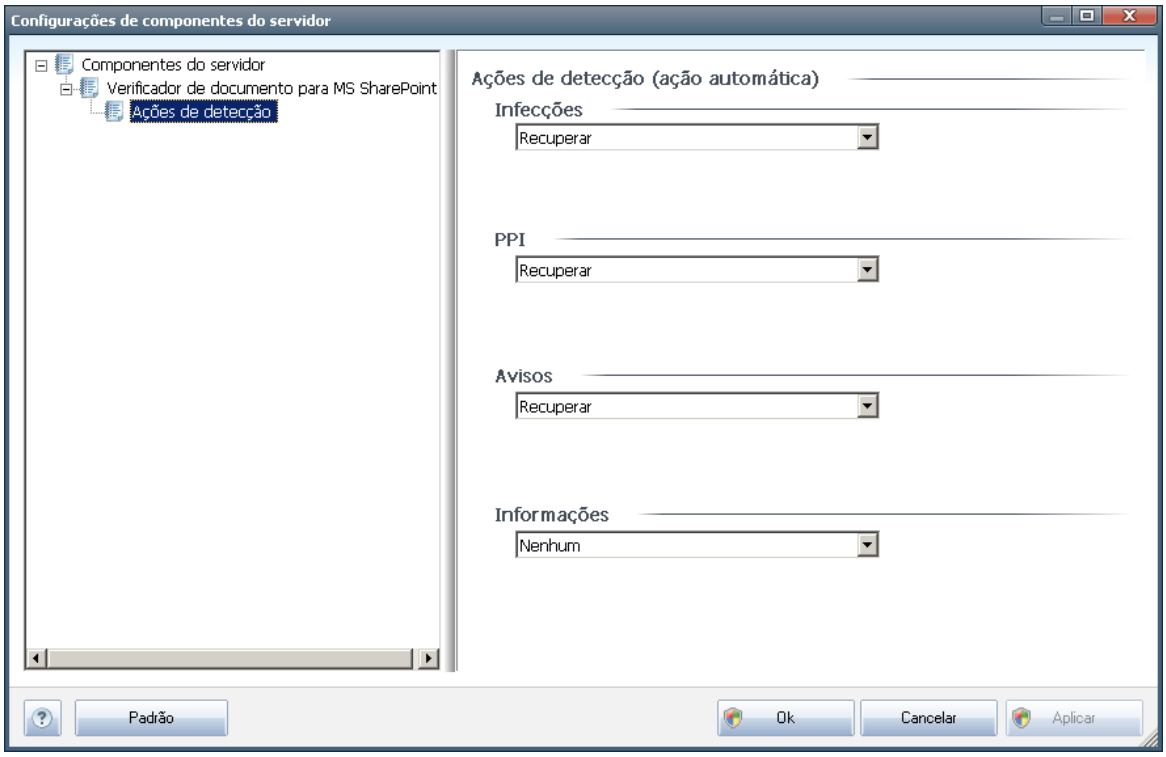
- ***Reportar arquivos protegidos por senha –*** arquivos (ZIP, RAR, etc.) protegidos por senha não podem ser verificados em busca de vírus. Marque a caixa de seleção para reportá-los como potencialmente perigosos.

- ***Reportar documentos protegidos por senha*** – documentos protegidos por senha não podem ser verificados em busca de vírus. Marque a caixa de seleção para reportá-los como potencialmente perigosos.

- ***Reportar arquivos contendo macros*** – uma macro é uma sequência predefinida de etapas com o objetivo de executar certas tarefas mais fáceis para um usuário (as macros do MS Word são amplamente conhecidas). Dessa forma, uma macro pode conter instruções potencialmente perigosas e convém você marcar a caixa de seleção para garantir que os arquivos com macros sejam reportados como suspeitos.

- ***Reportar extensões ocultas –*** extensões ocultas podem fazer um arquivo executável suspeito, "alguma coisa.txt.exe", por exemplo, parecer-se com um arquivo de texto comum inofensivo "alguma coisa.txt". Marque a caixa de seleção para reportá-los como potencialmente perigosos.

11.13.2. Ações de detecção



Nesta caixa de diálogo você pode configurar como o componente ***Verificador de Documentos para MS SharePoint*** deve se comportar, quando detectar uma ameaça. As ameaças são divididas em várias categorias:

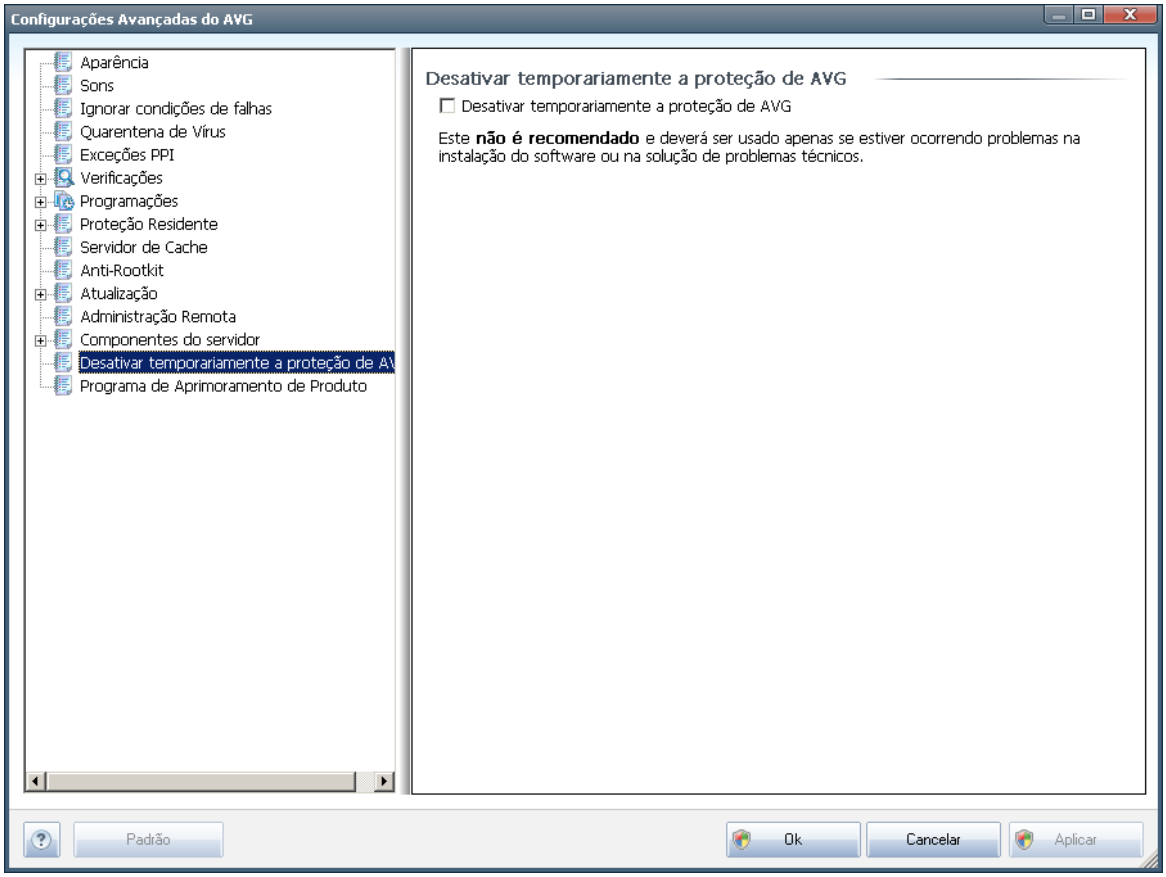
- ***Infecções*** – códigos maliciosos que copiam e espalham-se, passando muitas vezes despercebidos até que o estrago esteja feito.
- ***PPI Programas Potencialmente Indesejáveis)*** – em geral, esses programas variam de ameaças realmente sérias a apenas em potencial à sua privacidade.
- ***Avisos*** – objetos detectados que não podem ser verificados.
- ***Informações*** – inclui todas as possíveis ameaças detectadas que não possam ser classificadas em nenhuma das categorias acima.

Use os menus suspensos para selecionar uma ação automática para cada uma delas:

- ***Nenhuma*** – um documento contendo tal ameaça será ignorado.
- ***Recuperar*** - tenta recuperar o documento/arquivo infectado.
- ***Mover para Quarentena****** – cada documento infectado será movido para o ambiente de Quarentena de vírus.

- ***Remover*** – um documento onde um vírus foi detectado será excluído.

11.14. Desativar temporariamente a proteção do AVG



Na caixa de diálogo ***Desativar temporariamente a proteção do AVG***, você tem a opção de desativar toda a proteção oferecida pelo **AVG Email Server Edition 2011** de uma vez.

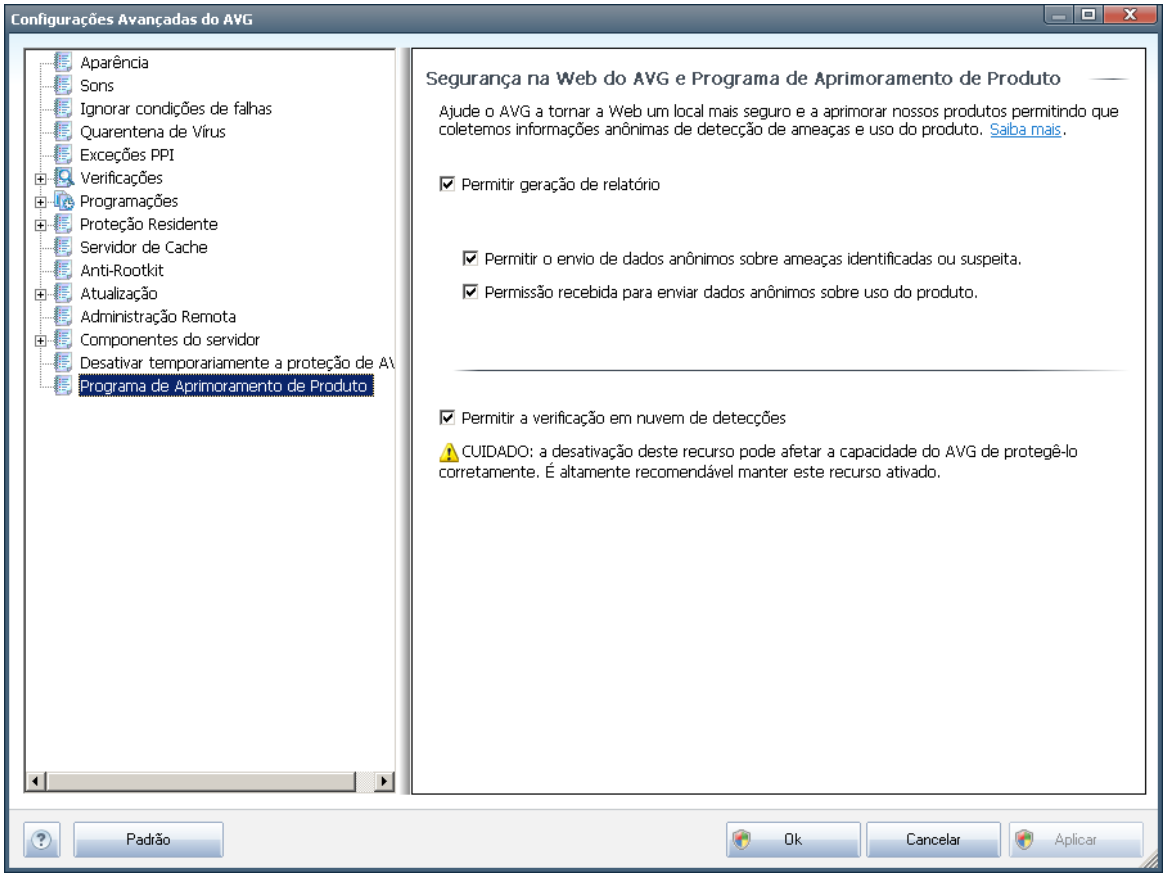
Lembre-se de que você não deve usar essa opção, a menos que ela seja absolutamente necessária!

Na maioria dos casos, não ***é necessário*** desativar o AVG antes de instalar novo software ou novos drivers, nem mesmo se o instalador ou assistente de software sugerir que programas e aplicativos em execução devem ser encerrados primeiro para garantir que não haja interrupções indesejadas durante o processo de instalação. Caso você tenha algum problema durante a instalação, tente desativar o componente ***Proteção Residente*** primeiro. Se precisar desativar temporariamente o AVG, você deverá reativá-lo assim que concluir a sua tarefa que solicitou a desativação. Se você estiver conectado à Internet ou a uma rede durante o período em que o software antivírus está desativado, o computador ficará vulnerável a ataques.

11.15. Programa de Aprimoramento de Produto

A caixa de diálogo ***Segurança na Web e Programa de Aprimoramento de Produto*** convida você a participar do aperfeiçoamento de produto AVG e nos ajudar a aumentar o nível de segurança geral na Internet. Marque a opção ***Permitir relatórios*** a fim de permitir a geração de relatórios de ameaças detectadas para o AVG. Isso nos ajuda a coletar informações atualizadas sobre as ameaças mais recentes dos participantes do mundo todo e, em retorno, podemos melhorar a proteção para todos.

O relatório é feito automaticamente, portanto, não causa nenhum inconveniente a você e nenhum dado pessoal é incluído nos relatórios. É opcional registrar ameaças detectadas; no entanto, solicitamos que ative esse recurso porque ele nos ajuda a melhorar a proteção de navegação online tanto para você quanto outros usuários do AVG.



Hoje em dia, existem muito mais ameaças do que apenas vírus comuns. Os criadores de códigos maliciosos e sites perigosos são muito inovadores, e novos tipos de ameaças surgem frequentemente, a vasta maioria na Internet. Estas são algumas das mais comuns:

- ***Um vírus é um código mal-intencionado que se copia e se espalha, muitas vezes não percebido até que o estrago seja feito.*** Alguns vírus são uma ameaça séria, excluindo ou alterando deliberadamente arquivos no seu

caminho, enquanto alguns vírus podem fazer algo aparentemente inofensivo, como reproduzir o trecho de uma música. No entanto, todos os vírus são perigosos devido à capacidade básica de se multiplicarem – mesmo um vírus simples pode ocupar toda a memória do computador em um instante e causar uma falha.

- ***Uma subcategoria de vírus é um worm*** que, diferentemente do vírus, não precisa de um objeto "transportador" ao qual se anexar; ele se envia a outros computadores dentro de si mesmo, normalmente por e-mail e, como resultado, muitas vezes sobrecarrega servidores de e-mail e sistemas de rede.

- ***O spyware normalmente é definido como uma categoria de malware (malware = qualquer software mal intencionado, incluindo vírus) que abrange programas – tipicamente Cavalos de Tróia – com o objetivo de roubar informações pessoais, senhas, números de cartão de crédito ou para se infiltrar em um computador e permitir que o atacante controle-o remotamente; é claro que tudo isso sem o conhecimento ou consentimento do dono do computador.***

- ***Programas potencialmente indesejados*** são um tipo de spyware que pode ser, mas não necessariamente precisa ser, perigoso ao computador. Um exemplo específico de um PPI é o adware, software projetado para distribuir propaganda, normalmente exibindo pop-ups de anúncio; é irritante, mas não diretamente prejudicial.

- Oσ***cookies de rastreamento*** podem também ser contados como um tipo de spyware, uma vez que esses pequenos arquivos, armazenados no navegador da Web e enviados automaticamente ao site "pai" quando você visitá-lo novamente, podem conter dados como seu histórico de navegação e outras informações similares.

- ***Vulnerabilidade*** é um código mal intencionado que se aproveita de uma falha ou vulnerabilidade em um sistema operacional, navegador da Internet ou outro programa essencial.

- ***Phishing*** é uma tentativa de adquirir dados pessoais confidenciais simulando uma organização confiável e bem conhecida. Normalmente, as possíveis vítimas são contatadas por um e-mail em massa solicitando que elas, por exemplo, atualizem os detalhes da sua conta bancária. Para fazer isso, elas são convidadas a seguir o link fornecido que leva a um site falso do banco.

- ***Hoax é um e-mail em massa contendo informações perigosas, alarmantes ou apenas irritantes e inúteis.*** Muitas das ameaças acima usam o e-mail hoax para se espalharem.

- ***Sites mal-intencionados*** são aqueles que deliberadamente instalam software mal-intencionado no seu computador, e sites invadidos fazem o mesmo, a única diferença é que esses sites são legítimos, foram invadidos e infectam os visitantes.

Para protegê-lo de todos esses tipos diferentes de ameaças, o AVG inclui estes

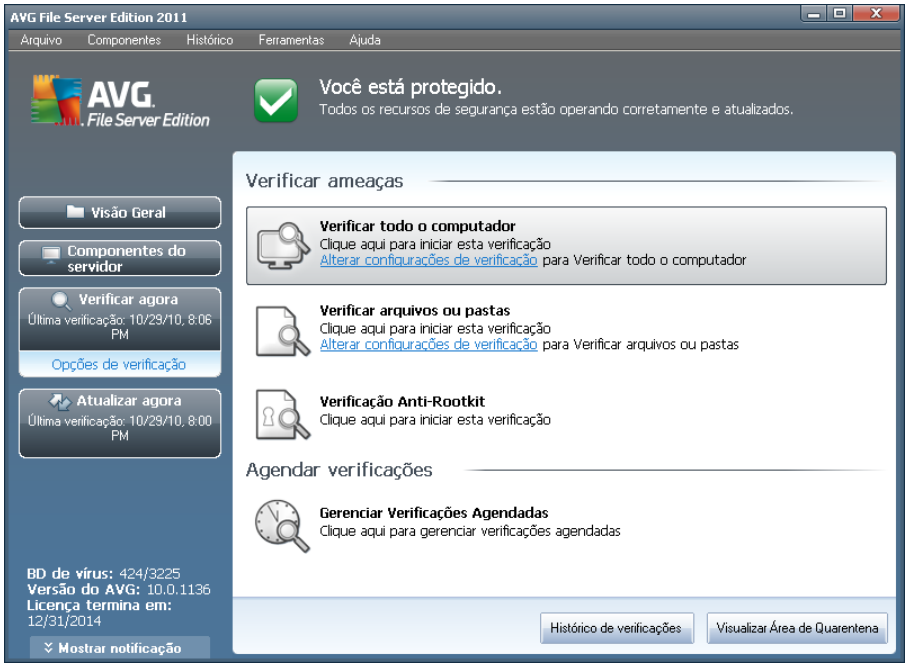
componentes especializados:

- ***Anti-Vírus*** para proteger seu computador de vírus,
- ***Anti-Spyware*** para proteger seu computador de spyware.

12. Verificação do AVG

A verificação é uma parte crucial da funcionalidade **AVG Email Server Edition 2011**. Você pode executar testes sob demanda ou programá-los para serem executados periodicamente , em momentos de sua conveniência.

12.1. Interface da verificação



A interface de verificação do AVG pode ser acessada pelo link rápido ***Verificador do computador***. Clique nesse link para passar para a caixa de diálogo ***Verificar ameaças*** . Nessa caixa de diálogo, você encontrará o seguinte:

- visão geral das verificações predefinidas - três tipos de verificação definidos pelo fornecedor do software estão prontos para uso imediato sob demanda ou de forma programada:
  - ***Verificação de todo o computador***
  - ***Verificar arquivos ou pastas específicas***
  - ***Verificação Anti-Rootkit***
- seção programação da verificação - onde é possível definir novos testes e criar novas programações, conforme necessário.

Botões de controle

Os botões de controle disponíveis na interface de teste são:

- ***Histórico da verificação*** - exibe a caixa de diálogo ***Visão geral dos resultados da verificação*** com todo o histórico da verificação

- ***Exibir Quarentena*** - abre uma nova janela com a ***Quarentena*** - um espaço em que as infecções detectadas são colocadas em quarentena

12.2. Verificações predefinidas

Um dos principais recursos do **AVG Email Server Edition 2011** é a verificação sob demanda. Testes sob demanda são desenvolvidos para verificar várias partes do seu computador, sempre que surgir a suspeita de uma possível infecção por vírus. De qualquer forma, é altamente recomendável realizar esses testes regularmente, ainda que você ache que nenhum vírus possa ser encontrado em seu computador.

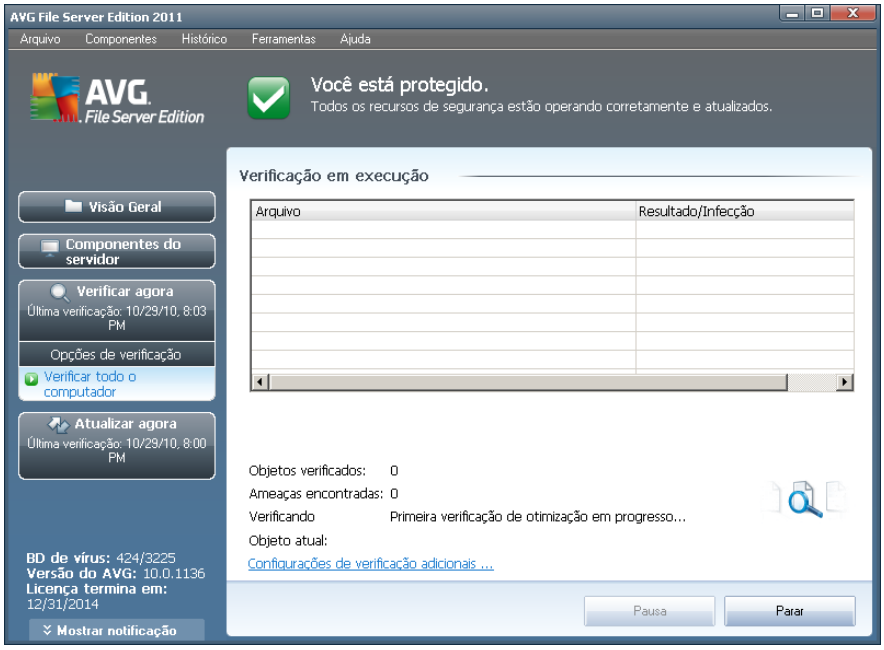
No **AVG Email Server Edition 2011** você encontrará os seguintes tipos de verificação predefinidos pelo fornecedor do software:

12.2.1. Verificação de todo o computador

Verificar todo o computador - verifica todo o computador em busca de infecções e/ou programas potencialmente indesejáveis. Esse teste verificará todos os discos rígidos do computador, detectará e reparará qualquer vírus encontrado ou removerá a infecção para a ***Quarentena de vírus***. A verificação de todo o computador deve ser programada em uma estação de trabalho pelo menos uma vez por semana.

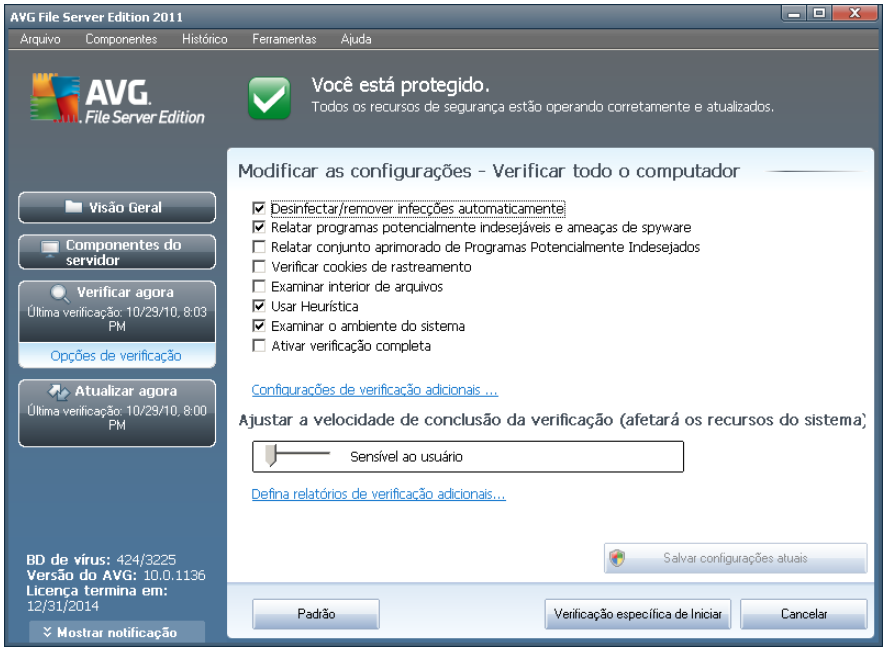
Iniciar verificação

Verificar todo o computador pode ser iniciado diretamente na interface de verificação, clicando no ícone de verificação. Se nenhuma outra configuração específica for configurada para esse tipo de verificação, ela será iniciada imediatamente dentro da caixa de diálogo de ***Verificação em andamento*** *(veja a imagem*). A verificação pode ser interrompida temporariamente (***Pausar***) ou cancelada (***Parar***) se necessário.



Verificar edições de configuração

Você tem a opção de editar as configurações padrão predefinidas de ***Verificar todo o computador***. Clique no link ***Alterar as configurações de verificação*** para acessar a caixa de diálogo ***Alterar configurações de verificação de Verificar todo o computador*** *(acessível pela interface de verificação por meio do link Alterar as configurações de verificação para Verificar todo o computador)*. ***É recomendável manter as configurações padrão, a menos que você tenha um motivo válido para alterá-las.***



- ***Parâmetros de verificação*** - na lista de parâmetros de verificação, você pode ativar ou desativar parâmetros específicos conforme suas necessidades:

  - ***Reparar ou remover infecção automaticamente*** (*ativada por padrão*) - se um vírus for identificado durante a verificação, ele pode ser reparado automaticamente, se houver solução disponível. Se o arquivo infectado não puder ser reparado automaticamente, o objeto infectado será movido para a ***Quarentena de Vírus***.

  - ***Informar programas potencialmente indesejáveis e ameaças de spyware*** (*ativada por padrão*) - marque para ativar o mecanismo ***Anti-Spyware*** e verificar se há spyware e vírus. Spyware representa uma categoria de malware questionável: embora ele geralmente represente um risco de segurança, alguns desses programas pode ser instalado intencionalmente. Recomendamos manter esse recurso ativado, pois aumenta a segurança do computador.

  - ***Informar conjunto avançado de programas potencialmente indesejáveis*** (*desativada por padrão*) - marque para detectar o pacote estendido de spyware: programas que estão perfeitamente ok e são inofensivos quando adquiridos do fabricante diretamente, mas podem ser mal-utilizados para finalidades mal-intencionadas posteriormente. Esta é uma medida adicional que aumenta ainda mais a segurança de seu computador; no entanto, pode eventualmente bloquear programas legais, e, portanto, é desativada por padrão.

  - ***Verificar cookies de rastreamento*** (*desativada por padrão*) - este parâmetro do componente ***Anti-Spyware*** define que os cookies devem ser detectados; (*cookies HTTP são usados para autenticar, controlar e manter informações específicas sobre usuários, como preferências de*

sites ou conteúdo de carrinhos de compras eletrônicas).

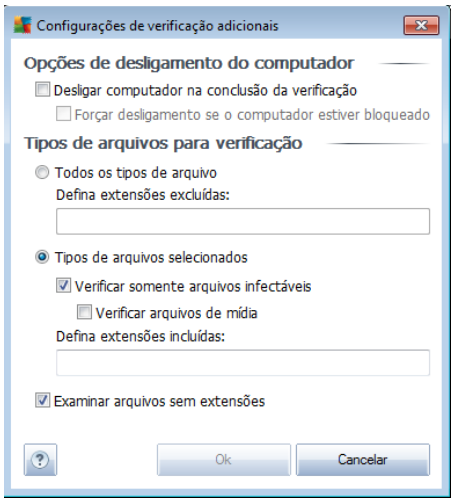
- **_Verificar dentro dos arquivos_** (*desativada por padrão*) - esse parâmetro define que a verificação deve ocorrer em todos os arquivos armazenados dentro de arquivos, como ZIP, RAR etc.

- **_Usar Heurística_** (*ativada por padrão*) - a análise heurística (*emulação dinâmica das instruções do objeto verificado, em um ambiente de computador virtual*) será um dos métodos usados para detecção de vírus durante a verificação

- **_Verificar ambiente do sistema_** (*ativada por padrão*) - a verificação também atuará nas áreas do sistema do seu computador.

- **_Ativar verificação completa_** (*desativada por padrão*) - em situações específicas (*suspeita de que seu computador foi infectado*), é possível marcar esta opção para ativar a maioria dos algoritmos de verificação completos que verificarão até mesmo as áreas do computador que dificilmente são infectadas, só para ter a absoluta certeza. Entretanto, lembre-se de que esse método consome bastante tempo.

- **_Configurações de verificação adicionais_** - o link abre uma nova caixa de diálogo **_Configurações de verificação adicionais_**, na qual é possível especificar os seguintes parâmetros:



- **_Opções de desligamento do computador_** - decida se o computador deve ser desligado automaticamente quando a execução do processo de verificação terminar. Ao confirmar essa opção (**_Desligar o computador quando o processo de verificação for concluído_**), uma nova opção permitirá que o computador seja desligado mesmo que ele esteja bloqueado (**_Forçar desligamento do computador se estiver bloqueado_**).

- **_Definir tipos de arquivo para verificação_** - além disso, você deve decidir se deseja verificar os seguintes itens:

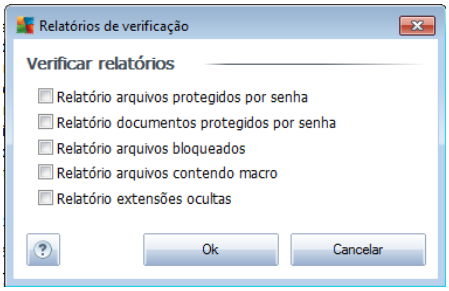
- ***Todos os tipos de arquivos*** com a possibilidade de definirem exceções a partir da verificação, fornecendo uma lista de extensões de arquivo separadas por vírgula que não devem ser verificadas;

- ***Tipos de arquivos selecionados*** - você pode especificar que deseja verificar apenas os arquivos possivelmente infectáveis (*arquivos que não podem ser infectados não serão verificados; por exemplo, alguns arquivos de texto simples ou outros arquivos não executáveis*), incluindo arquivos de mídia (*arquivos de áudio e vídeo - se você deixar essa caixa desmarcada, o tempo de verificação será ainda menor, pois esses arquivos costumam ser grandes, e é muito improvável que eles sejam infectados por vírus*). Mais uma vez, é possível especificar por extensões quais são os arquivos que sempre devem ser verificados.

- Opcionalmente, você pode optar por ***Verificar arquivos sem extensão*** - essa opção está ativada por padrão, e convém mantê-la nesse estado, a não ser que você tenha um motivo concreto para alterá-la. Arquivos sem extensão são relativamente suspeitos e devem ser verificados sempre.

- ***Ajustar a velocidade de conclusão da verificação*** - você pode usar este controle deslizante para alterar a prioridade do processo de verificação. Por padrão, a prioridade está definida para o nível *Sensível ao usuário*, que otimiza a velocidade do processo de verificação e o uso dos recursos do sistema. Se desejar, você pode executar o processo de verificação em nível mais baixo, fazendo com que o carregamento dos recursos do sistema seja minimizado (*procedimento útil quando for necessário trabalhar no computador sem se preocupar com o tempo que o sistema usará para fazer a verificação*), ou mais rápido, com maior necessidade de recursos (*por exemplo, quando o computador fica ocioso temporariamente*).

- ***Definir relatórios de verificação adicionais*** - o link abre uma nova caixa de diálogo ***Verificar relatórios*** que permite selecionar quais os possíveis tipos de descobertas devem ser relatados:



Aviso: *essas configurações de verificação são idênticas aos parâmetros de uma verificação definida recentemente, como descrito no capítulo* ***Verificação do AVG/ Programação da verificação/Como verificar****. Se você decidir alterar as configurações padrão de* ***Verificar todo o computador****, será possível salvar as novas configurações como o padrão a ser usado para todas as verificações futuras de todo o computador.*

12.2.2. Verificar arquivos ou pastas específicos

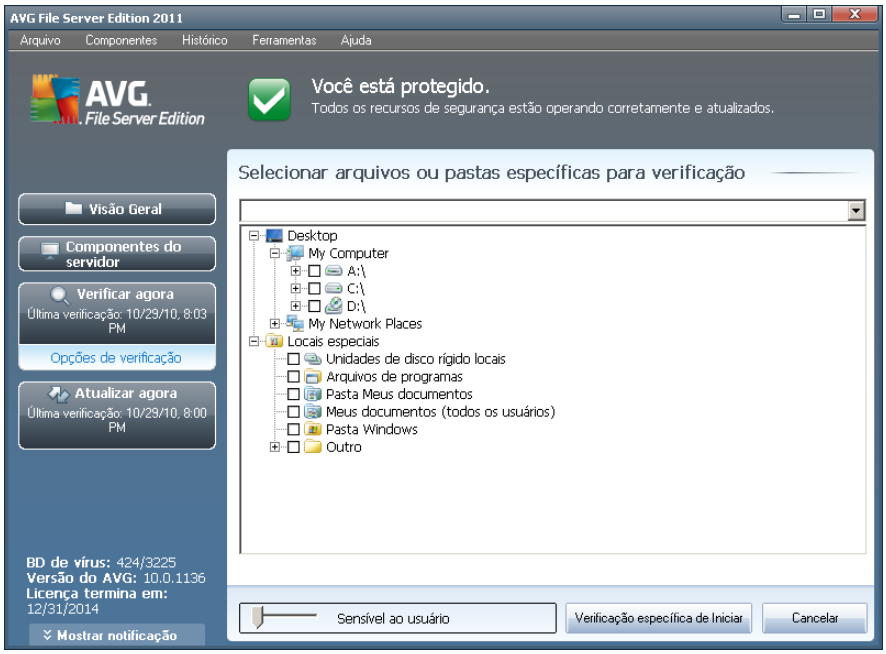
Verificar arquivos ou pastas específicos - verifica somente as áreas do computador que você tenha selecionado para verificação (*pastas selecionadas, discos rígidos, unidades de disquete, CDs etc.*). O andamento da verificação em caso de detecção e tratamento de vírus é o mesmo da verificação de todo o computador: todos os vírus encontrados serão reparados ou removidos para a ***Quarentena de vírus***. A verificação de arquivos ou pastas específicos pode ser usada para configurar seus próprios testes e sua programação com base nas necessidades.

Iniciar verificação

A opção ***Verificar arquivos ou pastas específicos*** pode ser iniciada diretamente na interface de verificação clicando no ícone de verificação. Uma nova caixa de diálogo chamada ***Selecionar arquivos ou pastas específicos para verificação*** será aberta. Na estrutura de árvores do computador, selecione as pastas que deseja verificar. O caminho para cada pasta selecionada será gerado automaticamente e exibido na caixa de texto na parte superior dessa caixa de diálogo.

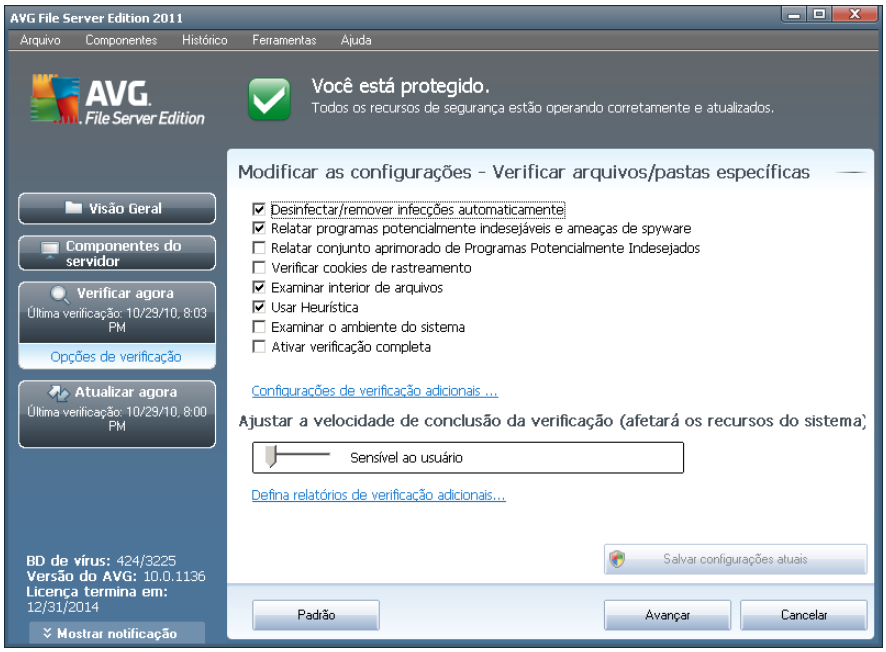
Também existe a possibilidade de fazer a verificação em uma determinada pasta enquanto suas subpastas são excluídas da verificação; para isso, insira um sinal de menos "**-**" na frente do caminho gerado automaticamente (*veja a imagem*). Para excluir da verificação a pasta inteira, use o parâmetro "!" .

Finalmente, para iniciar a verificação, pressione o botão ***Iniciar verificação***; o processo de verificação será basicamente idêntico a Verificar todo o computador.



Verificar edições de configuração

Você tem a opção de editar as configurações padrão predefinidas de ***Verificar arquivos ou pastas específicos***. Acesse o link ***Alterar as configurações de verificação*** para abrir a caixa de diálogo ***Alterar configurações de verificação de Verificar arquivos ou pastas específicos***. ***É recomendável manter as configurações padrão, a menos que você tenha um motivo válido para alterá-las.***



- ***Parâmetros de verificação*** - na lista de parâmetros de verificação, você pode ativar ou desativar parâmetros específicos conforme suas necessidades:

    - ***Reparar ou remover infecção automaticamente*** (*ativada por padrão*) - se um vírus for identificado durante a verificação, ele pode ser reparado automaticamente, se houver solução disponível. Se o arquivo infectado não puder ser reparado automaticamente, o objeto infectado será movido para a ***Quarentena de Vírus***.

    - ***Informar programas potencialmente indesejáveis e ameaças de spyware*** (*ativada por padrão*) - marque para ativar o mecanismo ***Anti-Spyware*** e verificar se há spyware e vírus. Spyware representa uma categoria de malware questionável: embora ele geralmente represente um risco de segurança, alguns desses programas pode ser instalado intencionalmente. Recomendamos manter esse recurso ativado, pois aumenta a segurança do computador.

    - ***Informar conjunto avançado de programas potencialmente indesejáveis*** (*desativada por padrão*) - marque para detectar o pacote estendido de spyware: programas que estão perfeitamente ok e são inofensivos quando adquiridos do fabricante diretamente, mas podem ser mal-utilizados para finalidades mal-intencionadas posteriormente. Esta é uma medida adicional que aumenta ainda mais a segurança de seu

computador; no entanto, pode eventualmente bloquear programas legais, e, portanto, é desativada por padrão.

- **Verificar cookies de rastreamento** (*desativada por padrão*) - este parâmetro do componente **Anti-Spyware** define que os cookies devem ser detectados; (*cookies HTTP são usados para autenticar, controlar e manter informações específicas sobre usuários, como preferências de sites ou conteúdo de carrinhos de compras eletrônicas*).

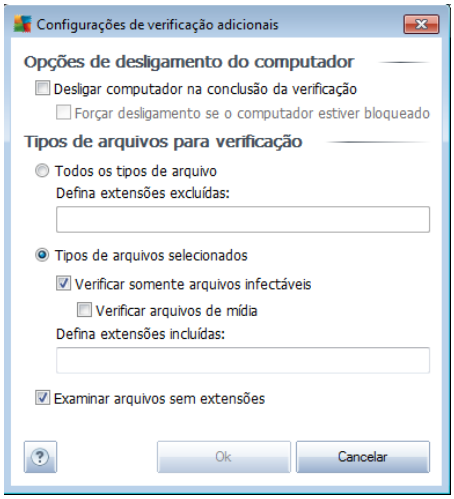
- **Verificar dentro dos arquivos** (*ativada por padrão*) - esse parâmetro define que a verificação deve ocorrer em todos os arquivos armazenados dentro de arquivos, como ZIP, RAR etc.

- **Usar heurística** (*desativada por padrão*) - a análise heurística (*emulação dinâmica das instruções do objeto verificado, em um ambiente de computador virtual*) será um dos métodos usados para detecção de vírus durante a verificação.

- **Verificar ambiente do sistema** (*desativada por padrão*) - a verificação também atuará nas áreas do sistema do seu computador.

- **Ativar verificação completa** (*desativada por padrão*) - em situações específicas (*suspeita de que seu computador foi infectado*), é possível marcar esta opção para ativar a maioria dos algoritmos de verificação completos que verificarão até mesmo as áreas do computador que dificilmente são infectadas, só para ter a absoluta certeza. Entretanto, lembre-se de que esse método consome bastante tempo.

- **Configurações de verificação adicionais** - o link abre uma nova caixa de diálogo **Configurações de verificação adicionais**, na qual é possível especificar os seguintes parâmetros:



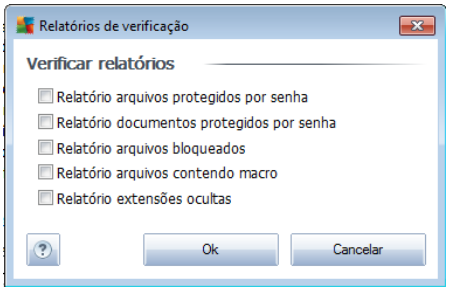
- **Opções de desligamento do computador** - decida se o computador deve ser desligado automaticamente quando a execução do processo de verificação terminar. Ao confirmar essa opção (**Desligar o computador**

quando o processo de verificação for concluído), uma nova opção permitirá que o computador seja desligado mesmo se ele estiver bloqueado (***Forçar desligamento do computador se estiver bloqueado***).

- ***Definir tipos de arquivo para verificação*** - além disso, você deve decidir se deseja verificar os seguintes itens:
  - ***Todos os tipos de arquivos*** com a possibilidade de definirem exceções a partir da verificação, fornecendo uma lista de extensões de arquivo separadas por vírgula que não devem ser verificadas;
  - ***Tipos de arquivos selecionados*** - você pode especificar que deseja verificar apenas os arquivos possivelmente infectáveis (*arquivos que não podem ser infectados não serão verificados; por exemplo, alguns arquivos de texto simples ou outros arquivos não executáveis*), incluindo arquivos de mídia (*arquivos de áudio e vídeo - se você deixar essa caixa desmarcada, o tempo de verificação será ainda menor, pois esses arquivos costumam ser grandes, e é muito improvável que eles sejam infectados por vírus*). Mais uma vez, é possível especificar por extensões quais são os arquivos que sempre devem ser verificados.
  - Opcionalmente, você pode optar por ***Verificar arquivos sem extensão*** - essa opção está ativada por padrão, e convém mantê-la nesse estado, a não ser que você tenha um motivo concreto para alterá-la. Arquivos sem extensão são relativamente suspeitos e devem ser verificados sempre.

- ***Prioridade do processo de verificação*** - você pode usar esse controle para alterar a prioridade do processo de verificação. Por padrão, a prioridade está definida para o nível *Sensível ao usuário*, que otimiza a velocidade do processo de verificação e o uso dos recursos do sistema. Se desejar, você pode executar o processo de verificação em nível mais baixo, fazendo com que o carregamento dos recursos do sistema seja minimizado (*procedimento útil quando for necessário trabalhar no computador sem se preocupar com o tempo que o sistema usará para fazer a verificação*), ou mais rápido, com maior necessidade de recursos (*por exemplo, quando o computador fica ocioso temporariamente*).

- ***Definir relatórios de verificação adicionais*** - o link abre uma nova caixa de diálogo ***Verificar relatórios*** que permite selecionar quais tipos de possíveis localizações devem ser relatados:



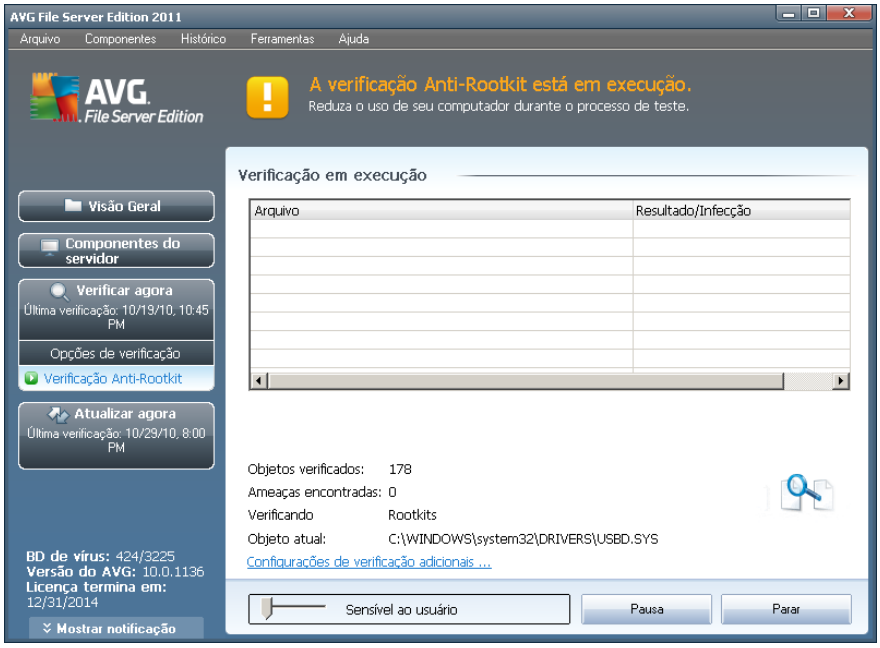
Aviso: *essas configurações de verificação são idênticas aos parâmetros de uma verificação definida recentemente, como descrito no capítulo* ***Verificação do AVG/ Programação da verificação/Como verificar****. Se você decidir alterar as configurações padrão de* ***Verificar arquivos ou pastas específicas****, será possível salvar as novas configurações como o padrão a ser usado para todas as verificações futuras de arquivos ou pastas específicas. Além disso, essa configuração será usada como modelo para todas as novas verificações programadas (todas as verificações personalizadas são baseadas na configuração atual de Verificação de arquivos ou pastas selecionados).*

12.2.3. Verificação Anti-Rootkit

A ***Verificação Anti-Rootkit*** verifica seu computador em busca de possíveis rootkits (*programas e tecnologias que possam ocultar atividades de malware no computador*). Se um rootkit for detectado, isso não quer dizer necessariamente que o computador está infectado. Em alguns casos, drivers específicos ou seções de aplicativos comuns podem ser detectados por engano como rootkits.

Iniciar verificação

A ***Verificação Anti-Rootkit*** pode ser iniciada diretamente na interface de verificação clicando no ícone de verificação. Se nenhuma outra configuração específica for definida para esse tipo de verificação, ela será iniciada imediatamente na caixa de diálogo ***Verificação em andamento*** *(veja a imagem*). A verificação pode ser interrompida temporariamente (***Pausar***) ou cancelada (***Parar***), se necessário.

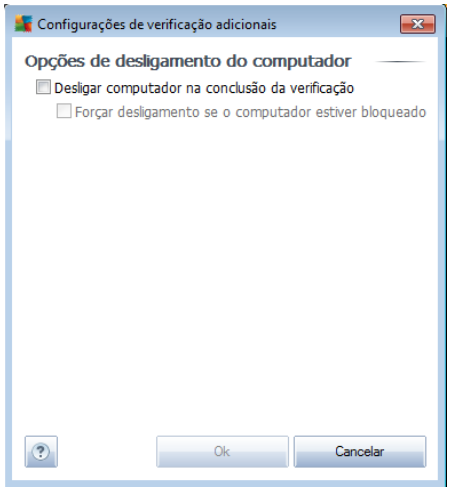


Verificar edições de configuração

A ***Verificação Anti-Rootkit*** é sempre iniciada nas configurações padrão, e a edição dos parâmetros de verificação só pode ser acessada na caixa de diálogo ***Configurações avançadas do AVG/Anti-Rootkit***. Na interface de verificação, a seguinte configuração está disponível, mas apenas enquanto a verificação está em execução:

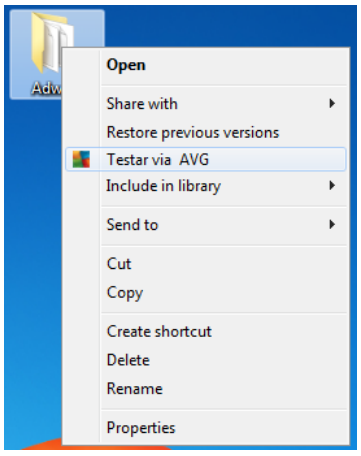
- ***Verificação automática*** - você pode usar este controle deslizante para alterar a prioridade do processo de verificação. Por padrão, a prioridade está definida no nível médio (*Verificação automática*) que otimiza a velocidade do processo de verificação e o uso dos recursos do sistema. Se desejar, você pode executar o processo de verificação em nível mais baixo, fazendo com que o carregamento dos recursos do sistema seja minimizado (*procedimento útil quando for necessário trabalhar no computador sem se preocupar com o tempo que o sistema usará para fazer a verificação*), ou mais rápido, com maior necessidade de recursos (*por exemplo, quando o computador fica ocioso temporariamente*).

- ***Configurações de verificação adicionais*** - este link abre uma nova caixa de diálogo ***Configurações de verificação adicionais***, na qual você pode definir possíveis condições de desligamento do computador relacionadas à ***Verificação Anti-Rootkit*** (***Desligar o computador após a conclusão da verificação*** e *possivelmente* ***Forçar encerramento se o computador estiver travado***):



12.3. Verificando o Windows Explorer

Além das verificações predefinidas iniciadas em todo o computador ou em áreas selecionadas, o **AVG Email Server Edition 2011 ainda oferece a opção de uma verificação rápida de um objeto específico diretamente no ambiente do Windows Explorer.** Se você desejar abrir um arquivo desconhecido e não tiver certeza sobre o seu conteúdo, poderá verificá-lo sob demanda. Siga estas etapas:



- No Windows Explorer, destaque o arquivo (ou pasta) que deseja verificar
- Clique com o botão direito do mouse no objeto para abrir o menu de contexto
- Selecione a opção ***Verificar com AVG*** para que o arquivo seja verificado com o AVG

12.4. Verificação de linha de comando

No **AVG Email Server Edition 2011** há a opção de executar a verificação a partir da linha de comando. Você pode usar esta opção em servidores, ou ao criar um script em lote para ser iniciado automaticamente após a inicialização do computador. A partir da linha de comando, você pode iniciar a verificação com a maioria dos parâmetros como oferecido em uma interface gráfica de usuário AVG.

Para iniciar a verificação AVG da linha de comando, execute o seguinte comando dentro da pasta em que o AVG está instalado:

- ***avgscanx*** para SO de 32 bits
- ***avgscana*** para SO de 64 bits

Sintaxe do comando

A seguir, a sintaxe do comando:

- ***avgscanx /parâmetro*** ... por exemplo. ***avgscanx /comp*** para verificação de todo o computador
- ***avgscanx /parâmetro /parâmetro*** .. com vários parâmetros, estes devem estar alinhados em uma fila e separados por um espaço e um caractere de barra
- se o parâmetro exigir um valor específico a ser fornecido (por exemplo, o parâmetro ***/scan*** requer informações sobre quais são as áreas selecionadas do seu computador a serem verificadas, e você precisa informar o caminho exato da seção selecionada), os valores serão divididos por ponto e vírgula, como por exemplo: ***avgscanx /scan=C:\;D:***

Parâmetros de verificação

Para exibir uma visão completa dos parâmetros disponíveis, digite o respectivo comando junto com o parâmetro /? ou /HELP (por ex., ***avgscanx /?***). O único parâmetro obrigatório é /SCAN, que especifica que áreas do computador que devem ser verificadas. Para obter uma explicação mais detalhada das opções, consulte a visão geral dos parâmetros da linha de comando.

Para executar a verificação, pressione ***Enter***. Durante a verificação, você pode interromper o processo ao pressionar ***Ctrl+C*** ou ***Ctrl+Pause***.

Verificação CMD iniciada pela interface gráfica

Quando você executa seu computador no Modo de segurança do Windows, também é possível iniciar a verificação das linhas de comando pela interface gráfica do usuário. A

verificação será iniciada pela linha de comando; a caixa de diálogo ***Composer da linha de comando*** apenas permite que você especifique a maioria dos parâmetros de verificação na interface gráfica amigável.

Como esta caixa de diálogo está acessível apenas pelo Modo de segurança do Windows, para obter uma descrição detalhada dela consulte o arquivo de ajuda acessível diretamente pela caixa de diálogo.

12.4.1. Parâmetros de verificação CMD

A seguir, veja uma lista de todos os parâmetros disponíveis para a verificação de linha de comando:

- ***/SCAN*** Verificar arquivos ou pastas específicos /SCAN=path;path (e.x. /SCAN=C:\;D:\)
- ***/COMP*** Verificar todo o computador
- ***/HEUR*** Usar análise heurística
- ***/EXCLUDE*** Excluir caminho ou arquivo da verificação
- ***/@*** Arquivo de comando/nome de arquivo/
- ***/EXT*** Verificar estas extensões/por exemplo, EXT=EXE,DLL
- ***/NOEXT*** Não verificar estas extensões/por exemplo, NOEXT=JPG/
- ***/ARC*** Verificar arquivos
- ***/CLEAN*** Limpar automaticamente
- ***/TRASH*** Mover arquivos infectados para a Quarentena de vírus
- ***/QT*** Teste rápido
- ***/MACROW*** Relatar macros
- ***/PWDW*** Relatar arquivos protegidos por senha
- ***/IGNLOCKED*** Ignorar arquivos bloqueados
- ***/REPORT*** Relatar para arquivo/ nome de arquivo/
- ***/REPAPPEND*** Acrescentar ao arquivo de relatório
- ***/REPOK*** Relatar arquivos não infectados como OK
- ***/NOBREAK*** Não permitir abortar com CTRL-BREAK
- ***/BOOT*** Ativar verificação de MBR/BOOT

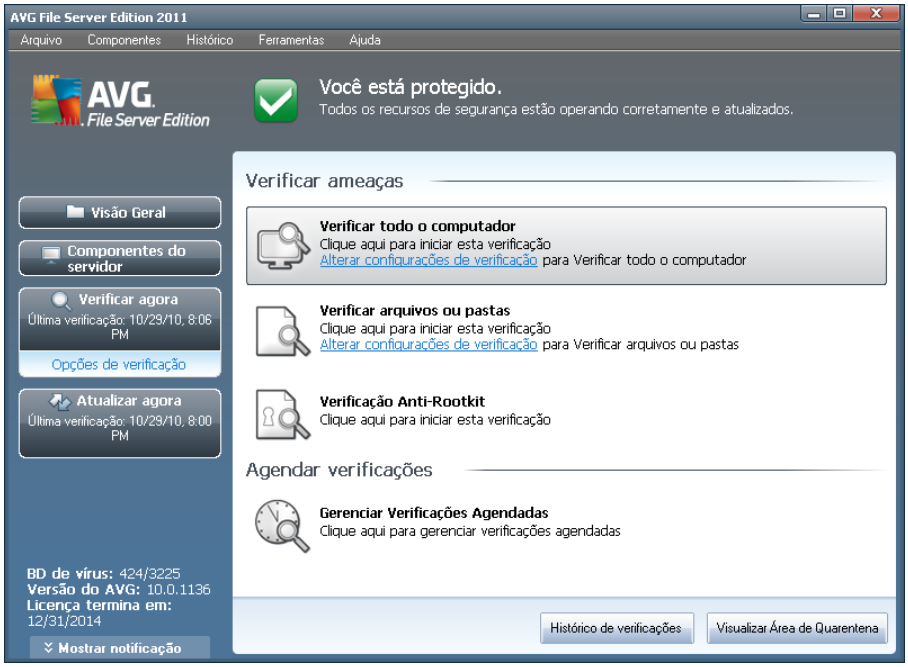
- ***/PROC*** Verificar processos ativos
- ***/PUP*** Relatar "Programas potencialmente indesejáveis"
- ***/REG*** Verificar registro
- ***/COO*** Verificar cookies
- ***/?*** Exibir ajuda neste tópico
- ***/HELP*** Exibir ajuda neste tópico
- ***/PRIORITY*** Definir prioridade de verificação/Baixa, Automática, Alta (veja Configurações avançadas/Verificações)
- ***/SHUTDOWN*** Desligar o computador na conclusão da verificação
- ***/FORCESHUTDOWN*** Forçar o computador a ser desligado na conclusão da verificação
- ***/ADS*** Verificar fluxos de dados alternativos (apenas NTFS)
- ***/ARCBOMBSW*** Informar arquivos compactados novamente

12.5. Programação de verificação

Com o **AVG Email Server Edition 2011**, é possível executar uma verificação sob demanda (por exemplo, quando você suspeitar de uma infecção no seu computador) ou com base em um plano programado. É altamente recomendável executar verificações com base em uma programação. Dessa forma, você pode assegurar que seu computador esteja protegido contra a possibilidade de infecção e não precisará se preocupar com a inicialização da verificação.

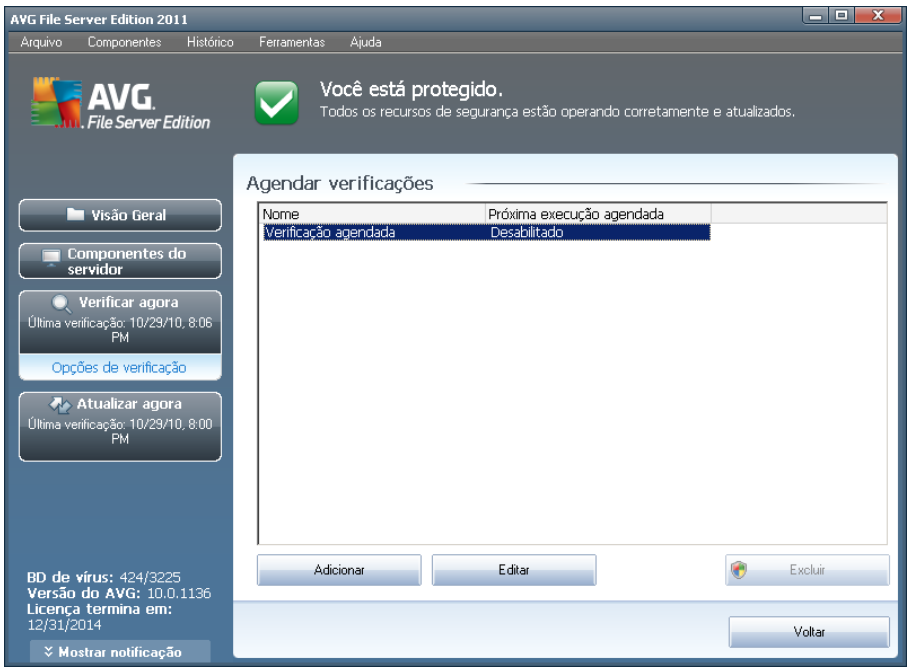
Você deve ***Verificar todo o computador*** regularmente, pelo menos uma vez por semana. Mas, se possível, inicie a verificação de todo o computador diariamente, conforme definido na configuração padrão da programação da verificação. Se o computador estiver "sempre ligado", você poderá programar verificações fora dos horários de trabalho. Se o computador for desligado algumas vezes, programe verificações para a inicialização do computador quando a tarefa tiver sido executada.

Para criar novas programações de verificação, consulte a interface de verificação do AVG e localize a seção ***Programar verificações*** , na parte inferior:



Agendar verificações

Clique no ícone gráfico na seção ***Programar verificações*** para abrir uma nova caixa de diálogo ***Programar verificações***, na qual você encontrará uma lista de todas as verificações atualmente programadas:



É possível editar/adicionar verificações usando os seguintes botões de controle:

- ***Adicionar programação de verificação*** - o botão abre a caixa de diálogo ***Configurações da verificação programada***, guia ***Configurações de programação***. Nessa caixa de diálogo, você pode especificar os parâmetros do teste definido recentemente.

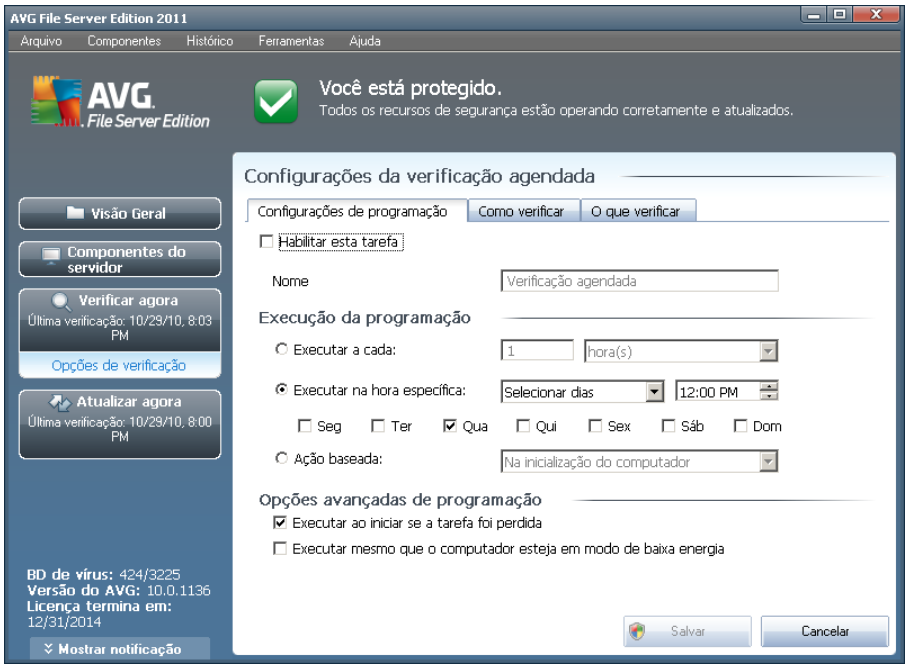
- ***Editar programação de verificação*** - esse botão só pode ser usado se você tiver selecionado um teste existente anteriormente na lista de testes programados. Nesse caso, o botão aparecerá ativo e você poderá clicar nele para passar para a caixa de diálogo ***Configurações da verificação programada*** , guia ***Configurações de programação***. Os parâmetros do teste selecionado já estão especificados e poderão ser editados aqui.

- ***Excluir programação de verificação*** - esse botão também ficará ativo se você tiver selecionado um teste existente anteriormente na lista de testes programados. Esse teste pode ser excluído da lista se você pressionar o botão de controle. Entretanto, você só poderá remover os próprios testes. O teste ***Programação de verificação de todo o computador*** predefinido com as configurações padrão nunca poderá ser excluído.

- ***Voltar*** - retornar à interface de verificação do AVG

12.5.1. Configurações de programação

Se quiser programar um novo teste e sua ativação regular, insira informações na caixa de diálogo ***Configurações para teste programado*** (*clique no botão* ***Adicionar verificação programada*** *na caixa de diálogo* ***Programar verificações***). A caixa de diálogo é dividida em três guias:***Configurações de programa*** - *veja imagem abaixo (a guia padrão à qual você será automaticamente redirecionado),****Como verificar*** e ***O que verificar***.



Na guia ***Configurações de agendamento***, você pode primeiro marcar/desmarcar o item ***Habilitar esta tarefa*** para simplesmente desativar temporariamente o teste programado e ativá-lo novamente conforme necessário.

Em seguida, informe o nome da verificação que você está prestes a criar e agendar. Digite o nome no campo de texto, no item ***Nome***. Tente usar nomes curtos, descritivos e apropriados para a verificação para tornar seu reconhecimento mais fácil posteriormente.

Exemplo: *não é apropriado denominar a verificação como "Nova verificação" ou "Minha verificação", pois esses nomes não se referem exatamente ao que será verificado. Por outro lado, um exemplo de nome descritivo ideal seria "Verificação de áreas do sistema" etc. Além disso, não é necessário especificar no nome da verificação se ela é uma verificação de todo o computador ou somente uma verificação de pastas ou arquivos selecionados. Suas verificações serão sempre uma versão específica da verificação de arquivos ou pastas selecionados.*

Nessa caixa de diálogo você ainda poderá definir os seguintes parâmetros de verificação:

- ***Execução do programa*** - especifica os intervalos de tempo para a inicialização de novas verificações programadas. O tempo pode ser definido pela repetição da inicialização da verificação depois de um determinado período (***Executar a cada ...***) pela definição de uma data e hora exatas (***Executar em uma hora específica...***), ou pela definição de um evento ao qual a inicialização da atualização deve ser associada (***Ação baseada na inicialização do computador***).

- ***Opções de programa avançadas*** - essa seção permite definir sob quais condições a verificação deverá ou não ser inicializada se o computador estiver no modo de pouca energia ou completamente desligado.

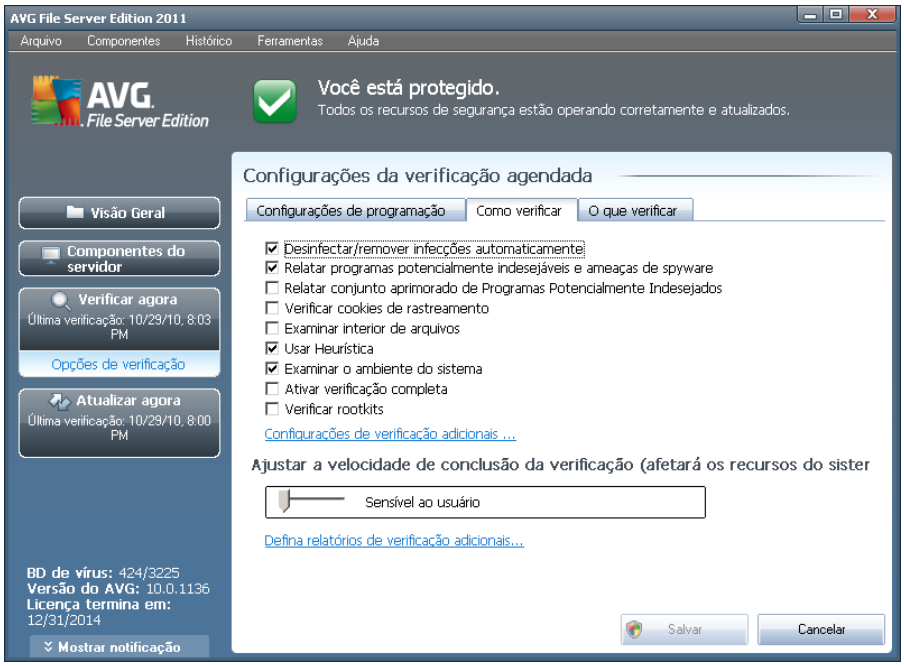
Botões de controle da caixa de diálogo Configurações para verificação programada

Há dois botões de controle disponíveis nas três guias da caixa de diálogo ***Configurações da verificação programada*** (***Configurações do programa***, ***Como verificar*** e ***O que verificar***), e eles têm a mesma funcionalidade, independentemente da guia em que você esteja no momento:

- ***Salvar*** - salva todas as alterações realizadas nessa guia ou em qualquer outra dessa caixa de diálogo e volta para a caixa de diálogo padrão da interface de verificação do AVG . Portanto, se você desejar configurar os parâmetros de teste em todas as guias, pressione o botão para salvá-los somente depois de ter especificado todos os requisitos.

- ***Cancelar*** - cancela todas as alterações realizadas nessa guia ou em qualquer outra guia dessa caixa de diálogo e volta para a caixa de diálogo padrão da interface do AVG .

12.5.2. Como verificar



Na guia ***Como verificar*** , você encontrará uma lista de parâmetros de verificação que podem ser ativados ou desativados. Por padrão, a maioria dos parâmetros é ativada e a funcionalidade será aplicada durante a verificação. A menos que você tenha um motivo válido para alterar as configurações, recomendamos manter a configuração predefinida:

- ***Reparar ou remover vírus automaticamente*** (*ativada por padrão*): se um vírus for identificado durante a verificação, ele pode ser reparado automaticamente, se houver solução disponível. Caso não seja possível reparar o arquivo infectado automaticamente ou se você decidir desativar essa opção, você será notificado das detecções de vírus e terá que decidir o que fazer com a infecção de vírus detectada. A ação recomendada é remover o arquivo infectado para a ***Quarentena de vírus***.

- ***Informar programas potencialmente indesejáveis e ameaças de spyware –*** marque para ativar o mecanismo ***Anti-Spyware*** ***e verificar spyware, bem como vírus.*** Spyware representa uma categoria de malware questionável: embora ele geralmente represente um risco de segurança, alguns desses programas pode ser instalado intencionalmente. Recomendamos manter esse recurso ativado, pois aumenta a segurança do computador.

- ***Informar conjunto avançado de programas potencialmente indesejáveis*** (*desativada por padrão*): marque para detectar o pacote estendido de spyware: programas que estão perfeitamente ok e são inofensivos quando adquiridos do fabricante diretamente, mas podem ser mal-utilizados para finalidades mal-intencionadas posteriormente. Esta é uma medida adicional que aumenta ainda mais a segurança de seu computador; no entanto, pode eventualmente bloquear programas legais, e, portanto, é desativada por

padrão.

- ***Verificar cookies de rastreamento*** (*desativada por padrão*): este parâmetro do componente ***Anti-Spyware*** define que os cookies devem ser detectados durante a verificação (*cookies HTTP são usados para autenticar, controlar e manter informações específicas sobre usuários, como preferências de sites ou conteúdo de carrinhos de compras eletrônicas*).

- ***Verificar interior dos arquivos*** (*desativada por padrão*): esse parâmetro define que a verificação deve atuar em todos os arquivos, mesmo se eles estiverem compactados em algum tipo de arquivo, como ZIP, RAR etc.

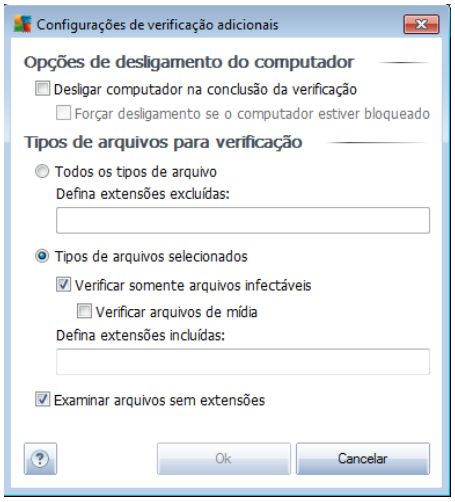
- ***Usar Heurística*** (*ativada por padrão*): a análise heurística (*emulação dinâmica das instruções do objeto verificado, em um ambiente de computador virtual*) será um dos métodos usados para detecção de vírus durante a verificação.

- ***Verificar ambiente do sistema*** (*ativada por padrão*): a verificação também atuará nas áreas do sistema do seu computador.

- ***Ativar verificação completa*** (*desativada por padrão*) - em situações específicas (*suspeita de que seu computador foi infectado*), é possível marcar esta opção para ativar a maioria dos algoritmos de verificação completos que verificarão até mesmo as áreas do computador que dificilmente são infectadas, só para ter a absoluta certeza. Entretanto, lembre-se de que esse método consome bastante tempo.

Em seguida, será possível alterar a configuração da verificação da seguinte maneira:

- ***Configurações de verificação adicionais*** - o link abre uma nova caixa de diálogo ***Configurações de verificação adicionais***, na qual é possível especificar os seguintes parâmetros:



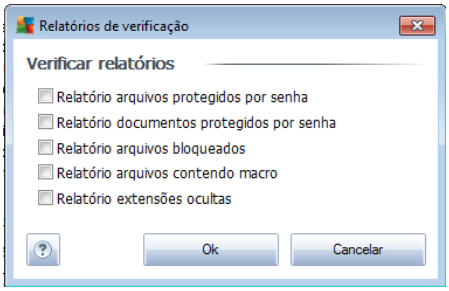
  - ***Opções de desligamento do computador*** - decida se o computador deve ser desligado automaticamente quando a execução do processo de

verificação terminar. Ao confirmar essa opção (***Desligar o computador quando o processo de verificação for concluído***), uma nova opção permitirá que o computador seja desligado mesmo que ele esteja bloqueado (***Forçar desligamento do computador se estiver bloqueado***).

- ***Definir tipos de arquivo para verificação*** - além disso, você deve decidir se deseja verificar os seguintes itens:
  - ***Todos os tipos de arquivos*** com a possibilidade de definirem exceções a partir da verificação, fornecendo uma lista de extensões de arquivo separadas por vírgula que não devem ser verificadas;
  - ***Tipos de arquivos selecionados*** - você pode especificar que deseja verificar apenas os arquivos possivelmente infectáveis (*arquivos que não podem ser infectados não serão verificados; por exemplo, alguns arquivos de texto simples ou outros arquivos não executáveis*), incluindo arquivos de mídia (*arquivos de áudio e vídeo - se você deixar essa caixa desmarcada, o tempo de verificação será ainda menor, pois esses arquivos costumam ser grandes, e é muito improvável que eles sejam infectados por vírus*). Mais uma vez, é possível especificar por extensões quais são os arquivos que sempre devem ser verificados.
  - Opcionalmente, você pode optar por ***Verificar arquivos sem extensão*** - essa opção está ativada por padrão, e convém mantê-la nesse estado, a não ser que você tenha um motivo concreto para alterá-la. Arquivos sem extensão são relativamente suspeitos e devem ser verificados sempre.

- ***Ajustar a velocidade de conclusão da verificação*** - você pode usar este controle deslizante para alterar a prioridade do processo de verificação. O nível médio otimiza a velocidade do processo de verificação e o uso dos recursos do sistema. Se desejar, você pode executar o processo de verificação em nível mais baixo, fazendo com que o carregamento dos recursos do sistema seja minimizado (*procedimento útil quando for necessário trabalhar no computador sem se preocupar com o tempo que o sistema usará para fazer a verificação*), ou mais rápido, com maior necessidade de recursos (*por exemplo, quando o computador fica ocioso temporariamente*).

- ***Definir relatórios de verificação adicionais*** - o link abre uma nova caixa de diálogo ***Verificar relatórios*** que permite selecionar quais os possíveis tipos de descobertas devem ser relatados:



Observação: *por padrão, a configuração da verificação é definida para desempenho ideal. A menos que você tenha um motivo válido para alterar essas configurações, é altamente recomendável manter a configuração predefinida. As alterações de configuração devem ser realizadas somente por usuários experientes. Para obter outras opções de configuração de verificação, consulte a caixa de diálogo* ***Configurações avançadas*** *por meio do item do menu de sistema* ***Arquivo/ Configurações avançadas****.*

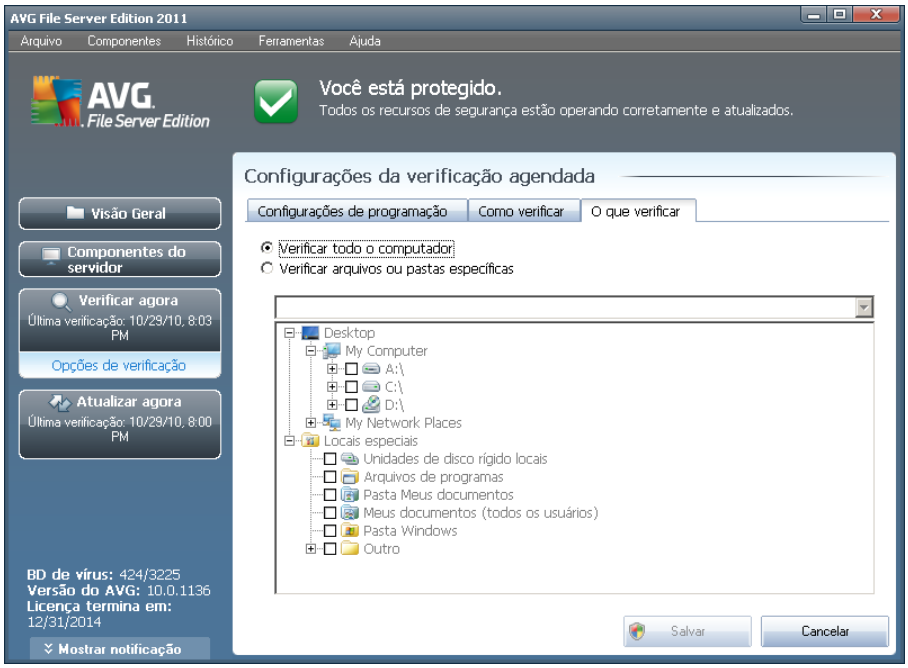
Botões de controle

Há dois botões de controle disponíveis nas três guias da caixa de diálogo ***Configurações da verificação programada*** (***Configurações de programação***, ***Como verificar e*** O que verificar***), e eles têm a mesma funcionalidade, independentemente da guia em que você esteja no momento:

- ***Salvar*** - salva todas as alterações realizadas nessa guia ou em qualquer outra dessa caixa de diálogo e volta para a caixa de diálogo padrão da interface de verificação do AVG . Portanto, se você desejar configurar os parâmetros de teste em todas as guias, pressione o botão para salvá-los somente depois de ter especificado todos os requisitos.

- ***Cancelar*** - cancela todas as alterações realizadas nessa guia ou em qualquer outra guia dessa caixa de diálogo e volta para a caixa de diálogo padrão da interface do AVG .

12.5.3. O que verificar



Na guia ***O que verificar***, você pode definir se deseja programar a verificação de todo o computador ou a verificação de arquivos ou pastas específicas***.

Se você selecionar a verificação de arquivos ou pastas específicas, na parte inferior dessa caixa de diálogo a estrutura de árvore exibida será ativada e você poderá especificar as pastas para verificação (expanda os itens clicando no nó de mais até encontrar a pasta que deseja verificar). Você pode selecionar várias pastas marcando as respectivas caixas. As pastas selecionadas aparecerão no campo de texto na parte superior da caixa de diálogo e o menu suspenso manterá o histórico das verificações selecionadas para um uso posterior. *Ou você pode inserir o caminho inteiro para a pasta desejada manualmente (se inserir vários caminhos, será necessário separar com pontos-e-vírgulas sem espaços extras*).

Na estrutura de árvore você também pode ver um ramo chamado ***Locais especiais***. A seguir encontre uma lista de locais que serão verificados uma vez que a respectiva caixa de seleção esteja marcada:

- ***Discos rígidos locais*** - todos os discos rígidos de seu computador
- ***Arquivos de programas***
    - C:\Arquivos de Programas\
    - *na versão de 64 bits* C:\Arquivos de Programas (x86)
- ***Pasta Meus documentos***
    - *para Windows XP:* C:\Documents and Settings\Usuário padrão\Meus

documentos\

- *para Windows Vista/7*: C:\Usuários\usuário\Documentos\

- ***Meus documentos (todos os usuários)***
  - *para Windows XP*: C:\Documents and Settings\Todos os usuários\Documentos\
  - *para Windows Vista/7*: C:\Usuários\Público\Documentos\

- ***Pasta do Windows*** - C:\Windows\

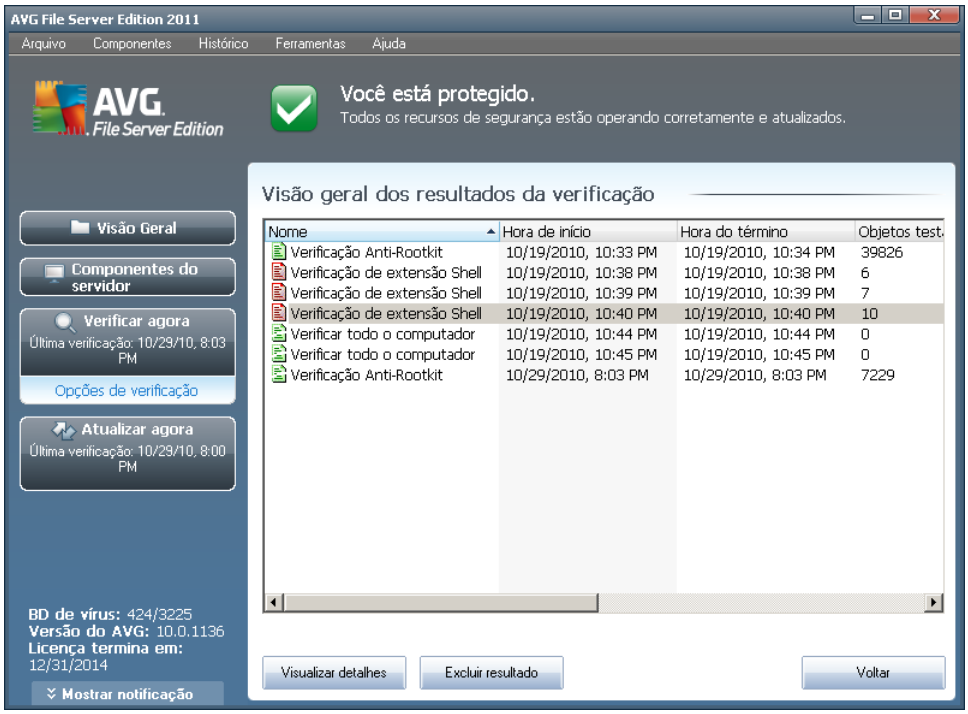
- ***Outro***
  - Drive de sistema – o disco rígido no qual o sistema operacional está instalado (normalmente C:)
  - *Pasta do sistema* - C:\Windows\System32\
  - *Pasta Arquivos Temporários* - C:\Documents and Settings\Usuário\Local\ (*Windows XP*); ou C:\Usuários\usuário\AppData\Local\Temp\ (*Windows Vista/7*)
  - *Arquivos Temporários de Internet* - C:\Documents and Settings\Usuário\Configurações locais\Arquivos temporários de Internet\ (*Windows XP*); ou C: \Usuários\usuário\AppData\Local\Microsoft\Windows\Arquivos Temporários de Internet (*Windows Vista/7*)

Botões de controle da caixa de diálogo Configurações para verificação programada

Há dois botões de controle disponíveis nas três guias da caixa de diálogo ***Configurações da verificação programada*** (***Configurações do programa***, ***Como verificar***e ***O que verificar***), e eles têm a mesma funcionalidade, independentemente da guia em que você esteja no momento:

- ***Salvar*** - salva todas as alterações realizadas nessa guia ou em qualquer outra dessa caixa de diálogo e volta para a caixa de diálogo padrão da interface de verificação do AVG . Portanto, se você desejar configurar os parâmetros de teste em todas as guias, pressione o botão para salvá-los somente depois de ter especificado todos os requisitos.
- ***Cancelar*** - cancela todas as alterações realizadas nessa guia ou em qualquer outra guia dessa caixa de diálogo e volta para a caixa de diálogo padrão da interface do AVG .

12.6. Visão geral dos resultados da verificação



A caixa de diálogo ***Visão geral dos resultados de verificação*** pode ser acessada da interface de verificação do AVG, por meio do botão ***Histórico de verificação***. A caixa de diálogo fornece uma lista de todas as verificações inicializadas anteriormente e as informações sobre seus resultados:

- ***Nome*** - designação da verificação; pode ser o nome de uma das verificações predefinidas ou o nome que você tenha dado à verificação que programou. Todos os nomes incluem um ícone indicando o resultado da verificação:

  - o ícone verde informa que não foram detectadas infecções durante a verificação

  - o ícone azul indica que uma infecção foi detectada durante a verificação, mas o objeto infectado foi removido automaticamente

  - o ícone vermelho avisa que uma infecção foi detectada durante a verificação e não foi possível removê-la!

  Cada ícone pode ser sólido ou cortado ao meio. O ícone sólido indica uma verificação que foi concluída adequadamente. O ícone cortado ao meio indica que a verificação foi cancelada ou interrompida.

  Nota: *para obter informações detalhadas sobre cada verificação, consulte a caixa de diálogo* ***Resultados da Verificação****, que pode ser acessada pelo botão* ***Exibir detalhes*** *(na parte inferior desta caixa de diálogo).*

- ***Horário de início*** - a data e a hora em que a verificação foi inicializada
- ***Horário de término*** - a data e a hora em que a verificação foi encerrada
- ***Objetos testados*** - número de objetos que foram verificados
- ***Infecções*** - número de infecções por vírus detectadas/removidas
- ***Spyware*** - número de spyware detectados/removidos
- ***Aviso*** - número de objetos suspeitos detectados ***
- ***Rootkits*** - número de rootkits detectados rootkits
- ***Informações do log de verificação*** - informações relacionadas ao processo e o resultado da verificação (geralmente em sua finalização ou interrupção)

Botões de controle

Os botões de controle da caixa de diálogo ***Visão geral dos resultados da verificação*** são:

- ***Exibir detalhes***- pressione-o para ativar a caixa de diálogo***Resultados da verificação*** para exibir dados detalhados na verificação selecionada
- ***Excluir resultado*** - pressione-o para remover o item selecionado a partir da visão geral dos resultados da verificação
- ***Voltar*** - volta para a caixa de diálogo padrão da interface de verificação do AVG

12.7. Detalhes dos resultados da verificação

Se na caixa de diálogo ***Visão Geral dos Resultados da Verificação*** uma verificação específica for selecionada, você poderá clicar no botão ***Exibir detalhes*** para passar para a caixa de diálogo ***Resultados da Verificação***, que fornece detalhes sobre o processo e o resultado da verificação selecionada.

A caixa de diálogo divide-se em várias guias:

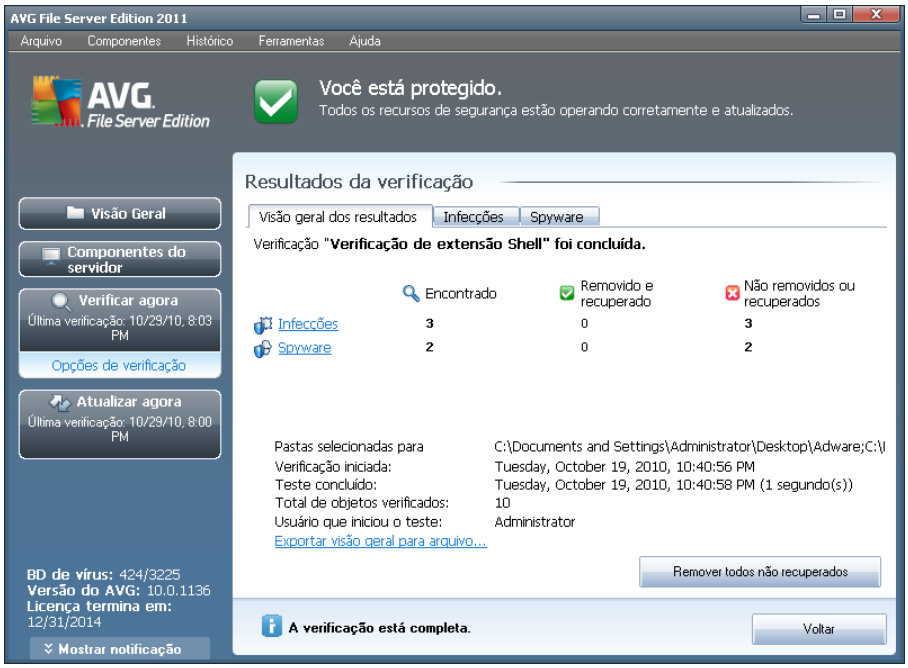
- ***Visão Geral dos Resultados*** - essa guia é exibida sempre e fornece dados estatísticos descrevendo o processo de verificação.
- ***Infecções*** - essa guia é exibida somente se uma infecção por vírus tiver sido detectada durante a verificação
- ***Spyware*** - essa guia é exibida somente se um spyware tiver sido detectado durante a verificação
- ***Aviso*** - essa guia é exibida somente se cookies forem detectados durante a

verificação

- ***Rootkits*** - essa guia é exibida somente se rootkits tiverem sido detectados durante a verificação

- ***Informações*** **-** essa guia é exibida somente se algumas ameaças potenciais tiverem sido detectadas, mas se não tiver sido possível classificá-las em nenhuma das categorias acima. A guia fornecerá uma mensagem de aviso sobre a descoberta. Além disso, você vai encontrar aqui informações sobre objetos que não podem ser verificados (por exemplo, arquivos protegidos por senha).

12.7.1. Guia Visão geral dos resultados



Na guia ***Verificar resultados***, é possível encontrar estatísticas detalhadas com informações sobre:

- infecções por vírus/spyware detectadas

- infecções por vírus/spyware removidas

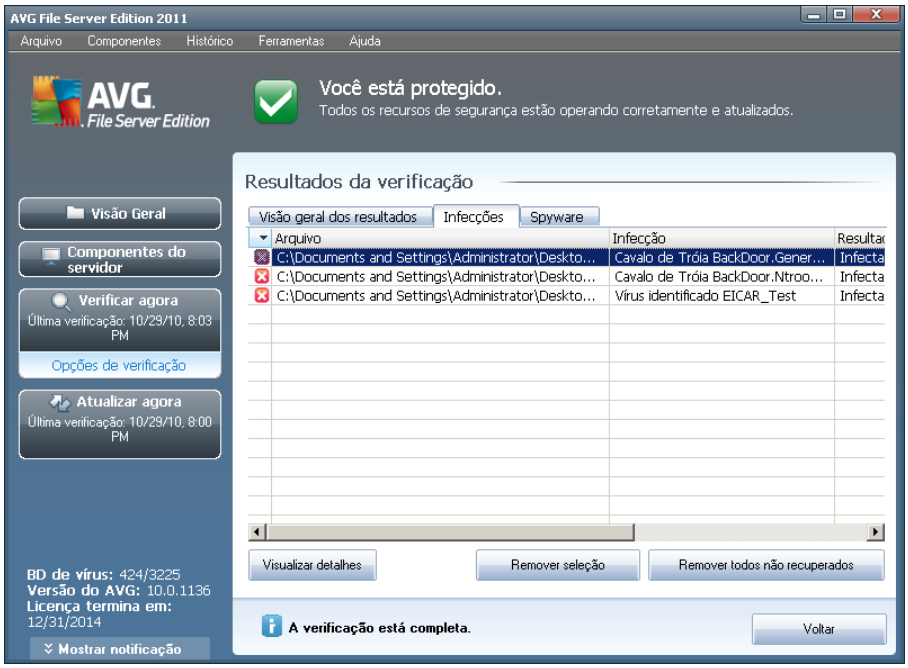
- o número de infecções por vírus/spyware que não puderam ser removidas ou reparadas

Além disso, você encontrará informações sobre a data e a hora exata da inicialização da verificação, o número total de objetos verificados, a duração da verificação e o número de erros ocorridos durante a verificação.

Botões de controle

Há somente um botão de controle disponível nessa caixa de diálogo. O botão ***Fechar resultados*** o leva de volta à caixa de diálogo ***Visão geral dos resultados da verificação***.

12.7.2. Guia Infecções



A guia ***Infecções*** só será exibida na caixa de diálogo ***Resultados da verificação*** se uma infecção de vírus for detectada durante uma verificação. A guia é dividida em três seções, que apresentam estas informações:

- ***Arquivo*** - caminho completo para o local original do objeto infectado
- ***Infecções*** - nome do vírus detectado (*para obter detalhes sobre o vírus específico, consulte a Enciclopédia de vírus online*).
- ***Resultado*** - define o status atual do objeto infectado detectado durante a verificação.
    - ***Infectado*** - o objeto infectado foi detectado e mantido no local original (*por exemplo, se você tiver desativado a opção de reparação automática em uma configuração de verificação específica*).
    - ***Reparado*** - o objeto infectado foi reparado automaticamente e mantido no local original
    - ***Movido para Quarentena de Vírus*** - o objeto infectado foi movido para a ***Quarentena de vírus***.
    - ***Excluído*** - o objeto infectado foi excluído.

- ***Adicionado às exceções PPI***- a detecção foi avaliada como exceção e adicionada à lista de exceções PPI (*configurada na caixa de diálogo* ***Exceções PPI*** *das configurações avançadas*)

- ***Arquivo bloqueado - não testado*** - o objeto é bloqueado e o AVG não pode verificá-lo.

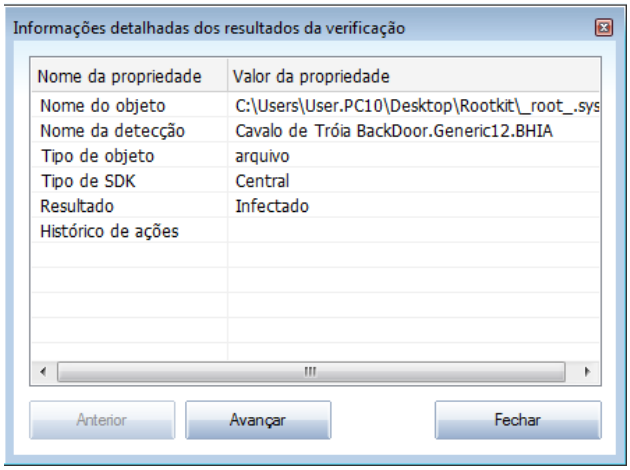
- ***Objeto potecialmente perigoso*** - o objeto foi detectado como potencialmente perigoso, mas não infectado (ele pode conter macros, por exemplo*).* As informações devem ser consideradas apenas como aviso.

- ***Reinicialização necessária para concluir ação*** - não é possível remover o objeto infectado. Para removê-lo completamente, é necessário reiniciar o computador.

Botões de controle

Há três botões de controle disponíveis nessa caixa de diálogo:

- ***Exibir detalhes***- o botão abre uma nova janela de diálogo denominada ***Informações detalhadas do objeto***:



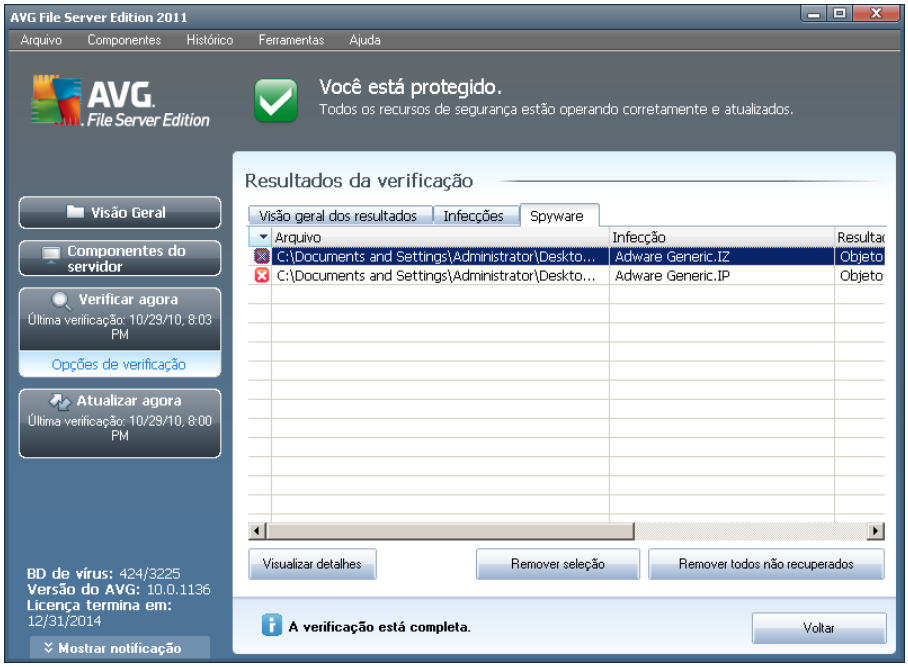
  Nesta caixa de diálogo, você pode encontrar informações detalhadas sobre o objeto infeccioso selecionado (*por exemplo, nome e local do objeto infeccioso, tipo de objeto, tipo de SDK, resultado da detecção e histórico de ações relacionado ao objeto detectado*). Usando os botões***Voltar***/ ***Avançar***, você pode ver informações sobre descobertas específicas. Use o botão ***Fechar*** para fechar a caixa de diálogo.

- ***Remover selecionadas*** - use o botão para mover a descoberta selecionada para a ***Quarentena***

- ***Remover todas as não reparadas*** - esse botão exclui todas as descobertas de vírus que não foram reparadas ou movidas para a ***Quarentena***

- ***Fechar resultados*** - fecha a visão geral das informações e volta para a caixa de diálogo ***Visão geral dos resultados da verificação***.

12.7.3. Guia Spyware



A guia ***Spyware*** só é exibida na caixa de diálogo ***Verificar resultados*** se um spyware for detectado durante uma verificação. A guia é dividida em três seções, que apresentam estas informações:

- ***Arquivo*** - caminho completo para o local original do objeto infectado
- ***Infecções*** - nome do spyware detectado (*para obter detalhes sobre os vírus específicos, consulte a* ***Enciclopédia de Vírus*** *online*)
- ***Resultado*** - define o status atual do objeto detectado durante a verificação.
    - ***Infectado*** - o objeto infectado foi detectado e mantido no local original (por exemplo, se você tiver desativado a opção de reparação automática em uma configuração de verificação específica).
    - ***Reparado*** - o objeto infectado foi reparado automaticamente e mantido no local original
    - ***Movido para Quarentena de vírus*** - o objeto infectado foi movido para a ***Quarentena de vírus***.
    - ***Excluído*** - o objeto infectado foi excluído.
    - ***Adicionado a extensões PPI*** - a detecção foi avaliada como exceção e adicionada à lista de exceções PPI (*configurada na caixa de diálogo*

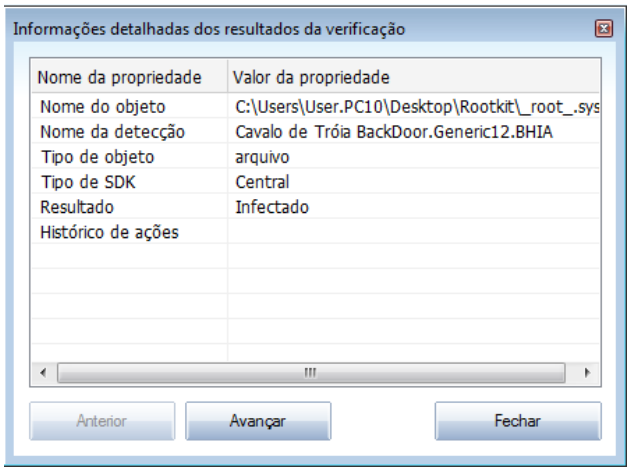
Exceções PPI *das configurações avançadas*)

- ***Arquivo bloqueado - não testado*** - o objeto é bloqueado e o AVG não pode verificá-lo.
- ***Objeto potencialmente perigoso*** - o objeto foi detectado como potencialmente perigoso, mas não infectado (ele pode conter macros, por exemplo). As informações devem ser consideradas apenas um aviso.
- ***Reinicialização necessária para concluir ação*** - não é possível remover o objeto infectado. Para removê-lo completamente, é necessário reiniciar o computador.

Botões de controle

Há três botões de controle disponíveis nessa caixa de diálogo:

- ***Exibir detalhes***- o botão abre uma nova janela de diálogo denominada ***Informações detalhadas do objeto***:



  Nesta caixa de diálogo, você pode encontrar informações detalhadas sobre o objeto infeccioso selecionado (*por exemplo, nome e local do objeto infeccioso, tipo de objeto, tipo de SDK, resultado da detecção e histórico de ações relacionado ao objeto detectado*). Usando os botões***Voltar***/ ***Avançar***, você pode ver informações sobre descobertas específicas. Use o botão ***Fechar*** para sair da caixa de diálogo.

- ***Remover selecionadas*** - use o botão para mover a descoberta selecionada para a ***Quarentena***
- ***Remover todas as não reparadas*** - esse botão exclui todas as descobertas de vírus que não foram reparadas ou movidas para a ***Quarentena***
- ***Fechar resultados*** - fecha a visão geral das informações e volta para a caixa

de diálogo ***Visão geral dos resultados da verificação***.

12.7.4. Guia Avisos

A guia ***Avisos*** exibe informações sobre objetos "suspeitos" (*normalmente arquivos*) detectados durante a verificação. Quando detectados pela ***Proteção Residente***, esses arquivos têm o acesso bloqueado. Exemplos típicos desse tipo de descoberta são: arquivos ocultos, cookies, chaves de Registro suspeitas, documentos ou arquivos protegidos por senha etc Tais arquivos não representam uma ameaça direta para o seu computador ou para a sua segurança. Informações sobre esses arquivos costumam ser úteis no caso de ser detectado um adware ou spyware no seu computador. Se o teste do AVG detectar apenas Avisos, nenhuma ação será necessária.

Esta é uma breve descrição dos exemplos mais comuns de tais objetos:

- ***Arquivos ocultos*** - por padrão, arquivos ocultos não são visíveis no Windows, e alguns vírus ou outras ameaças podem tentar evitar sua detecção armazenando seus arquivos com esse atributo. Se o AVG relatar um arquivo oculto que você suspeita ser mal-intencionado, será possível removê-lo para a ***Quarentena de vírus do AVG***.

- ***Cookies*** - cookies são arquivos de texto não-formatado usados em sites para armazenar informações específicas do usuário, usadas posteriormente para carregar o layout personalizado do site, preencher o nome do usuário etc.

- ***Chaves do registro suspeitas*** - certos tipos de malware armazenam suas informações no registro do Windows, para garantir o seu carregamento na inicialização ou ampliar seu efeito no sistema operacional.

12.7.5. Guia Rootkits

A guia ***Rootkits*** exibe informações sobre rootkits detectados durante a verificação caso você tenha iniciado a ***Verificação Anti-Rootkit***.

Um rootkit é um programa criado para assumir o controle fundamental de um sistema de computador, sem autorização dos proprietários do sistema e gerentes legítimos.*** O acesso ao hardware é realmente necessário, pois um rootkit tem o objetivo de executar o controle do sistema operacional executado no hardware. Geralmente, os rootkits atuam para obscurecer sua presença no sistema por meio de subversão ou evasão de mecanismos de segurança padrão do sistema operacional. Freqüentemente, eles também são cavalos-de-tróia, levando os usuários a acreditarem que é confiável executá-los no sistema. As técnicas usadas para conseguir isso podem incluir ocultar processos em execução de programas de monitoramento ou ocultar arquivos ou dados do sistema operacional.

A estrutura dessa guia é basicamente a mesma que a da ***guia Infecções*** ou da ***guia Spyware***.

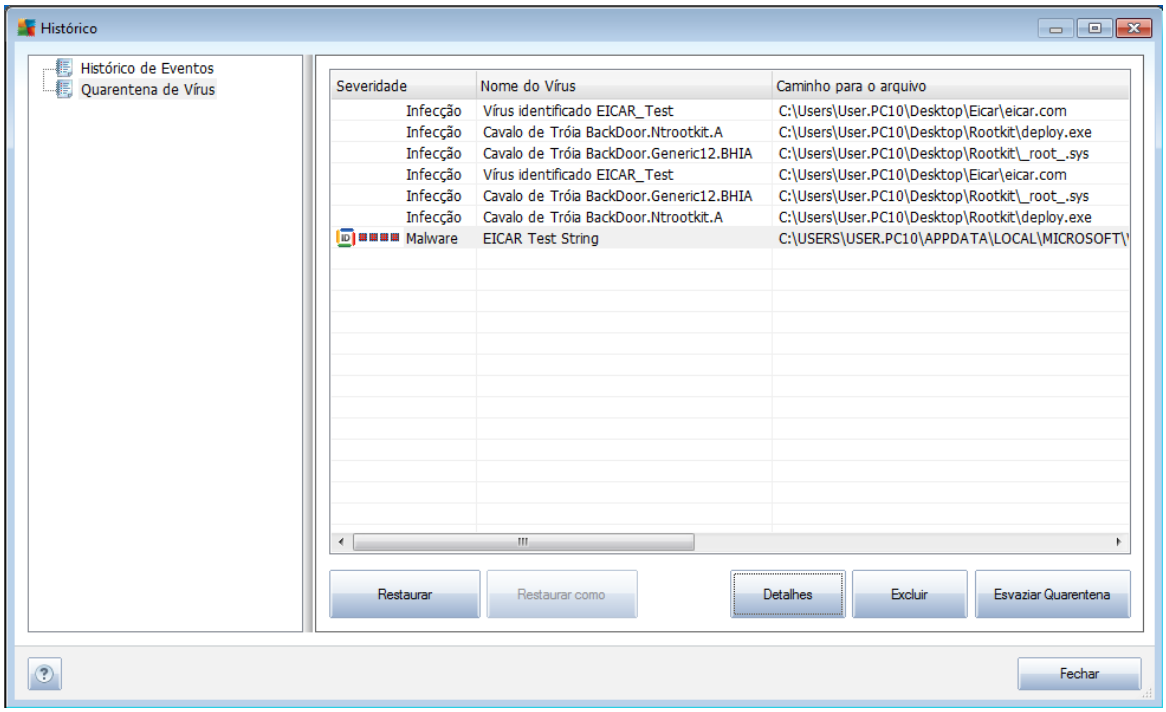
12.7.6. Guia Informações

A guia ***Informações*** contém dados como "descobertas" que não podem ser categorizadas como infecções, spyware etc. Elas também não podem ser rotuladas positivamente como perigosas, mas merecem a sua atenção. A verificação do AVG pode detectar arquivos que talvez não estejam infectados, mas que são suspeitos. Esses arquivos são indicados como ***Aviso*** ou como ***Informações***.

As ***Informações*** sobre severidade podem ser reportadas por um dos seguintes motivos:

- ***Compactado em tempo de execução*** - o arquivo foi compactado com um dos compactadores menos comuns, o que pode indicar uma tentativa de impedir a verificação desse arquivo. Entretanto, nem todos os relatórios de tal arquivo indica um vírus.
- ***Compactado em tempo de execução com recorrência*** - semelhante ao problema acima, mas menos freqüente entre os softwares comuns. Esses arquivos são suspeitos e convém considerar sua remoção ou envio para análise.
- ***Arquivamento ou documento protegido por senha*** - arquivos protegidos por senha não podem ser verificados pelo AVG (*ou em geral por qualquer outro programa anti-malware*).
- ***Documento com macros*** - o documento relatado contém macros, que podem ser mal-intencionadas.
- ***Extensão oculta*** - arquivos com extensão oculta podem parecer ser, por exemplo, imagens, quando na verdade são arquivos executáveis (*por exemplo, imagem.jpg.exe*). A segunda extensão não está visível no Windows por padrão, e o AVG relata esses arquivos para evitar a abertura acidental.
- ***Caminho de arquivo impróprio*** - se algum arquivo do sistema importante estiver em execução a partir de um caminho diferente do padrão (*por exemplo, winlogon.exe em execução a partir de um caminho diferente da pasta Windows*), o AVG irá relatar essa discrepância. Em alguns casos, vírus usam nomes de processos padrão do sistema para tornar sua presença menos aparente no sistema.
- ***Arquivo bloqueado*** - o arquivo relatado está bloqueado, e por isso não pode ser verificado pelo AVG. Isso normalmente significa que algum arquivo é&; constantemente utilizado pelo sistema (*por exemplo, arquivo swap*).

12.8. Quarentena de vírus



A Quarentena de vírus é um ambiente seguro para o gerenciamento de objetos suspeitos ou infectados detectados durante os testes do AVG. Depois que um objeto infectado for detectado durante a verificação e o AVG não puder repará-lo automaticamente, você será solicitado a decidir o que deve ser feito com o objeto suspeito. A solução recomendável é movê-lo para a ***Quarentena de Vírus*** para futuro tratamento. O principal objetivo da Quarentena de Vírus é conservar qualquer arquivo excluído por um certo período de tempo para que você tenha certeza de que não precisa mais dele em seu local original. Se você descobrir que a ausência de arquivos causa problemas, pode enviar o arquivo em questão para análise ou restaurá-lo para o local original.

A interface da ***Quarentena de Vírus*** é aberta em uma janela separada e oferece uma visão geral das informações de objetos infectados em quarentena:

- ***Severidade*** - especifica o tipo de infecção (*baseado em seu nível de infecção - todos os objetos listados podem estar positivamente ou potencialmente infectados*)
- ***Nome do vírus*** - especifica o nome da infecção detectada de acordo com a ***Enciclopédia de vírus*** (online)
- ***Caminho para o arquivo*** - caminho completo para o local original do arquivo infectado detectado
- ***Nome original do objeto*** - todos os objetos detectados listados na tabela foram rotulados com o nome padrão dado pelo AVG durante o processo de

verificação. No caso de o objeto ter tido um nome original que é conhecido (*por ex., o nome de um anexo de e-mail que não corresponda ao conteúdo real do anexo*), ele será fornecido nesta coluna.

- ***Data do armazenamento*** - data e hora que o arquivo suspeito foi detectado e armazenado na ***Quarentena de vírus***

Botões de controle

Os botões de controle a seguir podem ser acessados na interface da ***Quarentena de vírus***:

- ***Restaurar*** - remove o arquivo infectado de volta ao local original do disco
- ***Restaurar como*** - caso você decida mover o objeto infectado detectado da ***Quarentena de vírus*** para uma pasta selecionada, use este botão. O objeto suspeito e detectado será salvo com o nome original. Caso o nome original não seja conhecido, será usado o nome padrão.
- ***Excluir*** - remove de maneira completa e irreversível o arquivo infectado da ***Quarentena***
- ***Esvaziar a Quarentena*** - remove completamente todo o conteúdo da ***Quarentena de Vírus*** Removendo os arquivos da ***Quarentena***, esses arquivos serão removidos de modo irreversível do disco (*e não para a Lixeira*).

13. Atualizações do AVG

Manter o AVG atualizado é fundamental para garantir que todos os vírus recém-descobertos sejam detectados o mais rapidamente possível.

Como as atualizações do AVG não são lançadas de acordo com programações fixas, mas de acordo com o volume e a gravidade das novas ameaças, recomenda-se verificar as novas atualizações pelo menos uma vez ao dia ou com frequência ainda maior. Somente dessa forma você pode ter a certeza de que o seu **AVG Email Server Edition 2011** é mantido atualizado também durante o dia.

13.1. Níveis de atualização

O AVG oferece dois níveis de atualização à sua escolha:

- ***As definições de atualização*** contêm as alterações necessárias para a proteção antivírus confiável. Em geral, não inclui nenhuma alteração no código e atualiza apenas o banco de dados de definições. Essa atualização deverá ser aplicada assim que estiver disponível.

- ***A atualização do programa*** contém várias alterações, correções e aperfeiçoamentos para o programa.

Ao programar uma atualização, é possível selecionar o nível de prioridade a ser baixado e aplicado.

Observação: *se ocorrer uma coincidência de tempo de uma atualização de programa agendada e uma verificação agendada, o processo de atualização terá maior prioridade, e a verificação será interrompida.*

13.2. Tipos de atualização

Você pode distinguir entre dois tipos de atualização:

- ***A atualização sob demanda*** é uma atualização imediata do AVG que pode ser executada a qualquer momento que surgir a necessidade.

- ***Atualização programada*** - no AVG, também é possível predefinir um plano de atualização. A atualização planejada, então, será executada periodicamente, de acordo com a definição da configuração. Sempre que forem apresentados novos arquivos de atualização no local especificado, eles serão baixados diretamente da Internet ou do diretório da rede. Quando nenhuma atualização está disponível, nada acontece.

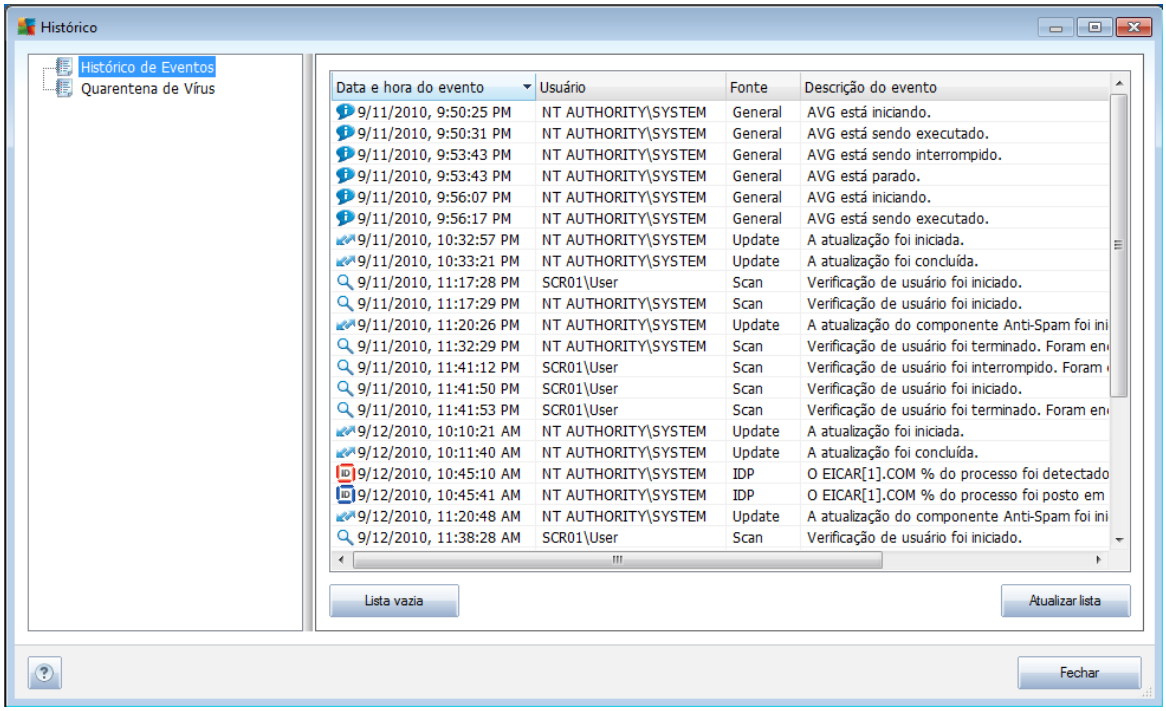
13.3. Processo de atualização

O processo de atualização pode ser inicializado imediatamente, conforme a necessidade surge, pelo link rápido ***Atualizar agora***. Esse link está disponível sempre em qualquer caixa de diálogo da Interface do usuário do AVG . Entretanto, é altamente recomendável realizar atualizações regularmente, conforme informado no programa de atualização editável com o componente Gerenciador de Atualizações.

Quando você inicia a atualização, o AVG primeiro verifica se há novos arquivos de atualização disponíveis. Se houver, o AVG inicia o download e inicializa o processo de atualização propriamente dito. Durante o processo de atualização, você será redirecionado para a interface ***Atualizar*** , onde poderá ver o andamento do processo em uma representação gráfica, bem como obter uma visão geral dos parâmetros estatísticos relevantes (*tamanho do arquivo de atualização, dados recebidos, velocidade de download, tempo decorrido etc.*).

***Nota**: Antes do início da atualização do programa AVG é criado um ponto de restauração. No caso de falha no processo de atualização e seu sistema operacional, você pode restaurar o seu SO para a configuração original deste ponto. Esta opção está disponível em Iniciar / Todos os Programas / Acessórios / Ferramentas do Sistema / Restauração do Sistema. Recomendável apenas para usuários experientes!*

14. Histórico de eventos



A caixa de diálogo ***Histórico*** pode ser acessada no menu do sistema por meio do item ***Histórico/Log do Histórico de Eventos***. Nesta caixa de diálogo, você encontrará um resumo dos eventos importantes que ocorreram durante a operação do AVG Email Server Edition 2011**.** ***Histórico*** registra os seguintes tipos de eventos:

- Informações sobre atualizações do aplicativo AVG
- Início, fim ou interrupção de verificações (*inclusive testes executados automaticamente*)
- Eventos associados à detecção de vírus (*pela Proteção Residente ou verificação*), incluindo o local de ocorrência
- Outros eventos importantes

Para cada evento, as seguintes informações são listadas:

- ***Data e hora do evento*** fornece a data e a hora exata em que o evento ocorreu
- ***Usuário*** declara quem iniciou o evento
- ***Origem*** fornece o componente de origem ou a outra parte do sistema AVG que disparou o evento

- ***Descrição do evento*** fornece um breve resumo do que realmente aconteceu

Botões de controle

- ***Esvaziar lista*** - exclui todas as entradas da lista dos eventos
- ***Atualizar lista*** - atualiza todas as entradas da lista dos eventos

15. Perguntas Freqüentes e Suporte Técnico

Se você tiver algum problema com o seu AVG, seja comercial ou técnico, consulte a seção ***Perguntas freqüentes*** do site da AVG (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***.