

# Avira Premium Security Suite

Manual do usuário

## Marcas comerciais e direitos autorais

### Marcas comerciais

AntiVir é uma marca registrada da Avira GmbH.

Windows é uma marca registrada da Microsoft Corporation nos Estados Unidos e em outros países.

Todas as outras marcas e nomes de produtos são marcas comerciais ou marcas registradas da empresa de seus respectivos proprietários.

As marcas comerciais protegidas não são marcadas como tal neste manual. No entanto, isso não significa que elas podem ser usadas livremente.

### Informações sobre direitos autorais

Um código fornecido por terceiros foi usado para o Avira Premium Security Suite. Agradecemos os detentores dos direitos autorais por disponibilizar o código para nós. Para obter informações detalhadas sobre direitos autorais, consulte a seção Licenças de terceiros da ajuda do Avira Premium Security Suite.

# Conteúdo

<b>1</b>	<b>Introdução .....</b>	<b>1</b>
<b>2</b>	<b>Ícones e ênfases .....</b>	<b>2</b>
<b>3</b>	<b>Informações do produto.....</b>	<b>3</b>
3.1	Escopo da entrega.....	3
3.2	Requisitos do sistema.....	4
3.3	Licença e atualização .....	5
<b>4</b>	<b>Instalação e desinstalação.....</b>	<b>6</b>
4.1	Instalação .....	6
4.2	Alterar instalação.....	12
4.3	Módulos de instalação .....	12
4.4	Desinstalação .....	13
<b>5</b>	<b>Visão geral do Premium Security Suite .....</b>	<b>15</b>
5.1	Interface de usuário e operação .....	15
5.1.1	Centro de controle .....	15
5.1.2	Configuração .....	18
5.1.3	Ícone de bandeja.....	21
5.2	Como...?.....	22
5.2.1	Ativar produto.....	22
5.2.2	Executar atualização automática.....	23
5.2.3	Iniciar uma atualização manual.....	24
5.2.4	Verificação sob demanda: Uso de um perfil de verificação para verificar a presença de vírus e malwares .....	25
5.2.5	Verificação sob demanda: Verificar presença de vírus e malwares com o método de arrastar e soltar .....	26
5.2.6	Verificação sob demanda: Verificar presença de vírus e malwares através do menu de contexto .....	27
5.2.7	Verificação sob demanda: Verificar presença de vírus e malwares automaticamente.....	27
5.2.8	Verificação sob demanda: Verificação direcionada de rootkits e malware ativo .....	28
5.2.9	Reação aos vírus e malwares detectados.....	29
5.2.10	Quarentena: Manipulação de arquivos em quarentena (*.qua) .....	33
5.2.11	Quarentena: Restaurar os arquivos em quarentena.....	34
5.2.12	Quarentena: Mover arquivos suspeitos para quarentena.....	35
5.2.13	Perfil da verificação: Corrigir ou excluir tipo de arquivo em um perfil de verificação .....	36
5.2.14	Perfil da verificação: Criar atalho na área de trabalho para o perfil de verificação.....	36
5.2.15	Eventos: Filtrar eventos.....	37
5.2.16	MailGuard: Excluir endereços de e-mail da verificação.....	37
5.2.17	MailGuard: Treinar o módulo antispam .....	38
5.2.18	FireWall: Selecionar o nível de segurança para o FireWall.....	38
5.2.19	Backup: Criar backups manualmente.....	39
5.2.20	Backup: Criar backups de dados automáticos.....	40

<b>6</b>	<b>Scanner</b> .....	<b>44</b>
<b>7</b>	<b>Atualizações</b> .....	<b>45</b>
<b>8</b>	<b>Avira FireWall :: Visão geral</b> .....	<b>46</b>
<b>9</b>	<b>Backup</b> .....	<b>48</b>
<b>10</b>	<b>Perguntas frequentes, dicas</b> .....	<b>49</b>
	10.1 Ajuda caso ocorra um problema.....	49
	10.2 Atalhos .....	53
	10.2.1 Nas caixas de diálogo .....	53
	10.2.2 Na ajuda.....	54
	10.2.3 No Centro de controle .....	54
	10.3 Central de segurança do Windows.....	56
	10.3.1 Geral .....	56
	10.3.2 A Central de segurança do Windows e o programa AntiVir.....	56
<b>11</b>	<b>Vírus e mais</b> .....	<b>59</b>
	11.1 Categorias de ameaça estendidas.....	59
	11.2 Vírus e outros malwares .....	62
<b>12</b>	<b>Informações e serviço</b> .....	<b>65</b>
	12.1 Endereço de contato .....	65
	12.2 Suporte técnico .....	65
	12.3 Arquivo suspeito .....	65
	12.4 Registrando falso-positivos.....	66
	12.5 Seus comentários para mais segurança .....	66
<b>13</b>	<b>Referência: opções de configuração</b> .....	<b>67</b>
	13.1 Scanner.....	67
	13.1.1 Fazer verificação.....	67
	13.1.1.1 Ação para detecção.....	70
	13.1.1.2 Exceções.....	72
	13.1.1.3 Heurística .....	73
	13.1.2 Relatório .....	74
	13.2 Guard.....	75
	13.2.1 Fazer verificação.....	75
	13.2.1.1 Ação para detecção.....	77
	13.2.1.2 Mais ações .....	79
	13.2.1.3 Exceções.....	79
	13.2.1.4 Heurística .....	83
	13.2.2 ProActiv .....	84
	13.2.2.1 Filtro de aplicativos: Aplicativos a serem bloqueados.....	85
	13.2.2.2 Filtro de aplicativos: Aplicativos permitidos .....	85
	13.2.3 Relatório .....	86
	13.3 MailGuard .....	87
	13.3.1 Fazer verificação.....	88
	13.3.1.1 Ação para detecção.....	89
	13.3.1.2 Outras ações .....	90
	13.3.1.3 Heurística .....	90
	13.3.1.4 AntiBot .....	91
	13.3.2 Geral .....	92
	13.3.2.1 Exceções.....	92
	13.3.2.2 Cache .....	94

13.3.2.3.	MailGuard .....	95
13.3.2.4.	Rodapé.....	96
13.3.3	Relatório .....	96
13.4	Firewall.....	97
13.4.1	Regras do adaptador .....	97
13.4.1.1.	Regras de entrada.....	100
13.4.1.2.	Regras de saída.....	107
13.4.2	Regras de aplicativo .....	108
13.4.3	Fornecedores confiáveis .....	110
13.4.4	Configurações.....	111
13.4.5	Configurações de pop-up .....	113
13.5	WebGuard .....	114
13.5.1	Fazer verificação.....	114
13.5.1.1.	Ação para deteção.....	115
13.5.1.2.	Solicitações bloqueadas .....	116
13.5.1.3.	Exceções.....	118
13.5.1.4.	Heurística .....	120
13.5.2	Relatório .....	121
13.6	Controles parentais .....	122
13.7	Backup.....	124
13.7.1	Configurações.....	124
13.7.2	Exceções.....	125
13.7.3	Relatório .....	127
13.8	Atualizar.....	127
13.8.1	Iniciar atualização do produto.....	128
13.8.2	Reiniciar configurações.....	129
13.9	Geral .....	130
13.9.1	Categorias de ameaça .....	130
13.9.2	Senha .....	131
13.9.3	Segurança .....	133
13.9.4	WMI.....	134
13.9.5	Proxy.....	134
13.9.6	Diretórios .....	135
13.9.7	Eventos .....	136
13.9.8	Limitar relatórios.....	136
13.9.9	Alertas acústicos.....	136
13.9.10	Avisos.....	137

# 1 Introdução

O programa AntiVir protege seu computador contra vírus, worms, cavalos de Troia, adwares, spywares e outros perigos. Neste manual, esses programas são chamados de vírus ou malware (software prejudicial) e programas mal-intencionados.

O manual descreve a instalação e a operação do programa.

Para obter mais opções e informações, visite nosso site:

<http://www.avira.pt>

No site [www.avira.com](http://www.avira.com), você pode...

- acessar informações sobre outros programas de desktop do AntiVir
- baixar os programas de desktop do AntiVir mais recentes
- baixar os manuais de produto mais recentes no formato PDF
- baixar as ferramentas gratuitas de suporte e reparo:
- acessar nosso abrangente banco de dados de conhecimento e perguntas frequentes para solucionar problemas
- acessar endereços de suporte específicos para outros países.

Equipe Avira

## 2 Ícones e ênfases

Os seguintes ícones são usados:

<b>Ícone/designação</b>	<b>Explicação</b>
✓	Colocado antes de uma condição que deve ser cumprida antes da execução de uma ação.
▶	Colocado antes de uma etapa de ação executada por você.
→	Colocado antes de um evento que segue a ação anterior.
<b>Aviso</b>	Colocado antes de um aviso de perigo de perda de dados críticos.
<b>Nota</b>	Colocado antes de um link para informações especialmente importantes ou uma dica que facilita o uso do programa AntiVir.

As seguintes ênfases são usadas:

<b>Ênfase</b>	<b>Explicação</b>
<i>Cursivo</i>	Dados do nome de arquivo ou do caminho.
	Elementos exibidos da interface do software (por exemplo, título da janela, campo da janela ou caixa de opções).
<b>Negrito</b>	Elementos clicados na interface do software (por exemplo, item de menu, seção ou botão).

## 3 Informações do produto

Este capítulo contém todas as informações relevantes para a compra e o uso do produto AntiVir:

- consulte o Capítulo: Escopo da entrega
- consulte o Capítulo: Requisitos do sistema
- consulte o Capítulo: Licenciamento
- consulte o Capítulo: Gerenciador de licença do

Os programas AntiVir são ferramentas abrangentes e flexíveis que protegem seu computador contra vírus, malwares, programas indesejados e outros perigos.

► Observe estas informações:

### **Nota**

A perda de dados valiosos normalmente tem consequências dramáticas. Até mesmo o melhor programa de proteção contra vírus não pode fornecer proteção total contra a perda de dados. Faça cópias regularmente (backups) de seus dados por motivos de segurança.

### **Nota**

Um programa só pode fornecer proteção confiável e eficiente contra vírus, malwares, programas indesejados e outros perigos se estiver atualizado. Verifique se o programa AntiVir está atualizado com atualizações automáticas. Configure o programa conforme necessário.

### 3.1 Escopo da entrega

O programa AntiVir fornece as seguintes funções:

- Centro de controle para monitorar, gerenciar e controlar o programa inteiro
- Configuração centralizada com opções padrão e avançadas amigáveis e ajuda contextual
- Scanner (verificação por demanda) com verificação configurável e controlada por perfis de todos os tipos conhecidos de vírus e malware
- A integração no Controle de Conta de Usuário do Windows Vista permite que você realize tarefas que exigem direitos de administrador.
- Guard (verificação por acesso) para o monitoramento contínuo de todas as tentativas de acesso a arquivos
- Componente ProActiv para o monitoramento permanente das ações do programa (apenas para sistemas de 32 bits, não disponível no Windows 2000)
- MailGuard (Scanner de POP3, IMAP e SMTP) para a verificação constante de emails em busca de vírus e malware. Os anexos de e-mail também são verificados
- WebGuard para monitorar dados e arquivos transferidos da Internet usando o protocolo HTTP (monitoramento das portas 80, 8080, 3128)



- Componente de controle dos pais para filtragem baseada em função de sites indesejados e limitação de uso da Internet
- Componente Backup para criar backups de seus dados (backups espelhados)
- Gerenciamento de quarentena integrado para isolar e processar arquivos suspeitos
- Proteção contra rootkits para detectar malware oculto instalado no sistema do seu computador (rootkits)  
(Não disponível no Windows XP de 64 bits)
- Acesso direto a informações detalhadas sobre vírus e malwares detectados via Internet
- Atualizações simples e rápidas do programa, das definições de vírus e do mecanismo de pesquisa através da Atualização de um único arquivo e de atualizações incrementais do VDF por meio de um servidor da Web na Internet
- Licenciamento amigável no Gerenciador de licença
- Programador integrado para planejar trabalhos individuais ou recorrentes, como atualizações ou verificações
- Altíssima taxa de detecção de vírus e malware com uma inovadora tecnologia de verificação (mecanismo de verificação), incluindo o método de verificação heurística
- Detecção de todos os tipos convencionais de arquivos, inclusive detecção de arquivos aninhados e detecção inteligente de extensões
- Função de multithreading de alto desempenho (verificação simultânea de vários arquivos em alta velocidade)
- AntiVir FireWall para proteger seu computador contra o acesso não autorizado da Internet ou de outra rede e contra o acesso não autorizado da Internet/rede por usuários não autorizados.

### 3.2 Requisitos do sistema

Os requisitos do sistema são os seguintes:

- Computador Pentium ou superior, com pelo menos 266 MHz
- Sistema operacional
- Windows XP, SP2 (32 ou 64 bits) ou
- Windows Vista (32 ou 64 bits, SP 1)
- Windows 7 (32 ou 64 bits)
- Pelo menos 150 MB de espaço livre no disco rígido (mais se a quarentena for usada para armazenamento temporário)
- Pelo menos 256 MB de RAM no Windows XP
- Pelo menos 1024 MB de RAM no Windows Vista, Windows 7
- Para a instalação do programa: direitos de administrador
- Para todas as instalações: Windows Internet Explorer 6.0 ou superior
- Conexão com a Internet se apropriado (consulte Instalação)

### 3.3 Licença e atualização

Para poder usar o produto AntiVir, você precisa de uma licença. Você aceita os termos de licença por meio desse processo.

A licença é fornecida na forma de uma chave de ativação. A chave de ativação é um código de letras e números que você receberá depois de adquirir o produto AntiVir. A chave de ativação contém os dados exatos de sua licença, isto é, os programas que foram licenciados e por quanto tempo.

A chave de ativação será enviada a você por e-mail, se tiver adquirido o programa AntiVir na Internet ou estará na embalagem do produto.

Para licenciar seu programa, insira sua chave de ativação para ativar o programa. A ativação do produto pode ser executada durante a instalação. No entanto, você também pode ativar o programa AntiVir após a instalação no Gerenciador de licenças, em Ajuda::Gerenciamento de licenças.

No Gerenciador de licenças, você tem a opção de iniciar uma atualização para um produto da família de produtos de desktop do AntiVir. A desinstalação manual do produto antigo e a instalação manual do novo produto não são necessárias. Ao fazer uma atualização usando o Gerenciador de licenças, insira o código de ativação para o produto que deseja atualizar na caixa de entrada Gerenciador de licenças. O novo produto é instalado automaticamente.

As seguintes atualizações do produto podem ser executadas automaticamente por meio do Gerenciador de licenças:

- Atualização do Avira AntiVir Personal para o Avira AntiVir Premium
- Atualização do Avira AntiVir Personal para o Avira Premium Security Suite
- Atualização do Avira AntiVir Premium para o Avira Premium Security Suite

## 4 Instalação e desinstalação

Este capítulo contém informações relacionadas à instalação e desinstalação do programa AntiVir.

- consulte o Capítulo Instalação: condições, tipos de instalação, instalação
- consulte o Capítulo Módulos de instalação
- consulte o Capítulo Instalação de modificação
- consulte o Capítulo Desinstalação: Desinstalar

### 4.1 Instalação

Antes da instalação, verifique se o computador satisfaz todos os requisitos mínimos de sistema. Se o computador satisfizer todos os requisitos, você poderá instalar o programa AntiVir.

#### **Nota**

Durante o processo de instalação, você poderá criar um ponto de restauração. Uma das finalidades do ponto de restauração é redefinir o sistema operacional para o seu status de pré-instalação. Se desejar usar essa opção, verifique se o sistema operacional permite a criação de um ponto de restauração:

Windows XP: Propriedades do sistema -> Restauração do sistema: Desative a opção

**Desativar restauração do sistema.**

Windows Vista/Windows 7: Propriedades do sistema -> Proteção do computador: Na área **Configurações de proteção**, realce a unidade na qual o sistema está instalado e clique no botão **Configurar**. Na janela **Proteção do sistema**, ative a opção

**Configurações do sistema e restauração das versões do arquivo anterior.**

#### **Tipos de instalação**

Durante a instalação, você pode escolher um tipo de instalação no assistente:

##### **Expresso**

- Nem todos os componentes do programa são instalados. Os componentes a seguir não são instalados:

Avira AntiVir ProActiv

Avira FireWall

- Os arquivos do programa são instalados em uma pasta padrão específica em C:\Arquivos de programas.
- O programa AntiVir é completamente instalado com as configurações padrão. Você tem a opção de definir configurações personalizadas usando o assistente de configuração.

##### **Definido pelo usuário**

- Você pode optar por instalar componentes individuais do programa (consulte o Capítulo Instalação e desinstalação::Módulos de instalação).

- Uma pasta de destino pode ser selecionada para os arquivos de programa a serem instalados.
- Você pode desativar Criar um ícone na área de trabalho e um grupo de programa no menu Iniciar.
- Usando o assistente de configuração, você pode definir configurações personalizadas para o programa AntiVir e inicia uma verificação rápida do sistema que é executada automaticamente após a instalação.

### Antes de começar a instalação

- ▶ Feche seu programa de e-mail. Também é recomendado encerrar todos os aplicativos em execução.
- ▶ Verifique se nenhuma outra solução de proteção contra vírus está instalada. As funções de proteção automática de várias soluções de segurança podem interferir uma na outra.
- ▶ Estabeleça uma conexão com a Internet: a conexão com a Internet é necessária para realizar as seguintes etapas de instalação:
- ▶ Download do arquivo de programa e do mecanismo de verificação atuais, e dos arquivos de definição de vírus mais recentes através do programa de instalação (para instalação baseada na Internet)
- ▶ Ativação do programa
- ▶ Quando apropriado, realize uma atualização após o término da instalação
- ▶ Tenha a chave de licença do programa AntiVir em mãos quando desejar ativar o programa.

### Nota

Instalação baseada na Internet:

Um programa de instalação é fornecido para a instalação do programa baseada na Internet. Esse programa carrega o arquivo do programa atual antes da instalação realizada pelos servidores da Web da Avira GmbH. Esse processo garante que o programa AntiVir seja instalado com o arquivo de definição de vírus mais recente.

Instalação com um pacote de instalação:

O pacote de instalação contém o programa de instalação e todos os arquivos de programa necessários. Nenhuma seleção de idioma para o programa AntiVir está disponível para a instalação feita com um pacote. Recomendamos que você realize uma atualização do arquivo de definição de vírus após a instalação.

### Observação

Para a ativação do produto, o programa AntiVir usa o protocolo HTTP e a porta 80 (comunicação da Web), bem como o protocolo de criptografia SSL e a porta 443 para se comunicar com os servidores da Avira GmbH. Se estiver usando um firewall, verifique se as conexões e/ou os dados de entrada ou saída necessários não estão bloqueados pelo firewall.

### Instalar

O programa de instalação é executado no modo com caixas de diálogo autoexplicativas. Cada janela contém alguns botões para controlar o processo de instalação.

Os botões mais importantes têm as seguintes funções:

- **OK:** confirma a ação.

- **Anular:** anula a ação.
- **Avançar:** vai para a próxima etapa.
- **Voltar:** vai para a etapa anterior.

Instalação do programa AntiVir:

### **Nota**

As ações a seguir para desativar o Windows FireWall aplicam-se apenas ao sistema operacional Windows XP.

- ▶ Inicie o programa de instalação clicando duas vezes no arquivo de instalação baixado da Internet ou insira o CD do programa.

### **Instalação baseada na Internet**

A caixa de diálogo *Bem-vindo...* é exibida.

- ▶ Clique em **Avançar** para continuar a instalação.

A caixa de diálogo *Seleção de idioma* é exibida.

- ▶ Selecione o idioma que deseja usar para instalar o programa AntiVir e confirme a seleção do idioma clicando em **Avançar**.

A caixa de diálogo *Download* é exibida. Todos os arquivos necessários para a instalação são baixados dos servidores da Web da Avira GmbH. A janela *Download* fecha quando o download termina.

### **Instalação com um pacote de instalação**

O assistente de instalação é aberto com a caixa de diálogo *Avira Premium Security Suite*.

- ▶ Clique em *Aceitar* para iniciar a instalação.

O arquivo de instalação é extraído. A rotina de instalação é iniciada.

A caixa de diálogo *Bem-vindo...* é exibida.

- ▶ Clique em **Avançar**.

### **Continuação da instalação baseada na Internet e da instalação com um pacote de instalação**

A caixa de diálogo com o contrato de licença é exibida.

- ▶ Confirme que você aceita o contrato de licença e clique em **Avançar**.

A caixa de diálogo *Gerar número de série* é exibida.

- ▶ Quando apropriado, confirme que um número de série aleatório foi gerado e transmitido durante a atualização e clique em **Avançar**.

A caixa de diálogo *Selecionar tipo de instalação* é exibida.

- ▶ Ative a opção **Expresso** ou **Definido pelo usuário**. Se desejar criar um ponto de restauração, ative a opção **Criar ponto de restauração do sistema**. Clique em **Avançar** para confirmar as configurações.

### **Instalação definida pelo usuário**

A caixa de diálogo *Selecionar diretório de destino* é exibida.

- ▶ Confirme o diretório de destino especificado clicando em **Avançar**.

- OU -

Use o botão **Procurar** para selecionar um diretório de destino diferente e confirme clicando em **Avançar**.

A caixa de diálogo *Instalar componentes* é exibida:

- ▶ Ative ou desative os componentes necessários e confirme clicando em **Avançar**.

Se você optou por instalar o componente ProActiv, a janela da *comunidade do Avira AntiVir ProActiv* será exibida. Você pode confirmar a participação na comunidade do Avira AntiVir ProActiv: Se essa opção estiver ativada, o Avira AntiVir ProActiv enviará dados de programas suspeitos detectados pelo componente ProActiv para o Centro de pesquisa de malware da Avira. Os dados são usados somente em uma verificação on-line avançada e para expandir e refinar a tecnologia de detecção. Você pode usar o link com **outras informações** para obter mais detalhes sobre a verificação on-line expandida.

- ▶ Ative e desative a participação na comunidade do AntiVir ProActiv e confirme clicando em **Avançar**.

Na próxima caixa de diálogo, você pode decidir se deseja criar um atalho na área de trabalho e/ou um grupo de programa no menu Iniciar.

- ▶ Clique em **Avançar**.
- ▶ Passe para a próxima seção, "Instalação expressa".

### **Instalação expressa**

A janela da *comunidade do AntiVir ProActiv* é exibida. Você pode confirmar a participação na comunidade do Avira AntiVir ProActiv: Se essa opção estiver ativada, o Avira AntiVir ProActiv enviará dados de programas suspeitos detectados pelo componente ProActiv para o Centro de pesquisa de malware da Avira. Os dados são usados somente em uma verificação on-line avançada e para expandir e refinar a tecnologia de detecção. Você pode usar o link com **outras informações** para obter mais detalhes sobre a verificação on-line expandida.

- ▶ Ative e desative a participação na comunidade do AntiVir ProActiv e confirme clicando em **Avançar**.

### **Continuar: Instalação expressa e instalação definida pelo usuário**

O assistente de licença é aberto.

Você tem as seguintes opções para ativar o programa.

- Insira uma chave de ativação.  
Quando a chave de ativação é inserida, o programa AntiVir é ativado com sua licença.
- Selecione a opção **Teste do produto**  
Se você selecionar **Teste do produto**, uma licença de avaliação para ativar o programa será gerada durante o processo de ativação. Você pode testar o programa AntiVir com todas as funções por um tempo limitado.

### **Observação**

Ao usar a opção **Arquivo de licença hbedv.key válido disponível**, você pode carregar um arquivo de licença válido. Durante a ativação do produto com uma chave de ativação válida, a chave de licença é gerada e salva no diretório do programa AntiVir. Use essa opção se já tiver ativado um produto e quiser reinstalar o programa AntiVir.

### **Observação**

Em algumas versões vendidas dos produtos AntiVir, uma chave de ativação já é incluída no produto. Por esse motivo, a chave não precisa ser inserida. Se e quando necessário, a chave de ativação é exibida no assistente de licença.

### **Observação**

Para ativar o programa, é estabelecida uma conexão com os servidores da Avira GmbH. Em **Configurações de proxy**, é possível configurar a conexão com a Internet através de um servidor proxy.

- ▶ Selecione um processo de ativação e clique em **Avançar** para confirmar.

### Ativação do produto

Uma caixa de diálogo será aberta, na qual é possível inserir seus dados pessoais.

- ▶ Insira seus dados e clique em **Avançar**

Os dados são transmitidos para os servidores da Avira GmbH e, em seguida, verificados. O programa AntiVir é ativado por meio da licença.

Os dados de sua licença serão exibidos na próxima janela.

- ▶ Clique em **Avançar**.
- ▶ Passe para o próximo capítulo em "Ativar selecionando a opção **hbedv.key válido disponível**".

### Selecione a opção "hbedv.key válido disponível"

Uma caixa será aberta para carregar o arquivo de licença.

- ▶ Selecione o arquivo de licença hbedv.key com os dados de sua licença do programa e clique em **Abrir**

Os dados de sua licença serão exibidos na próxima janela.

- ▶ Clique em **Avançar**

### Continuação após o término da ativação ou o carregamento do arquivo de licença

Os recursos do programa serão instalados. O progresso da instalação é exibido na caixa de diálogo.

Na caixa de diálogo a seguir, você pode escolher se deseja abrir o arquivo Leiam e se deseja reiniciar seu computador.

- ▶ Aceite se apropriado e conclua a instalação clicando em *Concluir*.

O assistente de instalação é fechado.

### Continuar: Instalação definida pelo usuário Assistente de configuração

Se você escolher a instalação definida pelo usuário, a etapa a seguir é aberta no assistente de configuração. O assistente de configuração permite que você defina configurações personalizadas para o programa AntiVir.

- ▶ Clique em **Avançar** na janela de boas-vindas do assistente de configuração para iniciar a configuração do programa.

A caixa de diálogo *Configurar a AHeAD* permite selecionar um nível de detecção para a tecnologia AHeAD. O nível de detecção selecionado é usado para as configurações da tecnologia AHeAD do Scanner (verificação sob demanda) e do Guard (verificação de acesso).

- ▶ Selecione um nível de detecção e continue a instalação clicando em **Avançar**.

Na próxima caixa de diálogo, *Selecionar categorias de ameaça estendidas*, você pode adaptar as funções de proteção do programa AntiVir para as categorias de ameaça especificadas.

- ▶ Quando apropriado, ative outras categorias de ameaça e continue a instalação clicando em *Avançar*.

Se você selecionou o módulo de instalação do AntiVir FireWall, a caixa de diálogo *Nível de segurança do fireWall* é exibida. Você pode definir se o Avira FireWall deve

permitir acesso externo para recursos ativados bem como o acesso à rede por aplicativos de empresas confiáveis.

- ▶ Ative as opções necessárias e continue a configuração clicando em *Avançar*.

Se você selecionou o módulo de instalação do AntiVir Guard, a caixa de diálogo *Modo de inicialização do Guard* é exibida. Você pode definir a hora de início do Guard. Em cada reinicialização do computador, o Guard será iniciado no modo de inicialização especificado.

### Nota

O modo de inicialização do Guard especificado é salvo no registro e não pode ser alterado na Configuração.

- ▶ Ative a opção necessária e continue a configuração clicando em *Avançar*.

Se você selecionou o módulo de instalação do AntiVir WebGuard, a caixa de diálogo *Ativar controles de pais* é exibida. Você pode definir a hora de início do Guard. Em cada reinicialização do computador, o Guard será iniciado no modo de inicialização especificado. Você tem a opção de atribuir diferentes funções – crianças, jovens, adultos – aos usuários do computador para o uso da Internet. Você pode desativar o controle dos pais.

- ▶ Defina as configurações de controle dos pais necessárias e continue a configuração clicando em *Avançar*.

Na caixa de diálogo *Atribuir senha* a seguir, você pode proteger com senha a Configuração contra acesso não autorizado. Isso é particularmente recomendado se o controle dos pais estiver ativado.

Na próxima caixa de diálogo, *Verificação do sistema*, é possível ativar ou desativar uma rápida verificação do sistema. Essa verificação é executada após a conclusão da configuração e antes da reinicialização do computador, e verifica a presença de vírus e malwares nos programas em execução e nos arquivos mais importantes do sistema.

- ▶ Ative ou desative a opção *Verificação curta do sistema* e continue a configuração clicando em *Avançar*.

Na próxima caixa de diálogo, você pode concluir a configuração clicando em *Concluir*

- ▶ Clique em *Concluir* para concluir a configuração.

As configurações especificadas e selecionadas são aceitas.

Se você tiver ativado a opção *Verificação curta do sistema*, a janela Luke Filewalker será aberta. O Scanner executa uma breve verificação no sistema.

### **Continuar: Instalação expressa e instalação definida pelo usuário**

Se você tiver selecionado a opção **Reiniciar computador**, no assistente de instalação final, o computador será reinicializado.

Depois da reinicialização do computador, o arquivo Leiam e é exibido, se você selecionou a opção **Mostrar Readme.txt** no assistente de instalação.

Após a instalação, recomendamos que você verifique se o programa está atualizado em Centro de controle em *Visão geral:: Status*.

- ▶ Quando apropriado, execute uma atualização para garantir que o arquivo de definição de vírus seja atualizado.
- ▶ Em seguida, realize uma verificação completa do sistema.



## 4.2 Alterar instalação

Você pode adicionar ou remover componentes individuais do programa da instalação atual do programa AntiVir (consulte o Capítulo Instalação e desinstalação::Módulos de instalação)

Se desejar adicionar ou remover módulos da instalação atual do, **você poderá usar a opção** Adicionar ou remover programas **no** Painel de controle do Windows **para** Alterar/remover programas.

Selecione o programa AntiVir e clique em **Alterar**. Na caixa de diálogo inicial do programa, selecione a opção **Modificar**. Você será orientado pelas alterações de instalação.

## 4.3 Módulos de instalação

Em uma instalação definida pelo usuário ou uma instalação de alteração, os módulos de instalação a seguir podem ser selecionados, adicionados ou removidos.

- **Premium Security Suite**  
Esse módulo contém todos os componentes necessários para uma instalação bem-sucedida do programa AntiVir.
- **AntiVir Guard**  
O AntiVir Guard é executado em segundo plano. Ele monitora e repara, se possível, os arquivos durante operações como abrir, gravar e copiar no modo de acesso. Sempre que o usuário realiza uma operação de arquivo (por exemplo, carregar documento, executar, copiar), o programa AntiVir verifica o arquivo automaticamente. A renomeação de um arquivo não aciona uma verificação do AntiVir Guard.
- **AntiVir ProActiv**  
O componente ProActiv monitora as ações do aplicativo e alerta os usuários quanto ao comportamento suspeito de aplicativo. Esse reconhecimento baseado em comportamento permite que você proteja você mesmo contra malware conhecido. O componente ProActiv é integrado ao AntiVir Guard.
- **AntiVir MailGuard**  
O MailGuard é a interface entre seu computador e o servidor de email do qual seu programa de email (cliente de email) baixa emails. O MailGuard é conectado como um proxy entre o programa e o servidor de email. Todos os e-mails recebidos passam por esse proxy, verificados quanto a vírus e programas indesejados e encaminhados ao seu programa de e-mail. Dependendo da configuração, o programa processa os e-mails afetados automaticamente ou solicita alguma ação para o usuário. Além disso, o MailGuard pode proteger você contra emails de spam de modo confiável.

### – **AntiVir WebGuard**

Ao navegar na Internet, você usa o navegador para solicitar dados de um servidor da Web. Os dados transferidos do servidor da Web (arquivos HTML, arquivos de script e de imagem, arquivos Flash, fluxos de vídeo e música etc.) em geral serão movidos diretamente no cache do navegador para serem exibidos no navegador, ou seja, uma verificação de acesso realizada pelo AntiVir Guard não é permitida. Isso poderia permitir o acesso de vírus e programas indesejado ao sistema do seu computador. O WebGuard é conhecido como um proxy HTTP que monitora as portas usadas para a transferência de dados (80, 8080, 3128) e verifica a presença de vírus e programas indesejados nos dados transferidos. Dependendo da configuração, o programa pode processar os arquivos afetados automaticamente ou solicitar uma ação específica para o usuário.

### – **Avira FireWall:**

O Avira FireWall controla a comunicação de entrada e saída do computador. Ele permite ou nega comunicações com base em políticas de segurança.

### – **AntiVir Rootkit Protection**

O AntiVir Rootkit Protection verifica se o software já está instalado no computador que não pode mais ser detectado com métodos convencionais de proteção contra malware após invadir o sistema no computador.

### – **Extensão Shell**

A extensão do Shell gera a entrada 'Verificar os arquivos selecionados com o AntiVir' no menu de contexto do Windows Explorer (botão direito do mouse). Com essa entrada, é possível verificar arquivos ou diretórios diretamente.

### – **Backup**

O componente Backup permite que você crie backups espelhados de seus dados manual e automaticamente.

## 4.4 Desinstalação

Se desejar remover o programa AntiVir de seu computador, use a opção **Adicionar ou remover programas** para **Alterar/remover** programas no Painel de controle do Windows.

Para desinstalar o programa AntiVir (por exemplo, no Windows XP e no Windows Vista):

- ▶ Abra o **Painel de controle** através do menu **Iniciar** do Windows.
- ▶ Clique duas vezes em **Programas** (Windows XP: **Software**).
- ▶ Selecione o programa AntiVir na lista e clique em **Remover**.

Será perguntado se você realmente deseja remover o programa.

- ▶ Clique em **Sim** para confirmar.

Será perguntado se você deseja reativar o Windows FireWall (o Avira FireWall é desativado).

- ▶ Clique em **Sim** para confirmar.

Todos os componentes do programa são removidos.

- ▶ Clique em **Concluir** para concluir a desinstalação.

Quando for apropriado, uma caixa de diálogo será exibida recomendando a

reinicialização do computador.

- ▶ Clique em **Sim** para confirmar.

O programa AntiVir é desinstalado e todos os diretórios, arquivos e entradas de registro do programa são excluídos quando o computador é reiniciado.

## 5 Visão geral do Premium Security Suite

Este capítulo contém uma visão geral da funcionalidade e da operação do programa AntiVir.

- consulte o Capítulo Interface e operação
- consulte o Capítulo Como...?

### 5.1 Interface de usuário e operação

É possível operar o programa AntiVir através de três elementos da interface do programa:

- Centro de controle: monitorar e controlar o programa AntiVir
- Configuração: Configuração do programa AntiVir
- Ícone de bandeja do sistema na barra de tarefas: Abre o Centro de controle e outras funções

#### 5.1.1 Centro de controle

O Centro de controle foi desenvolvido para monitorar o status de proteção de sistemas de computador e para controlar e operar os componentes e as funções de proteção do programa AntiVir.



A janela Centro de controle é dividida em três áreas: A **barra de menus**, a **barra de navegação** e a **Visualização** detalhada da janela:

- **Barra de menus:** Na barra de menus do Centro de controle, é possível acessar funções gerais do programa e informações sobre o programa.

- **Área de navegação:** nessa área, você pode alternar com facilidade entre as seções individuais do Centro de controle. As seções individuais contêm informações e funções dos componentes do programa e são organizadas na barra de navegação de acordo com a atividade. Exemplo: *Visão geral* da atividade - Seção **Status**.
- **Exibir:** essa janela mostra a seção selecionada na área de navegação. Dependendo da seção, você encontrará botões para executar funções e ações na barra superior da janela de detalhes. Os dados ou objetos de dados são exibidos em listas nas seções individuais. Para classificar as listas, clique na caixa que define como você deseja classificar a lista.

### Iniciando e fechando o Centro de controle

Para iniciar o Centro de controle, você tem as seguintes opções:

- Clique duas vezes no ícone do programa na área de trabalho
- Através da entrada do programa no menu Iniciar | Programas.
- Através do Ícone de bandeja do programa AntiVir.

Feche o Centro de controle com o comando de menu **Fechar** do menu **Arquivo** ou clicando na guia Fechar no Centro de controle.

### Operar o Centro de controle

Para navegar no Centro de controle

- ▶ Selecione uma atividade na barra de navegação.

A atividade é aberta e outras seções são exibidas. A primeira seção da atividade é selecionada e exibida na visualização.

- ▶ Se necessário, clique em outra seção para exibi-la na janela de detalhes.

- OU -

- ▶ Selecione uma seção no menu *Exibir*.

#### Nota

Você pode ativar a navegação do teclado na barra de menus com a ajuda da tecla [ALT]. Se a navegação estiver ativada, você poderá percorrer o menu com as teclas de seta. Com a tecla Voltar, é possível ativar o item de menu ativo.

Para abrir ou fechar menus no Centro de controle, ou para navegar pelos menus, você também pode usar as seguintes combinações de teclas: [Alt] + letra sublinhada no menu ou no comando de menu. Mantenha pressionada a tecla [Alt] se desejar acessar um menu, um comando de menu ou um submenu.

Para processar dados ou objetos exibidos na janela de detalhes:

- ▶ realce os dados ou o objeto que deseja editar.

Para realçar vários elementos (elementos nas colunas), mantenha pressionada a tecla ctrl ou a tecla shift enquanto seleciona os elementos.

- ▶ Clique no botão apropriado na barra superior da janela de detalhes para editar o objeto.

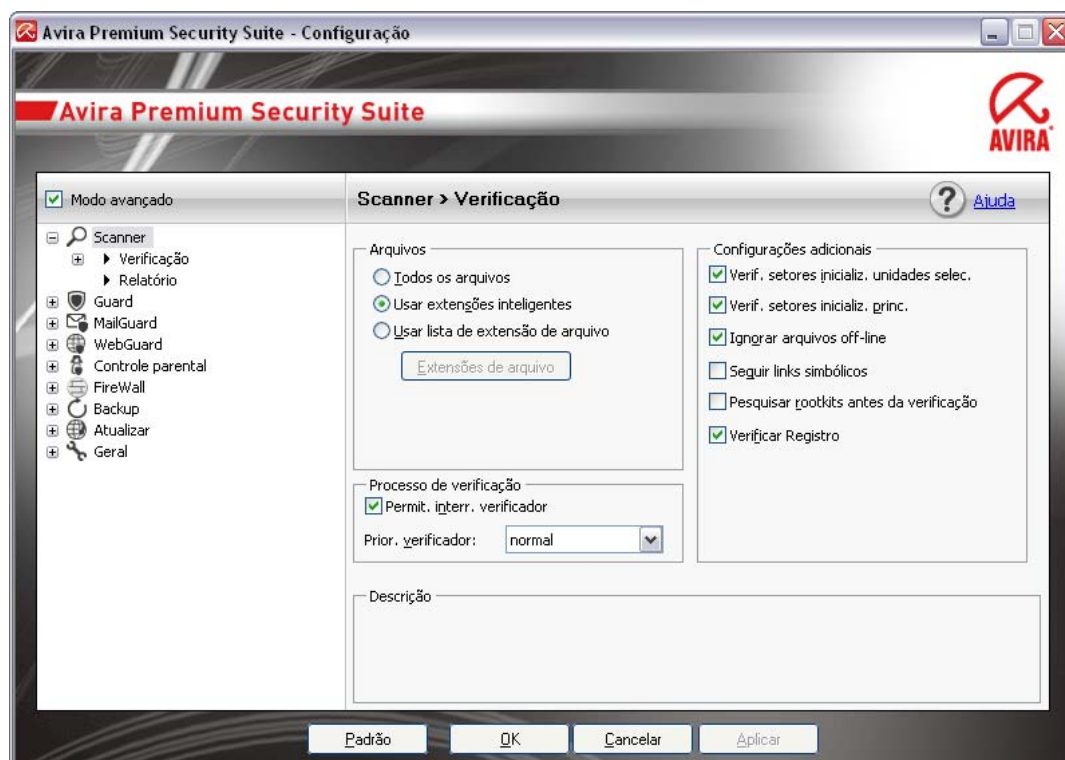
### Visão geral do Centro de controle

- **Visão geral:** Em **Visão geral**, você encontrará todas as seções com as quais é possível monitorar o funcionamento do programa AntiVir.

- A seção **Status** permite ver rapidamente quais módulos do programa estão ativos e fornece informações sobre a última atualização realizada. Você também pode ver se possui uma licença válida.
- A seção Eventos permite visualizar os eventos gerados por alguns módulos do programa.
- A seção Relatórios permite visualizar os resultados das ações executadas.
- **Proteção local:** Em **Proteção local**, você encontrará os componentes para verificar os arquivos do seu computador em busca de vírus e malwares.
- A seção Verificar permite que você configure e inicie uma verificação por demanda com facilidade. Perfis predefinidos ativa uma verificação com opções padrão já adaptadas. Do mesmo modo, é possível adaptar a verificação de vírus e programas indesejados de acordo com seus requisitos pessoais com a ajuda da seleção manual (não salva) ou com a criação de perfis definidos pelo usuário.
- A seção Guard exibe informações sobre os arquivos verificados, bem como outros dados estatísticos, que podem ser redefinidos a qualquer momento, e permite o acesso ao arquivo de relatório. Informações mais detalhadas sobre o último vírus ou programa indesejado detectado podem ser obtidas praticamente "com o pressionamento de um botão".
- **Proteção on-line:** Em **Proteção on-line**, você encontrará os componentes para proteger seu computador contra vírus e malwares da Internet e contra acesso não autorizado à rede.
- A seção MailGuard mostra todos os emails verificados pelo MailGuard, suas propriedades e outros dados estatísticos. Você também pode ajustar o filtro antispam e excluir endereços de e-mail de futuras verificações em busca de malware ou spam. Os e-mails também podem ser excluídos do buffer do MailGuard.
- A seção WebGuard mostra informações sobre URLs verificados e vírus detectados, bem como outros dados estatísticos, que podem ser redefinidos a qualquer momento, e permite o acesso ao arquivo de relatório. Informações mais detalhadas sobre o último vírus ou programa indesejado detectado podem ser obtidas praticamente "com o pressionamento de um botão".
- A seção FireWall permite definir as configurações básicas do Avira FireWall. Além disso, são exibidos todos os aplicativos ativos que usam uma conexão de rede e a taxa atual de transferência de dados.
- **Gerenciamento:** Em **Gerenciamento**, você encontrará ferramentas para isolar e gerenciar arquivos suspeitos ou infectados e para planejar tarefas recorrentes.
- A seção Quarentena contém o conhecido gerenciador de quarentena. Ele é o ponto central para os arquivos já colocados em quarentena ou para os arquivos suspeitos que você deseje colocar em quarentena. Também é possível enviar um arquivo selecionado para o Centro de pesquisa de malware da Avira por email.
- A seção Programador permite configurar trabalhos programados de verificação e atualização, bem como trabalhos de backup, e adaptar ou excluir os trabalhos existentes.
- **Ferramentas:** Em **Ferramentas**, você encontrará outras ferramentas de segurança de dados.
- Na seção Backup, é possível criar backups de dados com rapidez e facilidade, além de iniciar trabalhos de backup.

### 5.1.2 Configuração

Você pode definir as configurações do programa AntiVir na Configuração. Após ser instalado, o programa AntiVir é configurado com configurações padrão, garantindo uma excelente proteção para seu computador. No entanto, seu computador ou seus requisitos específicos para o programa AntiVir podem exigir que você faça adaptações nos componentes de proteção do programa.



A Configuração abre uma caixa de diálogo: Você pode salvar suas configurações através dos botões OK ou Aplicar, excluir suas configurações clicando no botão Cancelar ou restaurar as configurações padrão usando o botão Valores padrão. Você pode selecionar seções de configuração individuais na barra de navegação à esquerda.

#### Acessando a Configuração

Você tem várias opções para acessar a configuração:

- através do painel de controle do Windows.
- através da Central de segurança do Windows - no Windows XP Service Pack 2.
- Através do Ícone de bandeja do programa AntiVir.
- No Centro de controle através do item de menu Extras | Configuração.
- No Centro de controle através do botão Configuração.

#### Nota

Se estiver acessando a configuração através do botão **Configuração** no Centro de controle, vá até o registro de configuração da seção que está ativa no Centro de controle. O Modo de especialista deve estar ativado para selecionar registros de configuração individuais. Nesse caso, uma caixa de diálogo será exibida solicitando a ativação do modo de especialista.

#### Operação de configuração

Navegue na janela de configuração como você faria no Windows Explorer:

- ▶ Clique em uma entrada na estrutura em árvore para exibir essa seção de configuração na janela de detalhes.
- ▶ Clique no símbolo de adição ao lado da entrada para expandir a seção de configuração e exibir subseções de configuração na estrutura em árvore.
- ▶ Para ocultar subseções de configuração, clique no sinal de subtração ao lado da seção de configuração expandida.

### Nota

Para ativar ou desativar as opções da Configuração e usar os botões, você também pode usar as seguintes combinações de teclas: [Alt] + letra sublinhada no nome da opção ou na descrição do botão.

### Nota

Todas as seções de configuração são exibidas somente no modo de especialista. Ative o modo de especialista para exibir todas as seções de configuração. O modo de especialista pode ser protegido por uma senha que deve ser definida durante a ativação.

Se desejar confirmar suas configurações em Configuração:

- ▶ Clique em **OK**.  
A janela de configuração é fechada e as configurações são aceitas.  
- OU -

- ▶ Clique em **Aceitar**.  
As configurações são aplicadas. A janela de configuração permanece aberta.

Se desejar concluir a configuração sem confirmar as definições:

- ▶ Clique em **Cancelar**.  
A janela de configuração é fechada e as configurações são descartadas.

Se desejar restaurar todas as configurações aos valores padrão:

- ▶ Clique em **Restaurar padrões**.  
Todas as opções da configuração são restauradas aos valores padrão. Todas as correções e entradas personalizadas são perdidas quando as configurações padrão são restauradas.

## Visão geral das opções de configuração

As seguintes opções de configuração estão disponíveis:

- **Scanner**: Configuração da verificação sob demanda
  - Opções de verificação
  - Ação para detecção
  - Opções de verificação de arquivo
  - Exceções de verificação sob demanda
  - Heurística de verificação sob demanda
  - Configuração da função de registro
- **Guard**: Configuração da verificação durante o acesso
  - Opções de verificação
  - Ação para detecção



Exceções de verificação durante o acesso

Heurística de verificação durante o acesso

Configuração da função de registro

- **MailGuard:** Configuração do MailGuard

Opções de verificação: ativar o monitoramento das contas POP3, das contas IMAP, dos e-mails de saída (SMTP)

Ações para malware

Heurística de verificação do MailGuard

Função AntiBot: servidores SMTP permitidos, remetentes de email permitidos

Exceções de verificação do MailGuard

Configuração do cache, esvaziar cache

Configuração do banco de dados de treinamento antispam, banco de dados de treinamento vazio

Configuração de um rodapé nos emails enviados

Configuração da função de registro

- **WebGuard:** Configuração do WebGuard

Opções de verificação, ativação e desativação do WebGuard

Ação para detecção

Acesso bloqueado: Tipos de arquivo e tipos MIME indesejados, filtro da Web para URLs indesejados (malware, phishing etc.)

Exceções de verificação do WebGuard: URLs, tipos de arquivo, tipos MIME

Heurística do WebGuard

Função Controle dos pais: Filtro baseado em função e limite de tempo de uso da Internet baseado em função

Configuração da função de registro

- **FireWall:** Configuração do FireWall

Configuração da regra do adaptador

Configurações de regra de aplicativo definidas pelo usuário

Lista de fornecedores confiáveis (exceções para acesso de rede por parte dos aplicativos)

Configurações expandidas: Tempo limite de regras, bloquear arquivo de host do Windows, parar Windows FireWall, notificações

Configurações de pop-up (alertas para acesso de rede por parte dos aplicativos)

- **Backup:**

Configuração do componente Backup (backup incremental, verificar a presença de vírus durante o backup)

Exceções: definição de arquivos a serem salvos

Configuração da função de registro

- **Geral:**

Categorias de risco estendidas para verificação sob demanda e durante o acesso

Proteção com senha para acesso ao Centro de controle e à Configuração

Segurança: Exibição do status de atualização, exibição do status de verificação completa do sistema, proteção do produto

WMI: Ativar suporte para WMI

Configuração do registro de eventos

Configuração das funções de registro



Configuração dos diretórios usados

Atualizar: Configuração de conexão com o servidor de download, configuração das atualizações do produto

Configuração de alertas acústicos emitidos quando malwares são detectados

### 5.1.3 Ícone de bandeja

Após a instalação, você verá o ícone do programa AntiVir na bandeja do sistema, na barra de tarefas:

Ícone	Descrição
	O AntiVir Guard é ativado e o FireWall é ativado
	O AntiVir Guard é desativado e o FireWall é desativado

O ícone de bandeja exibe o status do serviço do Guard e do FireWall .

As funções centrais do programa AntiVir podem ser acessadas rapidamente através do menu de contexto do ícone da bandeja. Para abrir o menu de contexto, clique no ícone da bandeja com o botão direito do mouse.

#### Entradas do menu de contexto

- **Ativar AntiVir Guard:** Ativa ou desativa o AntiVir Guard.
- **Ativar o AntiVir MailGuard:** Ativa ou desativa o AntiVir MailGuard.
- **Ativar o AntiVir WebGuard:** Ativa ou desativa o AntiVir WebGuard.
- **FireWall:**
  - Ativar FireWall: Ativa ou desativa o FireWall
  - Bloquear todo o tráfego: Ativado: bloqueia todas as transferências de dados, exceto as transferência para o sistema do computador host (host local/endereço IP 127.0.0.1).
  - Ativar modo de jogo: Ativa ou desativa o modo:
    - Ativado: quando está ativado, todas as regras definidas de adaptador e aplicativo são aplicadas. Os aplicativos para os quais nenhuma regra é definida têm permissão para acessar a rede e nenhuma janela pop-up é aberta.
- **Iniciar o AntiVir:** Abre o Centro de controle.
- **Configurar o AntiVir:** Abre a Configuração
- **Iniciar atualização** Inicia uma atualização.
- Ajuda: abre a Ajuda on-line.

- **Sobre o Premium Security Suite:** Abre uma caixa de diálogo com informações sobre o programa AntiVir: Informações do produto, Informações da versão, Informações de licença.
- **Avira na Internet:** Abre o portal da Web do Avira na Internet. Para isso, é necessário ter uma conexão ativa com a Internet.

## 5.2 Como...?

### 5.2.1 Ativar produto

Para ativar seu produto AntiVir, você tem as seguintes opções:

- **Ativação com uma licença completa válida**  
Para ativar o programa com uma licença completa, você precisa de uma chave de ativação válida, que contém os dados da licença adquirida. A chave de ativação é enviada por nós por e-mail ou está impressa na embalagem do produto.
- **Ativação com uma licença de avaliação**  
Seu programa AntiVir é ativado com uma licença de avaliação gerada automaticamente, com a qual é possível testar o programa AntiVir com todas as suas funções por um período limitado.

#### **Nota**

Para a ativação do produto ou para obter uma licença de teste, é necessário ter uma conexão ativa com a Internet.

Se não for possível estabelecer nenhuma conexão com os servidores da Avira GmbH, verifique as configurações do firewall utilizado: as conexões feitas através do protocolo HTTP e da porta 80 (comunicação da Web) e através do protocolo de criptografia SSL e da porta 443 são usadas para a ativação do produto. Verifique se o seu firewall não bloqueia dados de entrada e de saída. Primeiro, verifique se você consegue acessar as páginas da Web com seu navegador.

#### **Para ativar seu produto AntiVir, você tem as seguintes opções:**

Caso ainda não tenha instalado seu programa AntiVir:

- ▶ Instale seu programa AntiVir.  
Durante o processo de instalação, você deverá escolher uma opção de ativação
  - *Ativar produto*  
= Ativação com uma licença completa válida
  - *Testar produto*  
= Ativação com uma licença de avaliação
- ▶ Insira a chave de ativação para ativar o produto com uma licença completa.
- ▶ Confirme a seleção do procedimento de ativação clicando em **Avançar**.
- ▶ Se e quando necessário, insira seus dados pessoais de registro e confirme clicando em **Avançar**.  
Os dados de sua licença serão exibidos na próxima janela. O programa AntiVir foi habilitado.
- ▶ Continue a instalação.

Caso já tenha instalado seu programa AntiVir:


- ▶ No Centro de Controle, selecione o item **Ajuda :: no menu Gerenciamento de licenças**.

O assistente de licença é aberto, no qual você pode escolher uma opção de ativação. As próximas etapas de ativação do produto são idênticas ao procedimento descrito acima.

## 5.2.2 Executar atualização automática

Para criar um trabalho com o AntiVir Scheduler para atualizar seu programa AntiVir automaticamente:

- ▶ No Centro de Controle, selecione a seção **Gerenciamento :: Programador**

- ▶ Clique no ícone  *Criar novo trabalho com o assistente*.

A caixa de diálogo *Nome e descrição do trabalho* é exibida.

- ▶ Dê um nome ao trabalho e, quando apropriado, uma descrição.

- ▶ Clique em **Avançar**.

A caixa de diálogo *Tipo de trabalho* é exibida.

- ▶ Selecione **Trabalho de atualização** na lista.

- ▶ Clique em **Avançar**.

A caixa de diálogo *Tempo do trabalho* é exibida.

- ▶ Selecione um horário para a atualização:

- **Imediatamente**
- **Diariamente**
- **Semanalmente**
- **Intervalo**
- **Única**
- **Login**

### Nota

Recomendamos que você faça atualizações regularmente e com frequência. O intervalo de atualização recomendado é: 2 horas.

- ▶ Quando apropriado, especifique uma data de acordo com a seleção.
- ▶ Quando apropriado, selecione opções adicionais (a disponibilidade depende do tipo de trabalho):

- **Também iniciar trabalho quando uma conexão com a Internet for estabelecida**

Além da frequência definida, o trabalho é executado quando uma conexão com a Internet é configurada.

- **Repetir trabalho se o tempo já tiver expirado**

Os trabalhos antigos são executados agora porque não foram executados no horário programado (por exemplo, o computador foi desligado).

- ▶ Clique em **Avançar**.

A caixa de diálogo *Selecionar modo de exibição* é exibida.

- ▶ Selecione o modo de exibição da janela do trabalho:
  - **Minimizar**: somente barra de andamento
  - **Maximizar**: janela de trabalho inteira
  - **Ocultar**: sem janela de trabalho
- ▶ Clique em **Concluir**.

O trabalho recém criado aparece na página inicial da seção **Gerenciador :: Seção Verificador** com o status ativado (marca de verificação).
- ▶ Quando apropriado, desative os trabalhos que não devem ser executados.

Use os ícones a seguir para definir seus trabalhos ainda mais:



Exibir propriedades de um trabalho



Modificar trabalho



Excluir trabalho



Iniciar trabalho



Interromper trabalho

### 5.2.3 Iniciar uma atualização manual

Você tem várias opções para iniciar uma atualização manualmente: quando uma atualização é iniciada manualmente, o arquivo de definição de vírus e o mecanismo de verificação sempre são atualizados. Uma atualização do produto só poderá ocorrer se você tiver ativado a opção **Baixar e instalar as atualizações do produto automaticamente** na configuração em Geral :: Atualizar

Para iniciar uma atualização manualmente de seu programa AntiVir:

- ▶ Com o botão direito do mouse, clique no ícone de bandeja do AntiVir na barra de tarefas.

Um menu de contexto é exibido.
- ▶ Selecione **Iniciar atualização**.

A caixa de diálogo *Atualizador* é exibida.

- OU -
- ▶ No Centro de Controle, selecione a seção **Visão geral :: Status**.
- ▶ No campo *Última atualização*, clique no link **Iniciar atualização**.

A caixa de diálogo *Atualizador* é exibida.

- OU -
- ▶ No Centro de controle, no menu **Atualizar**, selecione o comando de menu *Iniciar atualização*.

A caixa de diálogo *Atualizador* é exibida.

#### **Nota**

Recomendamos a realização de atualizações automáticas periódicas. O intervalo de atualização recomendado é: 2 horas.

**Nota**

Você também pode realizar uma atualização manual diretamente no Centro de segurança do Windows.

## 5.2.4 Verificação sob demanda: Uso de um perfil de verificação para verificar a presença de vírus e malwares

Um perfil de verificação é um conjunto de unidades e diretórios a serem verificados. As seguintes opções estão disponíveis para verificação com um perfil:

- Usar perfil de verificação predefinido  
se o perfil de verificação predefinido corresponder aos seus requisitos.
- Personalizar e aplicar perfil de verificação (seleção manual)  
se desejar verificar com um perfil personalizado.
- Criar e aplicar novo perfil de verificação  
se desejar criar seu próprio perfil de verificação.

Dependendo do sistema operacional, vários ícones estão disponíveis para iniciar um perfil de verificação:

- No Windows XP e 2000:



Esse ícone inicia a verificação através de um perfil.

- No Windows Vista:

No Microsoft Windows Vista, o Centro de Controle tem apenas direitos limitados no momento, por exemplo, para acessar diretórios e arquivos. Algumas ações e alguns acessos de arquivo só podem ser realizados no Centro de Controle com direitos de administrador estendidos. Esses direitos devem ser concedidos no início de cada verificação através de um perfil de verificação.



Esse ícone inicia uma verificação limitada através de um perfil. Somente os diretórios e arquivos aos quais o Windows Vista concedeu direitos de acesso são verificados.



Esse ícone inicia a verificação com direitos de administrador estendidos. Após a confirmação, todos os diretórios e arquivos no perfil selecionado são verificados.

Para verificar a presença de vírus e malwares com um perfil de verificação:

- ▶ Vá até o Centro de controle e selecione a seção **Proteção local :: Verificar**.  
Os perfis de verificação predefinidos são exibidos.
- ▶ Selecione um dos perfis de verificação predefinidos.  
-OU-
- ▶ Adapte o perfil de verificação *Seleção manual*.  
-OU-
- ▶ Criar um novo perfil de verificação
- ▶ Clique no ícone (Windows XP: ou Windows Vista: ).

- ▶ A janela *Luke Filewalker* é exibida e uma verificação por demanda é iniciada. Quando a verificação termina, os resultados são exibidos.



Se desejar adaptar um perfil de verificação:

- ▶ No perfil de verificação, expanda a árvore de arquivos **Seleção Manual** para que todas as unidades e todos os diretórios que deseja verificar sejam abertos.
  - Clique no ícone + : o próximo nível do diretório é exibido.
  - Clique no ícone - : o próximo nível do diretório é ocultado.
- ▶ Realce os nós e os diretórios que deseja verificar clicando na caixa do nível de diretório apropriado.

As seguintes opções estão disponíveis, para selecionar diretórios:

- Diretório, incluindo os subdiretórios (marca de verificação preta)
- Diretório, sem os subdiretórios (marca de verificação verde)
- Subdiretórios de apenas um diretório (marca de verificação cinza; os subdiretórios têm marcas de verificação pretas)
- Nenhum diretório (sem marca de verificação)

Se desejar criar um novo perfil de verificação:

- ▶ Clique no ícone  **Criar novo perfil**.  
O perfil *Novo perfil* aparece abaixo dos perfis criados anteriormente.
- ▶ Quando apropriado, renomeie o perfil de verificação clicando no ícone .
- ▶ Realce os nós e diretórios a serem salvos clicando na caixa de seleção do nível de diretório correspondente.

As seguintes opções estão disponíveis, para selecionar diretórios:

- Diretório, incluindo os subdiretórios (marca de verificação preta)
- Diretório, sem os subdiretórios (marca de verificação verde)
- Subdiretórios de apenas um diretório (marca de verificação cinza; os subdiretórios têm marcas de verificação pretas)
- Nenhum diretório (sem marca de verificação)

### 5.2.5 Verificação sob demanda: Verificar presença de vírus e malwares com o método de arrastar e soltar

Para verificar a presença de vírus e malwares sistematicamente com o método de arrastar e soltar:

O Centro de controle de seu programa AntiVir foi aberto.

- ▶ Realce o arquivo ou diretório que deseja verificar.
- ▶ Use o botão do mouse para arrastar o arquivo ou diretório realçado para o *Centro de controle*.

A janela *Luke Filewalker* é exibida e uma verificação por demanda é iniciada.

Quando a verificação termina, os resultados são exibidos.

## 5.2.6 Verificação sob demanda: Verificar presença de vírus e malwares através do menu de contexto

Para verificar a presença de vírus e malwares sistematicamente através do menu de contexto:


- ▶ Clique com o botão direito do mouse (por exemplo, no Windows Explorer, na área de trabalho ou em um diretório aberto do Windows) no arquivo ou diretório que deseja verificar.  
O menu de contexto do Windows Explorer é exibido.
- ▶ Selecione **Verificar arquivos selecionados com o AntiVir** no menu de contexto.  
A janela *Luke Filewalker* é exibida e uma verificação por demanda é iniciada.  
Quando a verificação termina, os resultados são exibidos.

## 5.2.7 Verificação sob demanda: Verificar presença de vírus e malwares automaticamente

### Nota

Depois da instalação, o trabalho de verificação *Verificação completa do sistema* é criado no Programador: Uma verificação completa do sistema é automaticamente executada em um intervalo recomendado.

Para criar um trabalho de verificação automática da presença de vírus e malwares:

- ▶ No Centro de Controle, selecione a seção **Gerenciamento:: Programador**.
- ▶ Clique no ícone  - :  
A caixa de diálogo *Nome e descrição do trabalho* é exibida.
- ▶ Dê um nome ao trabalho e, quando apropriado, uma descrição.
- ▶ Clique em **Avançar**.  
A caixa de diálogo *Tipo de trabalho* é exibida.
- ▶ Selecione **Trabalho de verificação**.
- ▶ Clique em **Avançar**.  
A caixa de diálogo *Selecionar perfil* é exibida.
- ▶ Selecione o perfil a ser verificado.
- ▶ Clique em **Avançar**.  
A caixa de diálogo *Tempo do trabalho* é exibida.
- ▶ Selecione um horário para a verificação:
  - **Imediatamente**
  - **Diariamente**
  - **Semanalmente**
  - **Intervalo**
  - **Única**
  - **Login**
- ▶ Quando apropriado, especifique uma data de acordo com a seleção.



- ▶ Quando apropriado, selecione as seguintes opções adicionais (a disponibilidade depende do tipo de trabalho):
  - **Repetir trabalho se o tempo já tiver expirado**

Os trabalhos antigos são executados agora porque não foram executados no horário programado (por exemplo, o computador foi desligado).
- ▶ Clique em **Avançar**.

A caixa de diálogo *Selecionar modo de exibição* é exibida.
- ▶ Selecione o modo de exibição da janela do trabalho:
  - **Minimizar**: somente barra de andamento
  - **Maximizar**: janela de trabalho inteira
  - **Ocultar**: sem janela de trabalho
- ▶ Selecione a opção *Desligar o computador* se você quiser que o computador seja desligado automaticamente quando a verificação for concluída. Essa opção está disponível apenas se o modo de exibição estiver definido para minimizado ou maximizado.
- ▶ Clique em **Concluir**.

O trabalho recém criado aparece na página inicial da seção *Gerenciador :: Seção Programador* com o status ativado (marca de verificação).
- ▶ Quando apropriado, desative os trabalhos que não devem ser executados.

Use os ícones a seguir para definir seus trabalhos ainda mais:



Exibir propriedades de um trabalho



Modificar trabalho



Excluir trabalho



Iniciar trabalho





Interromper trabalho

### 5.2.8 Verificação sob demanda: Verificação direcionada de rootkits e malware ativo

Para verificar rootkits ativos, use o perfil de verificação predefinido *Verificar rootkits e malware ativo*.

Para verificar rootkits ativos sistematicamente:

- ▶ Vá até o Centro de controle e selecione a seção **Proteção local :: Scanner**.

Os perfis de verificação predefinidos são exibidos.
- ▶ Selecionar o perfil de verificação predefinido **Verificar rootkits e malware ativo**
- ▶ Quando apropriado, realce outros nós e diretórios a serem verificados clicando na caixa de seleção do nível de diretório.
- ▶ Clique no ícone (Windows XP:  ou Windows Vista: )

A janela *Luke Filewalker* é exibida e uma verificação por demanda é iniciada. Quando a verificação termina, os resultados são exibidos.

### 5.2.9 Reação aos vírus e malwares detectados

Para os componentes de proteção individuais de seu programa AntiVir, você pode definir como ele reage a um vírus ou programa indesejado detectado na configuração, na seção *Ação para detecção*.

Nenhuma opção de ação configurável está disponível para o componente ProActiv do Guard: A Notificação de uma detecção é sempre dada na janela *Guard: Comportamento suspeito de aplicativo detectado*.

Opções de ação para o Scanner:

– **Interativo**

No modo de ação interativo, os resultados da verificação do Scanner são exibidos em uma caixa de diálogo. Essa opção é ativada como configuração padrão.

No caso de uma **verificação com o Scanner**, um alerta será emitido com uma lista dos arquivos afetados quando a verificação for concluída. Você pode usar o menu sensível ao contexto para selecionar uma ação a ser executada para os diversos arquivos afetados. Você pode executar as ações padrão para todos os arquivos afetados ou cancelar o Scanner.

– **Automático**

No modo de ação automático, quando um vírus ou programa indesejado é detectado, a ação selecionada nessa área é executada automaticamente.

Opções de ação para o Guard:

– **Interativo**

No modo de ação interativo, o acesso aos dados é negado e uma notificação de desktop é exibida. Na notificação de desktop, você pode remover o malware detectado ou transferi-lo para o componente Scanner, usando o botão Detalhes, para o gerenciamento futuro do vírus. O Scanner abre a janela contendo a notificação da detecção, que fornece a você várias opções para o gerenciamento do arquivo afetado por meio do menu de contexto (consulte Detecção::Scanner):

– **Automático**

No modo de ação automática, quando um vírus ou programa indesejado é detectado, a ação selecionada nessa área é executada automaticamente.

Opções de ação para MailGuard, WebGuard:

– **Interativo**

No modo de ação interativo, se um vírus ou programa indesejado for detectado, uma caixa de diálogo será exibida, na qual é possível selecionar o que deve ser feito com o objeto infectado. Essa opção é ativada como configuração padrão.

– **Automático**

No modo de ação automático, quando um vírus ou programa indesejado é detectado, a ação selecionada nessa área é executada automaticamente.

No modo de ação interativo, você pode reagir aos vírus e programas indesejados detectados selecionando uma ação para o objeto infectado, exibido no alerta, e executando a ação selecionada ao clicar em Confirmar.

As seguintes ações estão disponíveis para manipular os objetos infectados:

### **Nota**

As ações disponíveis para seleção dependem do sistema operacional, dos componentes de proteção (AntiVir Guard, AntiVir Scanner, AntiVir MailGuard, AntiVir WebGuard) do relatório da detecção e do tipo de malware detectado.

### **Ações do Scanner e do Guard (não detecções do ProActiv):**

#### – **Reparar**

O arquivo é reparado.

Essa opção só estará disponível se for possível reparar o arquivo infectado.

#### – **Mover para quarentena**

O arquivo é compactado em um formato especial (\*.qua) e movido para o diretório de Quarentena *INFECTED* em seu disco rígido para que o acesso direto não seja mais permitido. Os arquivos nesse diretório podem ser reparados na quarentena e posteriormente ou, se necessário, enviados para a Avira GmbH.

#### – **Excluir**

O arquivo será excluído. Esse processo é muito mais rápido do que *sobrescrever e excluir*. Se um vírus de setor de inicialização for detectado, será necessário excluir o setor de inicialização para excluir o vírus. Um novo setor de inicialização é gravado.

#### – **Substituir e excluir**

O arquivo é substituído por um modelo padrão e, em seguida, excluído. Não é possível restaurá-lo.

#### – **Renomear**

O arquivo é renomeado com uma extensão \*.vir. Portanto, o acesso direto a esses arquivos (por exemplo, com clique duplo) não é mais possível. Os arquivos podem ser reparados e voltar a ter seus nomes originais posteriormente.

#### – **Ignorar**

Nenhuma outra ação será realizada. O arquivo infectado permanece ativo em seu computador.

### **Aviso**

Isso pode resultar em perda de dados e danos ao sistema operacional. Selecione a opção *Ignorar* somente em casos excepcionais.

#### – **Sempre ignorar**

Opção de ação para detecções do Guard: O Guard não realiza nenhuma ação. O acesso ao arquivo é permitido. Todos os outros acessos a esse arquivo são permitidos e nenhuma notificação será fornecida até que o computador seja reiniciado ou o arquivo de definição de vírus seja atualizado.

#### – **Copiar para quarentena**

Opção de ação para uma detecção de rootkit: a detecção é copiada para a quarentena.

#### – **Reparar setor de inicialização | Baixar ferramenta de reparo**

Opções de ação quando setores de inicialização infectados são detectados: Há várias opções disponíveis para reparar unidades de disquete infectadas. Se o seu programa Antivir não puder executar o reparo, você poderá baixar uma ferramenta especial para detecção e remoção dos vírus do setor de inicialização.

### Nota

Se você executar ações nos processos em execução, os processos em questão serão finalizados antes de as ações serem executadas.

### Ações do Guard para detecção feita pelo componente ProActiv (notificação das ações de aplicativo suspeitas):

#### – Programa confiável

O aplicativo continua a ser executado. O programa é adicionado à lista de aplicativos permitidos e é excluído do monitoramento feito pelo componente ProActiv. Quando adicionado à lista de aplicativos permitidos, o tipo de monitoramento é definido para *Conteúdo*. Isso significa que o aplicativo só será excluído do monitoramento feito pelo componente ProActiv se o conteúdo permanecer inalterado (consulte Configuração::Guard::ProActiv::Filtro de aplicativos: Aplicativos permitidos).

#### – Bloquear programa uma vez

O aplicativo é bloqueado, isto é, ele é encerrado. As ações do aplicativo continuam sendo monitoradas pelo componente ProActiv.

#### – Sempre bloquear este programa

O aplicativo é bloqueado, isto é, ele é encerrado. O programa é adicionado à lista de aplicativos bloqueados e não pode mais ser executado (consulte Configuração::Guard::ProActiv::Filtro de aplicativos: Aplicativos a serem bloqueados).

#### – Ignorar

O aplicativo continua a ser executado. As ações do aplicativo continuam sendo monitoradas pelo componente ProActiv.

### Ações do MailGuard: emails recebidos

#### – Mover para quarentena

O e-mail com todos os anexos é movido para a quarentena. O e-mail afetado é excluído. O corpo do texto e todos os anexos do email são substituídos por um texto padrão.

#### – Excluir

O e-mail afetado é excluído. O corpo do texto e todos os anexos do email são substituídos por um texto padrão.

#### – Excluir anexo

O anexo infectado é substituído por um texto padrão. Se o corpo do e-mail for afetado, ele será excluído e também substituído por um texto padrão. O e-mail propriamente dito é entregue.

#### – Mover anexo para quarentena

O anexo infectado é colocado na Quarentena e excluído em seguida (substituído por um texto padrão). O corpo do e-mail é entregue. O anexo afetado pode ser entregue posteriormente pelo Gerenciador de quarentena.

#### – Ignorar

O e-mail afetado é entregue.

### **Aviso**

Isso poderia permitir o acesso de vírus e programas indesejado ao sistema do seu computador. Selecione a opção **Ignorar** somente em casos excepcionais. Desative a visualização em seu cliente de e-mail. Nunca abra nenhum anexo clicando duas vezes nele.

### **Ações do MailGuard: Emails enviados**

#### – **Mover email para quarentena (não enviar)**

O e-mail e todos os anúncios serão copiados na Quarentena e não serão enviados. O e-mail permanece na caixa de saída de seu cliente de e-mail. Uma mensagem de erro será exibida em seu programa de e-mail. Todos os outros e-mails enviados de sua conta serão verificados em busca de malwares.

#### – **Bloquear envio de e-mails (não enviar)**

O e-mail não é enviado e permanece na caixa de saída de seu cliente de e-mail. Uma mensagem de erro será exibida em seu programa de e-mail. Todos os outros e-mails enviados de sua conta serão verificados em busca de malwares.

#### – **Ignorar**

O e-mail afetado é enviado.

### **Aviso**

Vírus e programas indesejados podem penetrar no sistema do computador do destinatário do e-mail desse modo.

### **Ações do WebGuard:**

#### – **Negar acesso**

O site solicitado do servidor da Web e/ou todos os dados ou arquivos transferidos não são enviados para seu navegador. Uma mensagem de erro para notificar que o acesso foi negado é exibida no navegador.

#### – **Mover para quarentena**

O site solicitado do servidor da Web e/ou todos os dados ou arquivos transferidos são movidos para a quarentena. O arquivo afetado pode ser recuperado do Gerenciador de quarentena se tiver um valor informativo ou, se necessário, enviado para o Centro de pesquisa de malware da Avira.

#### – **Ignorar**

O site solicitado do servidor da Web e/ou os dados e arquivos que foram transferidos são encaminhados pelo WebGuard para seu navegador.

### **Aviso**

Isso poderia permitir o acesso de vírus e programas indesejado ao sistema do seu computador. Selecione a opção **Ignorar** somente em casos excepcionais.

### **Nota**

Recomendamos que você envie todos os arquivos suspeitos que não possam ser reparados para a quarentena.

### Nota

Você também pode enviar os arquivos registrados pela heurística para serem analisados por nós.

Por exemplo, você pode enviar esses arquivos para nosso

site:[http://www.avira.pt/sample\\_upload](http://www.avira.pt/sample_upload)


Você pode identificar os arquivos registrados pela heurística pela designação *HEUR/* or *HEURISTIC/* que aparece antes do nome do arquivo, por exemplo: *HEUR/testfile.\**.

### 5.2.10 Quarentena: Manipulação de arquivos em quarentena (\*.qua)

Para manipular os arquivos em quarentena:

- ▶ No Centro de Controle, selecione a seção **Gerenciamento :: Seção** Quarentena.
- ▶ Verifique quais arquivos estão envolvidos para que, se necessário, você possa recarregar o original no computador a partir de outro local.


Se desejar ver mais informações sobre um arquivo:

- ▶ Realce o arquivo e clique em .

A caixa de diálogo *Propriedades* é exibida com mais informações sobre o arquivo.

Se desejar verificar um arquivo novamente:


É recomendado verificar um arquivo se o arquivo de definição de vírus do seu programa Antivir tiver sido atualizado e houver uma suspeita de um falso-positivo. Desse modo, você pode confirmar o falso-positivo com uma nova verificação e restaurar o arquivo.

- ▶ Realce o arquivo e clique em .

O arquivo é verificado em busca de vírus e malwares com as configurações da verificação sob demanda.


Após a verificação, a caixa de diálogo *Estatísticas da verificação* será exibida mostrando estatísticas sobre o status do arquivo antes e depois da nova verificação.

Para excluir um arquivo:

- ▶ Realce o arquivo e clique em .

Se você quiser carregar o arquivo para um servidor da web do Centro de pesquisa de malware da Avira para análise:

- ▶ Realce o arquivo que deseja enviar.

- ▶ Clique em .

Uma caixa de diálogo é aberta com um formulário para inserir seus dados de contato.

- ▶ Insira todos os dados necessários.
- ▶ Selecione um tipo: **Arquivo suspeito** ou **Falso-positivo**.
- ▶ Clique em **OK**.

O arquivo é carregado em um servidor da Web do Centro de pesquisa de malware da Avira em formato compactado.

**Nota**

Nos seguintes casos, é recomendada a análise do Centro de pesquisa de malware da Avira:

**Acessos heurísticos (arquivo suspeito):** durante uma verificação, um arquivo foi classificado como suspeito por seu programa Antivir e movido para a quarentena: a análise do arquivo, feita pelo Centro de pesquisa de malware da Avira, foi recomendada na caixa de diálogo de detecção de vírus ou no arquivo de relatório gerado pela verificação.

**Arquivo suspeito:** você considera um arquivo suspeito e, por isso, move esse arquivo para a quarentena, mas uma verificação do arquivo quanto a vírus e malware é negativa.

**Falso-positivo:** você supõe que uma detecção de vírus é um falso-positivo: Seu programa Antivir registra uma detecção em um arquivo que pouco provavelmente foi infectado por malware.


**Nota**

Os arquivos enviados podem ter no máximo 20 MB (quando não estão compactados) ou 8 MB (quando estão compactados).

**Observação**

Você só pode enviar um arquivo de cada vez.


Se você quiser copiar um objeto da quarentena para outro diretório:

- ▶ Realce o objeto em quarentena e clique em .  
Uma caixa de diálogo é aberta para que você selecione um diretório.
- ▶ Selecione um diretório em que deseja salvar uma cópia do objeto em quarentena e confirme sua seleção.  
O objeto em quarentena selecionado é salvo no diretório selecionado.

**Nota**

O objeto em quarentena não é idêntico ao arquivo restaurado. O objeto em quarentena é criptografado e não pode ser executado ou lido em seu formato original.

Se você quiser exportar as propriedades de um objeto em quarentena para um arquivo de texto:

- ▶ Realce o objeto em quarentena e clique em .
- ▶ Um arquivo de texto é aberto contendo dados do objeto de quarentena selecionado.
- ▶ Salve o arquivo de texto.

Você também pode restaurar os arquivos em quarentena:


- consulte o Capítulo: Quarentena: Restauração de arquivos em quarentena

### 5.2.11 Quarentena: Restaurar os arquivos em quarentena

Ícones diferentes controlam o processo de restauração, dependendo do sistema operacional:

- No Windows XP e 2000:

 Esse ícone restaura os arquivos em seu diretório original.

 Esse ícone restaura os arquivos em um diretório de sua preferência.

- No Windows Vista:

No Microsoft Windows Vista, o Centro de Controle tem apenas direitos limitados no momento, por exemplo, para acessar diretórios e arquivos. Algumas ações e alguns acessos de arquivo só podem ser realizados no Centro de Controle com direitos de administrador estendidos. Esses direitos devem ser concedidos no início de cada verificação através de um perfil de verificação.



Esse ícone restaura os arquivos em um diretório de sua preferência.



Esse ícone restaura os arquivos em seu diretório original. Se direitos de administrador estendidos forem necessários para acessar esse diretório, será exibida uma solicitação correspondente.

Para restaurar os arquivos em quarentena:


### Aviso

Isso pode resultar em perda de dados e danos ao sistema operacional do computador. Use a função *Restaurar objeto selecionado* em casos excepcionais. Restaure somente os arquivos que podem ser reparados por uma nova verificação.



Arquivo verificado novamente e reparado.

- ▶ No Centro de Controle, selecione a seção **Gerenciamento :: Seção** Quarentena.


### Nota

Os e-mails e anexos só podem ser restaurados com a opção  se a extensão do arquivo for *\*.eml*.

Para restaurar um arquivo ao seu local original:

- ▶ Realce o arquivo e clique no ícone (Windows 2000/XP: , Windows Vista ).
- Essa opção não está disponível para e-mails.

### Nota


Os e-mails e anexos só podem ser restaurados com a opção  se a extensão do arquivo for *\*.eml*.

Será exibida uma mensagem perguntando se você deseja restaurar o arquivo.

- ▶ Clique em **Sim**.

O arquivo é restaurado para o diretório em que estava antes de ser movido para a quarentena.

Para restaurar um arquivo em um diretório específico:

- ▶ Realce o arquivo e clique em .

Será exibida uma mensagem perguntando se você deseja restaurar o arquivo.

- ▶ Clique em **Sim**.

A janela padrão do Windows para selecionar o diretório é exibida.

- ▶ Selecione o diretório onde o arquivo será restaurado e confirme.


O arquivo é restaurado no diretório selecionado.

## 5.2.12 Quarentena: Mover arquivos suspeitos para quarentena

Para mover um arquivo suspeito para a quarentena manualmente:



- ▶ No Centro de Controle, selecione a seção **Gerenciamento :: Seção** Quarentena.

- ▶ Clique em .

A janela padrão do Windows para selecionar um arquivo é exibida.

- ▶ Selecione o arquivo e confirme.  
O arquivo é movido para a quarentena.

Você pode verificar os arquivos em quarentena com o AntiVir Scanner:

- consulte o Capítulo: Quarentena: Manipulação de arquivos em quarentena (\*.qua)

### 5.2.13 Perfil da verificação: Corrigir ou excluir tipo de arquivo em um perfil de verificação

Para especificar outros tipos de arquivo a serem verificados ou excluir determinados tipos da verificação em um perfil (possível apenas para seleção manual e perfis de verificação personalizados):

No Centro de controle, vá até a seção **Proteção local :: Seção** Verificar.

- ▶ Com o botão direito do mouse, clique no perfil de verificação que deseja editar.  
Um menu de contexto é exibido.
- ▶ Selecione **Filtro de arquivo**.
- ▶ Expanda o menu de contexto ainda mais clicando no pequeno triângulo à direita do menu de contexto.

As entradas *Padrão*, *Verificar todos os arquivos* e *Definido pelo usuário* são exibidas.

- ▶ Selecione **Definido pelo usuário**.

A caixa de diálogo *Extensões de arquivo* é exibida com uma lista de todos os tipos de arquivo a serem verificados com o perfil de verificação.

Se desejar excluir um tipo de arquivo da verificação:

- ▶ Realce o tipo de arquivo e clique em **Excluir**.

Se desejar adicionar um tipo de arquivo à verificação:

- ▶ Realce o tipo de arquivo.
- ▶ Clique em **Adicionar** e insira a extensão do tipo de arquivo na caixa de entrada.

Use no máximo 10 caracteres e não insira nenhum ponto antes. Os caracteres curinga (\* e ?) são aceitos como substitutos.


### 5.2.14 Perfil da verificação: Criar atalho na área de trabalho para o perfil de verificação

Você pode iniciar uma verificação sob demanda diretamente na área de trabalho através de um atalho para um perfil de verificação sem acessar o Centro de controle de seu programa AntiVir'.

Para criar um atalho na área de trabalho para o perfil de verificação:

No Centro de controle, vá até a seção **Proteção local :: Seção** Verificar.

- ▶ Selecione o perfil de verificação para o qual deseja criar um atalho.

- ▶ Clique no ícone  - :

O atalho é criado na área de trabalho.

### 5.2.15 Eventos: Filtrar eventos

Os eventos que foram gerados pelos componentes do programa AntiVir são exibidos no Centro de controle, em **Visão Geral::Eventos** (análogo à exibição do evento do seu sistema operacional Windows). Os componentes do programa são:

- Atualizador
- Programador
- Guard
- MailGuard
- Scanner
- FireWall
- WebGuard
- Backup
- Serviço de ajuda
- ProActiv

Os seguintes tipos de evento são exibidos:

- Informações
- Aviso
- Erro
- Detecção

Para filtrar os eventos exibidos:

- ▶ No Centro de Controle, selecione a seção **Visão geral :: Eventos**.
- ▶ Marque a caixa dos componentes do programa para exibir os eventos dos componentes ativados.  
- OU -  
Desmarque a caixa dos componentes do programa para ocultar os eventos dos componentes desativados.
  
- ▶ Marque a caixa de tipo de evento para exibir esses eventos.  
- OU -  
Desmarque a caixa de tipo de evento para ocultar esses eventos.

### 5.2.16 MailGuard: Excluir endereços de e-mail da verificação

Para definir quais endereços de email (remetentes) devem ser excluídos da verificação do MailGuard (lista branca):

- ▶ Vá até o Centro de controle e selecione a seção **Proteção on-line :: MailGuard**.  
A lista mostra os e-mails recebidos.
- ▶ Realce o email que deseja excluir da verificação do MailGuard.
- ▶ Clique no ícone apropriado para excluir o email da verificação do MailGuard:



No futuro, o endereço de e-mail selecionado não será mais verificado em busca de vírus e programas indesejados.



No futuro, o endereço de e-mail selecionado não será mais verificado em busca de spam.

O endereço de e-mail do remetente é incluído na lista de exclusões e não será mais verificado quanto a vírus, malwares ou spam .

### **Aviso**

Exclua endereços de email da verificação do MailGuard somente se os remetentes forem totalmente confiáveis.



### **Nota**

Em Configuração, em MailGuard :: Geral :: Exceções, é possível adicionar outros endereços de e-mail à lista de exclusões ou remover endereços de e-mail dessa lista.

## 5.2.17 MailGuard: Treinar o módulo antispam

O módulo antispam contém um banco de dados de treinamento. Seus critérios de classificação individuais são registrados nesse banco de dados de treinamento. Com o passar do tempo, os filtros internos, os algoritmos e os critérios de avaliação de spam se adaptam automaticamente a seus critérios pessoais.

Para classificar os e-mails para o banco de dados de treinamento:

- ▶ Vá até o Centro de controle e selecione a seção **Proteção on-line :: MailGuard**.  
A lista mostra os e-mails recebidos.
- ▶ Realce o e-mail que deseja classificar.
- ▶ Clique no ícone apropriado para identificar o e-mail como spam  ou desejado, isto é, um “bom” e-mail .

O e-mail é inserido no banco de dados de treinamento e aplicado ao próximo processo de reconhecimento de spam.

### **Nota**

Você pode excluir o banco de dados de treinamento na configuração em MailGuard:: Geral :: AntiSpam.

## 5.2.18 FireWall: Selecionar o nível de segurança para o FireWall

É possível escolher entre vários níveis de segurança. Dependendo do escolhido, você terá diferentes opções de configuração da regra do adaptador.

Os seguintes níveis de segurança estão disponíveis:

- **Baixo**
  - Inundação e verificação de porta são detectadas.
- **Médio**
  - Os pacotes suspeitos de TCP e UDP são descartados.
  - Inundação e verificação de porta são evitadas.
- **Alto**
  - O computador não está visível na rede.

- As conexões externas são bloqueadas.
- Inundação e verificação de porta são evitadas.
- **Usuário**
  - Regras definidas pelo usuário: se esse nível de segurança for selecionado, o programa reconhecerá automaticamente que as regras do adaptador foram modificadas.

### Nota

A configuração padrão de nível de segurança para todas as regras predefinidas do Avira FireWall é **Alto**

Para definir o nível de segurança para o FireWall:

- ▶ Vá até o Centro de controle e selecione a seção **Proteção on-line :: . FireWall**.
- ▶ Mova o controle deslizante até o nível de segurança desejado.  
O nível de segurança selecionado é aplicado imediatamente.

### 5.2.19 Backup: Criar backups manualmente

A ferramenta de backup do Centro de controle permite que você faça backup de seus dados pessoais com rapidez e facilidade. No Avira Backup, você pode criar backups espelhados que permitem salvar e armazenar seus dados mais recentes usando o mínimo de recursos. O Avira Backup permite verificar seu dados quanto a vírus e malware durante o processo de backup. Os arquivos infectados não são salvos.

### Nota


Diferente dos backups de versão, os backups espelhados não salvam versões de backup individuais. O backup espelhado contém os dados armazenados no momento do último backup. No entanto, se os arquivos do armazenamento de dados salvo forem excluídos, nenhuma correspondência ocorrerá no próximo backup, isto é, os arquivos excluídos ainda estarão disponíveis no backup.

### Nota

Com as configurações padrão do Avira Backup, somente os arquivos modificados são salvos e os arquivos são verificados quanto à presença de vírus e malwares. Você pode alterar essas definições na configuração em Backup::Configurações.

Para salvar seus dados usando a ferramenta de backup:

- ▶ No Centro de Controle, selecione a seção **Ferramentas::Backup**.  
Os perfis de backup predefinidos são exibidos.
- ▶ Selecione um dos perfis de backup predefinidos.  
-OU-
- ▶ Adapte o perfil de backup *Seleção manual*.  
-OU-
- ▶ Criar um novo perfil de backup
- ▶ Insira um local de salvamento para o perfil selecionado na caixa *Diretório de destino*.  
O local de salvamento do backup pode ser um diretório do seu computador, uma unidade de rede conectada ou um disco removível, como um pendrive ou um disquete.

- ▶ Clique no ícone  - :

A janela *Avira Backup* é exibida e o backup começa. O status e os resultados do backup são exibidos na janela de backup.

Se desejar modificar um perfil de backup:

- ▶ No perfil de verificação, expanda a árvore de arquivos *Seleção manual* para que todas as unidades e todos os diretórios a serem salvos sejam abertos:
  - Clique no ícone + : o próximo nível do diretório é exibido.
  - Clique no ícone - : o próximo nível do diretório é ocultado.
- ▶ Realce os nós e diretórios a serem salvos clicando na caixa do nível de diretório correspondente:


As seguintes opções estão disponíveis, para selecionar diretórios:

- Diretório, incluindo os subdiretórios (marca de verificação preta)
- Diretório, sem os subdiretórios (marca de verificação verde)
- Subdiretórios de apenas um diretório (marca de verificação cinza; os subdiretórios têm marcas de verificação pretas)
- Nenhum diretório (sem marca de verificação)

Se desejar criar um novo perfil de backup:

- ▶ Clique no ícone  **Criar novo perfil.**

O perfil *Novo perfil* aparece abaixo dos perfis criados anteriormente.

- ▶ Quando apropriado, forneça um nome ao perfil de backup clicando no ícone .
- ▶ Realce os nós e diretórios a serem salvos clicando na caixa de seleção de cada nível de diretório.


As seguintes opções estão disponíveis, para selecionar diretórios:

- Diretório, incluindo os subdiretórios (marca de verificação preta)
- Diretório, sem os subdiretórios (marca de verificação verde)
- Subdiretórios de apenas um diretório (marca de verificação cinza; os subdiretórios têm marcas de verificação pretas)
- Nenhum diretório (sem marca de verificação)

### 5.2.20 Backup: Criar backups de dados automáticos

Essa seção mostra como iniciar um trabalho para criar backups de dados automáticos:

- ▶ No Centro de Controle, selecione a seção **Gerenciamento::Programador**.

- ▶ Clique no ícone .

A caixa de diálogo *Nome e descrição do trabalho* é exibida.

- ▶ Dê um nome ao trabalho e, quando apropriado, uma descrição.
- ▶ Clique em **Avançar**.

A caixa de diálogo *Tipo de trabalho* é exibida.

- ▶ Selecione **Trabalho de backup**.
- ▶ Clique em **Avançar**.

A caixa de diálogo *Selecionar perfil* é exibida.

- ▶ Selecione o perfil a ser verificado.

### Nota

Somente os perfis de backup com um local de salvamento definido são exibidos.

- ▶ Clique em **Avançar**.

A caixa de diálogo *Tempo do trabalho* é exibida.

- ▶ Selecione um horário para a verificação:

- **Imediatamente**
- **Diariamente**
- **Semanalmente**
- **Intervalo**
- **Única**
- **Login**
- **Plug&Play**

Um backup sempre será criado para o evento Plug&Play se o disco removível selecionado como local de salvamento do perfil de backup estiver conectado ao computador. O evento de backup Plug&Play requer a inserção de um pendrive como local de salvamento.

- ▶ Quando apropriado, especifique uma data de acordo com a seleção.
- ▶ Quando apropriado, selecione as seguintes opções adicionais (a disponibilidade depende do tipo de trabalho):
  - **Repetir trabalho se o tempo já tiver expirado**

Os trabalhos antigos são executados agora porque não foram executados no horário programado (por exemplo, o computador foi desligado).

- ▶ Clique em **Avançar**.

A caixa de diálogo *Selecionar modo de exibição* é exibida.

- ▶ Selecione o modo de exibição da janela do trabalho:

- **Minimizar**: somente barra de andamento
- **Maximizar**: janela de backup inteira
- **Ocultar**: sem a janela de backup

- ▶ Clique em **Concluir**.

O trabalho recém criado aparece na página inicial da seção *Gerenciador :: Seção Programador* com o status ativado (marca de verificação).

- ▶ Quando apropriado, desative os trabalhos que não devem ser executados.

Use os ícones a seguir para definir seus trabalhos ainda mais:



Exibir propriedades de um trabalho



Modificar trabalho



Excluir trabalho



Iniciar trabalho



Interromper trabalho





## 6 Scanner

Com o componente Scanner, você pode realizar verificações direcionadas (sob demanda) em busca de vírus e programas indesejados. As seguintes opções estão disponíveis para verificação de arquivos infectados:

- **Verificação sob demanda através do menu de contexto**

A verificação por demanda através do menu de contexto (botão direito do mouse, entrada **Verificar arquivos selecionados com AntiVir**) é recomendada se, por exemplo, você deseja verificar arquivos e diretórios individuais. Outra vantagem é o fato de que não é necessário iniciar primeiro o Centro de controle para realizar uma verificação por demanda através do menu de contexto.

- **Verificação sob demanda através do método de arrastar e soltar**

Quando um arquivo ou diretório é arrastado na janela do programa do Centro de controle, o Scanner verifica o arquivo ou diretório e todos os subdiretórios contidos. Esse procedimento é recomendado se você deseja verificar arquivos e diretórios individuais que foram salvos, por exemplo, em sua área de trabalho.

- Verificação sob demanda através de perfis

Esse procedimento é recomendado se você deseja verificar regularmente alguns diretórios e unidades (por exemplo, seu diretório de trabalho ou as unidades nas quais você armazena novos arquivos regularmente). Você não precisa selecionar esses diretórios e unidades novamente em cada nova verificação; basta selecionar o perfil relevante.

- **Verificação por demanda através do Programador**

O Programador permite que você realize verificações controladas por tempo.

Processos especiais são necessários ao verificar em busca de rootkits e vírus de setor de inicialização e ao verificar os processos ativos. As seguintes opções estão disponíveis:

- Verificar rootkits através do perfil de verificação *Verificar rootkits e malware ativo*
- Verificar processos ativos através do perfil de verificação **Processos ativos**
- Verificar vírus do setor de inicialização através do comando **Verificar vírus do setor de inicialização** no menu **Extras**

## 7 Atualizações

A eficiência do software antivírus depende de como o programa é atualizado, especialmente o arquivo de definição de vírus e o mecanismo de verificação. Para executar as atualizações regulares, o componente Atualizador é integrado ao AntiVir. O Atualizador garante que o programa AntiVir esteja sempre atualizado e permite lidar com os novos vírus que aparecem todos os dias. O Atualizador atualiza os seguintes componentes:

- Arquivo de definição de vírus:

O arquivo de definição de vírus contém os padrões de vírus dos programas prejudiciais usados pelo programa AntiVir para verificar a presença de vírus e malwares e reparar objetos infectados.

- Mecanismo de verificação:

O mecanismo de verificação contém os métodos usados pelo programa AntiVir para verificar a presença de vírus e malwares.

- Arquivos do programa (atualização do produto):

Os pacotes de atualização do produto disponibilizam funções adicionais para os componentes individuais do programa.

Uma atualização verifica se o arquivo de definição de vírus e o mecanismo de verificação estão atualizados e, se necessário, implementa uma atualização. Dependendo das configurações definidas, o Atualizador também realiza uma atualização do produto ou informa que existem atualizações disponíveis. Depois da atualização do produto, talvez seja necessário reiniciar o sistema do computador. Se apenas o arquivo de definição de vírus e o mecanismo de verificação forem atualizados, o computador não precisará ser reiniciado.

### **Nota**

Por motivos de segurança, o Atualizador verifica se o arquivo de hosts do Windows do seu computador foi alterado de modo que, por exemplo, o URL de atualização foi manipulado por malwares e desvia o Atualizador de sites de download indesejados. Se o arquivo de hosts do Windows tiver sido manipulado, isso será mostrado no arquivo de relatório do Atualizador.

Uma atualização é executada automaticamente no seguinte intervalo: 2 horas. Você pode editar ou desativar a atualização automática na configuração (Configuração::Atualizar).

No Centro de controle, no Programador, você pode criar trabalhos de atualização adicionais que são executados pelo Atualizador nos intervalos especificados. Você também pode iniciar uma atualização manualmente:

- No Centro de controle: no menu Atualizar e na seção Status
- através do menu de contexto do ícone da bandeja

As atualizações podem ser obtidas na Internet através de um servidor da Web do fabricante. A conexão de rede existente é a conexão padrão com os servidores de download da Avira GmbH. Você pode alterar essa configuração padrão na Configuração em Geral :: Atualizar.

## 8 Avira FireWall :: Visão geral

O Avira FireWall monitora e regulamenta o tráfego de entrada e saída de dados do sistema de seu computador e protege você contra diversos ataques e ameaças da Internet: Com base nas diretrizes de segurança, o tráfego de entrada ou saída de dados ou a escuta nas portas será permitido ou negado. Você receberá uma notificação na área de trabalho se o Avira FireWall negar a atividade de rede e, assim, bloquear as conexões de rede. As seguintes opções estão disponíveis para configurar o Avira FireWall:

- definindo o nível de segurança no Centro de controle

Você pode definir um nível de segurança no Centro de controle. Os níveis de segurança *baixo*, *médio* e *alto* contêm várias regras de segurança complementares com base em filtros de pacote. Essas regras de segurança são salvas como regras de adaptador predefinidas na Configuração, em FireWall::Regras do adaptador.

- salvando ações na janela Evento de rede

Quando um aplicativo primeiro tenta criar uma conexão de rede ou Internet, a janela pop-up *Evento de rede* é exibida. A janela *Evento de rede* permite que o usuário decida se a atividade de rede do aplicativo deve ser permitida ou negada. Se a opção **Salvar ação para este aplicativo** for ativada, a ação será criada como uma regra de aplicativo e será salva na configuração em FireWall::Regras de aplicativo. Ao salvar as ações na janela Evento de rede, você tem acesso a um conjunto de regras para as atividades de rede dos aplicativos.

### Observação

Para os aplicativos de fornecedores confiáveis, o acesso à rede é permitido por padrão, a não ser que haja uma regra do adaptador proibindo esse acesso. Você pode remover fornecedores da lista de fornecedores confiáveis.

- criando regras de adaptador e aplicativos na Configuração

Você pode alterar regras de adaptador predefinidas ou criar novas regras na Configuração. O nível de segurança do FireWall será definido automaticamente como o valor *Usuário* se você adicionar ou alterar regras de adaptador.

Com as regras de aplicativo, você pode definir regras de monitoramento específicas para aplicativos:

Você pode usar regras de aplicativo simples para definir se todas as atividades de rede de um software devem ser negadas ou permitidas ou se devem ser manipuladas através da janela pop-up *Evento de rede*.

Na configuração avançada de *Regras de aplicativo*, é possível definir filtros de pacote diferentes para um aplicativo, que são executados como regras de aplicativo específicas.

**Observação**

Existem dois modos diferentes das regras de aplicativo: *Com privilégios e Filtrado*. Para as regras de aplicativo no modo *filtrado*, as regras de adaptador relevantes têm prioridade, isto é, são executadas após a regra de aplicativo. Desse modo, o acesso à rede pode ser negado devido a um nível de segurança alto ou a regras de adaptador correspondentes. Para as regras de aplicativo no modo *com privilégios*, as regras de adaptador são ignoradas. Se os aplicativos forem permitidos no modo *com privilégios*, o acesso à rede sempre será permitido.

## 9 Backup

Existem várias opções disponíveis para criar um backup de seus dados:

### **Backup através da ferramenta de backup**

Você pode usar a ferramenta de backup para selecionar ou criar perfis de backup e iniciar o backup de um perfil selecionado manualmente.

### **Backup através de um trabalho de backup no Programador**

O Programador permite que você crie trabalhos de backup programados ou controlados por evento. O Programador executa os trabalhos de backup automaticamente. Esse processo é útil especialmente se você desejar fazer backups regulares de dados específicos.

## 10 Perguntas frequentes, dicas

Este capítulo contém todas as informações relevantes para a solução de problemas e dicas adicionais sobre o uso do programa AntiVir.

consulte o Capítulo Solução de problemas

consulte o Capítulo Comandos do teclado

consulte o Capítulo Central de segurança do Windows

### 10.1 Ajuda caso ocorra um problema

Aqui você encontrará informações sobre causas e soluções de possíveis problemas.

- A mensagem de erro *O arquivo de licença não pode ser aberto* é exibida.
- O AntiVir MailGuard não funciona.
- Não haverá nenhuma conexão de rede disponível em uma máquina virtual (por exemplo, VMWare, PC virtual...) se o Avira FireWall estiver instalado na máquina do host e o nível de segurança do Avira FireWall estiver definido como médio ou alto.
- A conexão VPN (Virtual Private Network, Rede privada virtual) será bloqueada se o nível de segurança do Avira FireWall estiver definido como médio ou alto.
- Um email enviado por uma conexão TSL foi bloqueado pelo MailGuard.
- O bate-papo on-line não está funcionando: as mensagens de bate-papo não serão exibidas

#### **A mensagem de erro *O arquivo de licença não pode ser aberto* é exibida.**

Motivo: o arquivo está criptografado.

- ▶ Para ativar a licença, você não precisa abrir o arquivo, basta salvá-lo no diretório do programa.

#### **A mensagem de erro *Falha de conexão ao baixar o arquivo...* é exibida ao tentar iniciar uma atualização.**

Motivo: sua conexão com a Internet não está ativa. Não foi possível estabelecer a conexão com o servidor da Web na Internet.

- ▶ Teste se outros serviços da Web, como WWW ou e-mail, funcionam. Em caso negativo, restabeleça a conexão com a Internet.

Motivo: não foi possível conectar o servidor proxy.

- ▶ Verifique se o login do servidor proxy foi alterado e adapte-o à sua configuração se necessário.

Motivo: o arquivo update.exe não foi totalmente aprovado por seu firewall pessoal.

- ▶ Verifique se o arquivo update.exe foi totalmente aprovado por seu firewall pessoal.

Caso contrário:

- ▶ Verifique suas configurações na Configuração (modo de especialista) em Geral::Atualizar suas configurações.

### **Vírus e malwares não podem ser movidos nem excluídos.**

Motivo: o arquivo foi carregado pelo Windows e está ativo.

- ▶ Atualize o produto AntiVir.
- ▶ Se você usar o sistema operacional Windows XP, desative a restauração do sistema.
- ▶ Inicie o computador no modo de segurança.
- ▶ Inicie o programa AntiVir e a Configuração (modo de especialista).
- ▶ Selecione Scanner::Fazer verificação::Arquivos::Todos os arquivos e confirme a janela com **OK**.
- ▶ Inicie uma verificação de todas as unidades locais.
- ▶ Inicie o computador no modo normal.
- ▶ Realize uma verificação no modo normal.
- ▶ Se nenhum outro vírus ou malware for encontrado, ative a restauração do sistema se estiver disponível e for necessário utilizá-la.

### **O status do ícone da bandeja está desativado.**

Motivo: o AntiVir Guard está desativado.

- ▶ No Centro de controle, na seção Visão geral::Status, na área do AntiVir Guard, clique no link **Ativar**.

Motivo: o AntiVir Guard está bloqueado por um firewall.

- ▶ Defina uma aprovação geral para o AntiVir Guard na configuração do seu firewall. O AntiVir Guard funciona apenas com o endereço 127.0.0.1 (localhost). Uma conexão com a Internet não é estabelecida. O mesmo se aplica ao AntiVir MailGuard.

Caso contrário:

- ▶ Verifique o tipo de inicialização do serviço do AntiVir Guard. Se necessário, ative o serviço: na barra de tarefas, selecione "Iniciar | Configurações | Painel de controle". Inicie o painel de configuração "Serviços" clicando duas vezes nele (no Windows 2000 e no Windows XP, o applet de serviços está localizado no subdiretório "Ferramentas administrativas"). Localize a entrada do *Avira AntiVir Guard*. "Automático" deve ser inserido como o tipo de inicialização e "Iniciado" como o status. Se necessário, inicie o serviço manualmente selecionando a linha relevante e o botão "Iniciar". Se uma mensagem de erro for exibida, verifique a exibição do evento.

### **O computador fica extremamente lento quando faço backup dos dados.**

Motivo: Durante o procedimento de backup, o AntiVir Guard verifica todos os arquivos que estão sendo usados pelo procedimento de backup.

- ▶ Na Configuração (modo de especialista), escolha Guard::Verificar::Exceções e insira os nomes dos processos do software de backup.

### **Meu firewall reporta o AntiVir Guard e o AntiVir MailGuard imediatamente depois da ativação.**

Motivo: a comunicação com o AntiVir Guard e o AntiVir MailGuard ocorre através do protocolo de Internet TCP/IP. Um firewall monitora todas as conexões através desse protocolo.

▶ Defina uma aprovação geral para o AntiVir Guard e o AntiVir MailGuard. O AntiVir Guard funciona apenas com o endereço 127.0.0.1 (localhost). Uma conexão com a Internet não é estabelecida. O mesmo se aplica ao AntiVir MailGuard.

### **O AntiVir MailGuard não funciona.**

Verifique o funcionamento correto do AntiVir MailGuard com a ajuda das listas de verificação a seguir se ocorrerem problemas com o AntiVir MailGuard.

#### **Lista de verificação**

- ▶ Verifique se seu cliente de e-mail estabelece conexão com o servidor via Kerberos, APOP ou RPA. No momento, não há suporte para esses métodos de verificação.
- ▶ Verifique se o seu cliente de email se conecta ao servidor usando SSL (também conhecido como TSL – Transport Layer Security). O AntiVir MailGuard não é compatível com SSL e, portanto, é finaliza qualquer conexão SSL criptografada. Se você quiser usar conexões SSL criptografadas sem que elas sejam protegidas pelo MailGuard, será necessário usar uma porta que não seja monitorada pelo MailGuard para conexão. As portas monitoradas pelo MailGuard podem ser definidas na configuração, em MailGuard::Verificar.
- ▶ O serviço do AntiVir MailGuard está ativo? Se necessário, ative o serviço: na barra de tarefas, selecione "Iniciar | Configurações | Painel de controle". Inicie o painel de configuração "Serviços" clicando duas vezes nele (no Windows 2000 e no Windows XP, o applet de serviços está localizado no subdiretório "Ferramentas administrativas"). Localize a entrada do *Avira AntiVir MailGuard*. "Automático" deve ser inserido como o tipo de inicialização e "Iniciado" como o status. Se necessário, inicie o serviço manualmente selecionando a linha relevante e o botão "Iniciar". Se uma mensagem de erro for exibida, verifique a exibição do evento. Se isso não funcionar, desinstale por completo o programa AntiVir em "Iniciar | Configurações | Painel de controle | Adicionar ou remover programas", reinicie o computador e reinstale o programa AntiVir.

#### **Geral**

- ▶ As conexões POP3 criptografadas via SSL (Secure Sockets Layer, também conhecido como TLS - Transport Layer Security, Segurança da camada de transporte) não podem ser protegidas no momento e são ignoradas.
- ▶ No momento, a verificação do servidor de email só é permitida através de "senhas". "Kerberos" e "RPA" não têm suporte atualmente.
- ▶ O programa AntiVir não verifica os e-mails enviados em busca de vírus e programas indesejados.

#### **Nota**

Recomendamos que você instale as atualizações da Microsoft regularmente para preencher todas as lacunas de segurança.

**Não haverá nenhuma conexão de rede disponível em uma máquina virtual (por exemplo, VMWare, PC virtual...) se o Avira FireWall estiver instalado na máquina do host e o nível de segurança do Avira FireWall estiver definido como médio ou alto.**



Se o Avira FireWall estiver instalado em um computador que tem uma máquina virtual (por exemplo, VMWare, PC virtual etc.) em execução, o firewall bloqueará todas as conexões de rede da máquina virtual quando o nível de segurança do Avira FireWall estiver definido como médio ou alto. Se o nível de segurança estiver definido como baixo, o FireWall funcionará conforme o esperado.

Motivo: A máquina virtual simula uma placa de rede através do software. Essa emulação encapsula os pacotes de dados do sistema convidado em pacotes especiais (pacotes IDP) e os encaminha por meio de um gateway externo para o sistema do host. O Avira FireWall rejeita esses pacotes externos, com nível de segurança médio.

Para evitar esse comportamento, faça o seguinte:

- ▶ Vá até o Centro de controle e selecione a seção **Proteção on-line :: FireWall**.
- ▶ Clique no link **Configuração**.
- ▶ A caixa de diálogo *Configuração* é exibida. Você está na seção de configuração *Regras de aplicativo*.
- ▶ Ative a opção **Modo de especialista**.
- ▶ Selecione a seção de configuração **Regras do adaptador**.
- ▶ Clique em **adicionar**.
- ▶ Selecione **UDP** na seção *Regras de entrada*.
- ▶ Digite o **nome** da regra na seção Nome da regra.
- ▶ Clique em **OK**.
- ▶ Verifique se a regra está diretamente acima da regra **Negar todos os pacotes IP**.

### **Aviso**

Essa regra é perigosa em potencial porque permitirá os pacotes UDP sem nenhuma filtragem. Depois de trabalhar com a máquina virtual, volte ao seu nível de segurança anterior.

### **A conexão VPN (Virtual Private Network, Rede privada virtual) será bloqueada se o nível de segurança do Avira FireWall estiver definido como médio ou alto.**

Motivo: esse problema é causado pela última regra **Negar todos os pacotes IP**, que descarta todos os pacotes que não estão em conformidade com nenhuma regra acima deles. O tipo de pacote enviado pelo software da VPN (também conhecidos como pacotes GRE) não se enquadra em nenhuma outra categoria e, portanto, é filtrado por essa regra.

Substitua a regra **Negar todos os pacotes IP** por duas novas regras que negarão os pacotes TCP e UDP. Desse modo, é possível permitir pacotes de outros protocolos.

### **Um email enviado por uma conexão TSL foi bloqueado pelo MailGuard.**

Motivo: a segurança da camada de transporte (TLS: protocolo de criptografia para transferências de dados na Internet) não é compatível com o MailGuard no momento. As seguintes opções estão disponíveis para o envio de e-mails:

- ▶ Use uma porta que não seja a porta 25, que é usada pelo SMTP. Isso não será observado pelo monitoramento do MailGuard.
- ▶ Desative a conexão TSL criptografada e desative o suporte para TSL em seu cliente de e-mail.

► Desative (temporariamente) o monitoramento dos emails enviados por parte do MailGuard na configuração em MailGuard::Verificar.

### **O bate-papo on-line não está funcionando: as mensagens de bate-papo não são exibidas; os dados estão sendo carregados no navegador.**

Esse fenômeno pode ocorrer durante bate-papos que são baseados no protocolo HTTP com "transfer-encoding= chunked".

Motivo: o WebGuard verifica todos os dados enviados em busca de vírus e programas indesejados em primeiro lugar, antes que os dados sejam carregados no navegador da Web. Durante uma transferência de dados com "transfer-encoding= chunked", o WebGuard não consegue determinar o tamanho da mensagem nem o volume de dados.

► Insira a configuração do URL dos bate-papos on-line como uma exceção (consulte Configuração: WebGuard::Exceções).

## 10.2 Atalhos

Os comandos de teclado, também chamados de atalhos, permitem navegar rapidamente através do programa, para recuperar módulos individuais e iniciar ações.

Veja, a seguir, um resumo dos comandos de teclado disponíveis. Mais informações sobre a funcionalidade estão disponíveis no capítulo correspondente da ajuda.

### 10.2.1 Nas caixas de diálogo

<b>Atalho</b>	<b>Descrição</b>
Ctrl + Tab Ctrl + Page down	Navegação no Centro de controle Vai para a próxima seção.
Ctrl + Shift + Tab Ctrl + Page up	Navegação no Centro de controle Vai para a seção anterior.
← ↑ → ↓	Navegação nas seções de configuração Primeiro, use o mouse para definir o foco em uma seção de configuração.
Tab	Altera para a próxima opção ou grupo de opções.
Shift + Tab	Altera para a opção ou grupo de opções anterior.
← ↑ → ↓	Alterna entre as opções de uma lista suspensa marcada ou entre várias opções de um grupo de opções.
Espaço	Ativa ou desativa uma caixa de seleção, se a opção ativa for uma caixa de seleção.
Alt + letra sublinhada	Seleciona a opção ou inicia o comando.

Alt + ↓ F4	Abre a lista suspensa selecionada.
Esc	Fecha a lista suspensa selecionada. Cancela o comando e fecha a caixa de diálogo.
Enter	Inicia o comando da opção ou do botão ativo.

### 10.2.2 Na ajuda

<b>Atalho</b>	<b>Descrição</b>
Alt + Espaço	Exibe o menu do sistema.
Alt + Tab	Alterna entre a ajuda e as outras janelas abertas.
Alt + F4	Fecha a ajuda.
Shift + F10	Exibe o menu de contexto da ajuda.
Ctrl + Tab	Vai para a próxima seção na janela de navegação.
Ctrl + Shift + Tab	Vai para a seção anterior na janela de navegação.
Page up	Muda para o assunto, que é exibido acima do sumário, no índice ou na lista de resultados de pesquisa.
Page down	Muda para o assunto, que é exibido abaixo do assunto atual no sumário, no índice ou na lista de resultados de pesquisa.
Page up Page down	Navega por um assunto.

### 10.2.3 No Centro de controle

#### Geral

<b>Atalho</b>	<b>Descrição</b>
F1	Exibe a ajuda
Alt + F4	Fecha o Centro de controle
F5	Atualizar
F8	Abre a configuração
F9	Iniciar atualização

#### Seção Verificar

<b>Atalho</b>	<b>Descrição</b>
F2	Renomear perfil selecionado
F3	Iniciar verificação com o perfil selecionado

F4	Criar link na área de trabalho para o perfil selecionado
Ins	Criar novo perfil
Del	Excluir perfil selecionado

### Seção FireWall

Atalho	Descrição
Voltar	Propriedades

### Seção Quarentena

Atalho	Descrição
F2	Refazer varredura do objeto
F3	Restaurar objeto
F4	Enviar objeto
F6	Restaurar objeto para...
Voltar	Propriedades
Ins	Adicionar arquivo
Del	Excluir objeto

### Seção Programador

Atalho	Descrição
F2	Editar trabalho
Voltar	Propriedades
Ins	Inserir novo trabalho
Del	Excluir trabalho

### Seção Relatórios

Atalho	Descrição
F3	Exibir arquivo de relatório
F4	Imprimir arquivo de relatório
Voltar	Exibir relatório
Del	Excluir relatório(s)

### Seção Eventos

Atalho	Descrição
F3	Exportar evento(s)

Voltar	Mostrar evento
Del	Excluir evento(s)

## 10.3 Central de segurança do Windows

- Windows XP Service Pack 2 ou superior -

### 10.3.1 Geral

A Central de segurança do Windows verifica o status do computador com relação a importantes aspectos de segurança.

Se algum problema for detectado em um desses pontos importantes (por exemplo, um programa antivírus desatualizado), a Central de segurança emitirá um alerta e fará recomendações sobre como proteger melhor seu computador.

### 10.3.2 A Central de segurança do Windows e o programa AntiVir

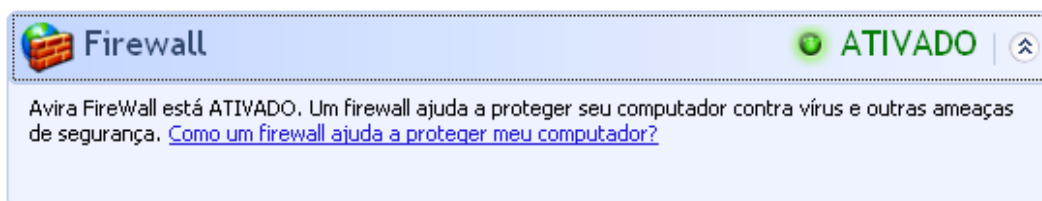
#### FireWall

Você poderá receber as seguintes informações da Central de segurança com relação ao seu firewall:

- FireWall ATIVO/FireWall ativado
- FireWall INATIVO/FireWall desativado

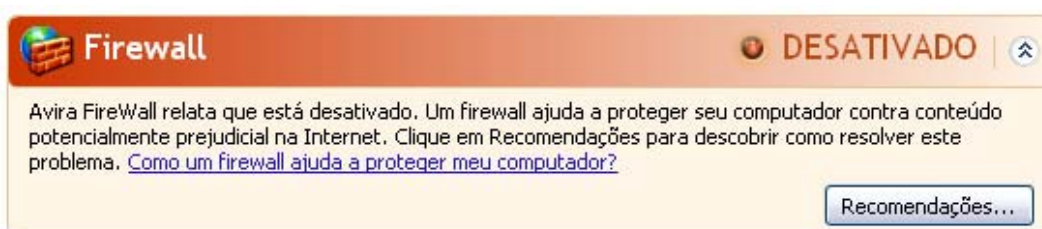
#### **FireWall ATIVO/FireWall desativado**

Após a instalação do programa AntiVir e a desativação do Windows Firewall, a seguinte mensagem será exibida:



#### **FireWall INATIVO/FireWall desativado**

Você receberá a seguinte mensagem assim que desativar o Avira FireWall:



#### **Nota**

Você pode ativar ou desativar o Avira FireWall por meio da guia Status no Centro de controle.

### Aviso

Se o Avira FireWall for desativado, seu computador não impedirá mais o acesso de usuários não autorizados através de uma rede ou da Internet.

### Software de proteção contra vírus/Proteção contra software malicioso

Você poderá receber as seguintes informações da Central de segurança do Windows com relação à proteção contra vírus:

Proteção contra vírus NÃO ENCONTRADA

Proteção contra vírus DESATUALIZADA

Proteção contra vírus ATIVADA

Proteção contra vírus DESATIVADA

Proteção contra vírus NÃO MONITORADA

#### Proteção contra vírus NÃO ENCONTRADA

Essas informações aparecem quando a Central de segurança do Windows não encontra nenhum software antivírus em seu computador.

**Proteção contra vírus** NÃO ENCONTRADO

O Windows não encontrou nenhum programa antivírus neste computador. Programas antivírus ajudam a proteger seu computador contra vírus e outras ameaças de segurança. Clique em Recomendações para obter sugestões de ações a serem tomadas. [Como programas antivírus ajudam a proteger meu computador?](#)

Obs.: O Windows não detecta todos os programas antivírus.

Recomendações...

#### Nota

Instale o programa AntiVir em seu computador para protegê-lo contra vírus e outros programas indesejados.

#### Proteção contra vírus DESATUALIZADA

Se você já tinha instalado o Windows XP Service Pack 2 ou o Windows Vista e, em seguida, instalou o programa AntiVir ou se você instalar o Windows XP Service Pack 2 ou o Windows Vista em um sistema no qual o programa AntiVir já está instalado, a seguinte mensagem será exibida:

**Proteção contra vírus** DESATUALIZADO

AntiVir Desktop relata que pode estar desatualizado. Clique em Recomendações para obter sugestões de ações a serem tomadas. [Como programas antivírus ajudam a proteger meu computador?](#)

Obs.: o Windows não detecta todos os programas antivírus.

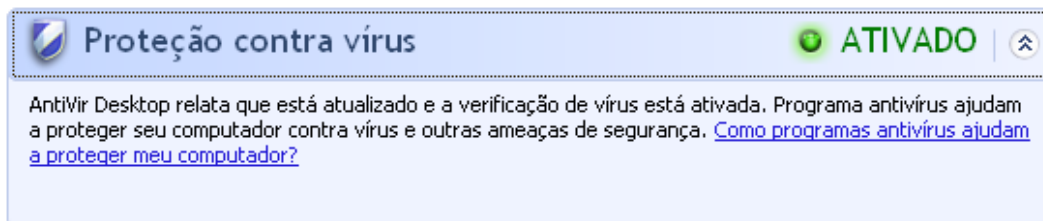
Recomendações...

#### Nota

Para que a Central de segurança do Windows reconheça o programa AntiVir como um produto atualizado, é necessário executar uma atualização após a instalação. Atualize o sistema executando uma atualização.

#### Proteção contra vírus ATIVADA

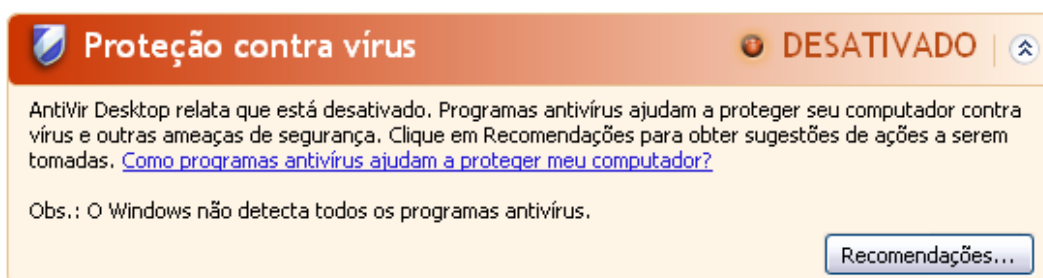
Após a instalação do programa AntiVir e a execução de uma atualização em seguida, a seguinte mensagem será exibida:



O programa AntiVir agora está atualizado e o AntiVir Guard está ativado.

### **Proteção contra vírus DESATIVADA**

A seguinte mensagem será exibida se você desativar o AntiVir Guard ou interromper o serviço do Guard.



### **Nota**

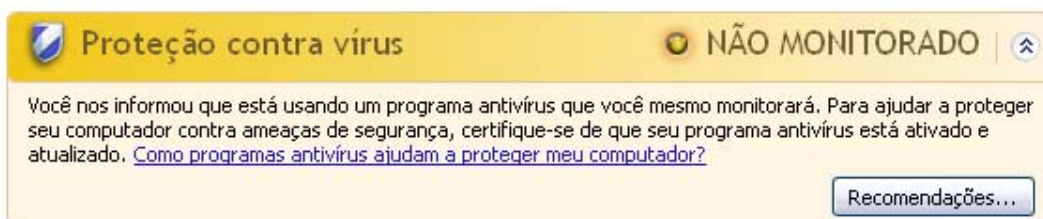
Você pode ativar ou desativar o AntiVir Guard na seção Visão geral::Status do Centro de controle. Você também poderá saber se o AntiVir Guard está ativado observando a presença do guarda-chuva vermelho aberto na barra de tarefas.

### **Proteção contra vírus NÃO MONITORADA**

Se a seguinte mensagem da Central de segurança do Windows for exibida, você decidiu monitorar seu software antivírus por conta própria.

### **Nota**

Essa função não é compatível com o Windows Vista.



### **Nota**

A Central de segurança do Windows é compatível com o programa AntiVir. Você pode ativar essa opção a qualquer momento com o botão "Recomendações..."

### **Nota**

Mesmo que você tenha instalado o Windows XP Service Pack 2 ou o Windows Vista, ainda precisará de uma solução de proteção contra vírus. Embora o Windows XP Service Pack 2 monitore seu software antivírus, ele não contém nenhuma função antivírus. Desse modo, você não tem proteção contra vírus e outros malwares sem uma solução antivírus adicional.

# 11 Vírus e mais

## 11.1 Categorias de ameaça estendidas

### **Discador (DIALER)**

É necessário pagar por alguns serviços disponíveis na Internet. Eles são faturados na Alemanha através de discadores com os números 0190/0900 (ou através dos números 09x0 na Áustria e na Suíça; na Alemanha, o número é definido para mudar para 09x0 a médio prazo). Depois de serem instalados no computador, esses programas garantem uma conexão através de um número de taxa premium que pode ter tarifas muito variadas.

A comercialização de conteúdo on-line pela conta de telefone é legal e pode ser vantajosa para o usuário. Os discadores genuínos não deixam dúvidas de que estão sendo usados deliberada e intencionalmente pelo usuário. Eles são instalados somente no computador do usuário com o consentimento do usuário, que deve ser fornecido através de uma marcação ou solicitação totalmente sem ambiguidade e claramente visível. O processo de discagem dos discadores genuínos é exibido claramente. Além disso, os discadores genuínos mostram os custos incorridos de maneira exata e sem erros.

Infelizmente, também existem discadores que se instalam nos computadores sem serem percebidos de modo duvidoso ou até mesmo com a intenção de enganar o usuário. Por exemplo, eles substituem o link de comunicação de dados padrão do usuário da Internet pelo ISP (Internet Service Provider, Provedor de serviço de Internet) e discam para um número 0190/0900 que geralmente acarreta custos altíssimos sempre que uma conexão é estabelecida. O usuário afetado provavelmente não perceberá até receber a próxima conta de telefone que um discador 0190/0900 indesejado em seu computador discou para um número de taxa premium em cada conexão, resultando em custos significativamente maiores.

Recomendamos que você entre em contato diretamente com a operadora de telefone para solicitar o bloqueio dessa faixa de números para que seja protegido imediatamente contra discadores indesejados (discadores 0190/0900).

O programa AntiVir pode detectar os discadores conhecidos por padrão.

Se a opção **Discadores** estiver ativada com uma marca de verificação na configuração, em Categorias de ameaça estendidas, você receberá um alerta correspondente se um discador for detectado. Agora você pode simplesmente excluir o discador 0190/0900 possivelmente indesejado. No entanto, se for um programa de discagem desejado, você poderá declará-lo como um arquivo excepcional e esse arquivo não será mais verificado no futuro.

### **Jogos (GAMES)**



Os jogos de computador são permitidos, mas não necessariamente no trabalho (talvez na hora do almoço). No entanto, com a variedade de jogos disponíveis para download na Internet, o Campo minado e o jogo da Paciência não são os únicos que fazem parte do dia a dia dos funcionários e dos usuários em geral. Você pode baixar diversos jogos pela Internet. Os jogos por e-mail também estão cada vez mais populares: diversas variações estão em circulação, desde um simples jogo de xadrez até "Batalha naval" (incluindo combates com torpedos): os movimentos correspondentes são enviados para os adversários por programas de e-mail, que jogam em seguida.

Estudos mostram que o número de horas de trabalho dedicadas aos jogos de computador tem atingido proporções economicamente significativas. Portanto, não é surpreendente o fato de cada vez mais empresas procurarem meios para banir os jogos de computador do local de trabalho.

O programa AntiVir reconhece jogos de computador. Se a opção **Jogos** estiver ativada com uma marca de verificação na configuração, em Categorias de ameaça, você receberá um alerta correspondente se o programa AntiVir detectar um jogo. Agora o jogo acabou (literalmente) porque você pode simplesmente excluí-lo.

### Piadas (JOKES)

As piadas servem simplesmente para assustar alguém ou provocar o divertimento de todos sem causar danos. Quando um programa de piadas é carregado, o computador normalmente começa, em algum ponto, a reproduzir um som ou exibir algo incomum na tela. A máquina de lavar na unidade de disco (DRAIN.COM) e o comedor de tela (BUGSRES.COM) são exemplos de piadas.

Mas tome cuidado! Todos os sintomas dos programas de piadas também podem se originar de um vírus ou cavalo de Troia. Em último caso, os usuários terão um choque ou entrarão em pânico, o que pode causar danos reais.

Graças à extensão das rotinas de verificação e identificação, o programa AntiVir pode detectar programas de piada e eliminá-los como programas indesejados se necessário. Se a opção **Piadas** estiver ativada com uma marca de verificação na configuração, em Categorias de ameaça, um alerta correspondente será acionado se um programa de piadas for detectado.

### Risco de privacidade de segurança (SPR)

Software que pode comprometer a segurança do seu sistema, iniciar atividades do programa indesejado, danificar sua privacidade ou espionar o comportamento do usuário e, assim, pode ser indesejado.

O programa AntiVir detecta softwares de "Risco de privacidade de segurança". Se a opção **Risco de privacidade de segurança** estiver ativada com uma marca de verificação na configuração, em Categorias de ameaça estendidas, você receberá um alerta correspondente se o programa AntiVir detectar esse software.

### Cientes back-door (BDC)

Para roubar dados ou manipular computadores, um programa de servidor back-door é introduzido no sistema sem o conhecimento do usuário. Esse programa pode ser controlado por terceiros com o uso de um software de controle back-door (cliente) via Internet ou por uma rede.

O programa AntiVir reconhece "softwares de controle back-door". Se a opção **Softwares de controle back-door** estiver ativada com uma marca de verificação na configuração, em Categorias de ameaça estendidas, você receberá um alerta correspondente se o programa AntiVir detectar esse software.

### **Adware/Spyware (ADSPY)**

Software que exhibe propaganda ou software que envia dados pessoais do usuário para terceiros, geralmente sem seu conhecimento ou consentimento, e, por esse motivo, pode ser indesejado.

O programa AntiVir reconhece "Adware/Spyware". Se a opção **Adware/Spyware (ADSPY)** estiver ativada com uma marca de verificação na configuração, em Categorias de ameaça estendidas, você receberá um alerta correspondente se o programa AntiVir detectar o adware ou spyware.

### **Compactadores de tempo de execução incomuns (PCK)**

Arquivos que foram compactados com um compactador incomum de tempo de execução e, assim, podem ser classificados como possivelmente suspeitos.

O programa AntiVir reconhece "Compactadores de tempo de execução incomuns". Se a opção **Compactadores de tempo de execução incomuns** estiver ativada com uma marca de verificação na configuração, em Categorias de ameaça estendidas, você receberá um alerta correspondente se o programa AntiVir detectar esses compactadores.

### **Arquivos com extensão dupla (HEUR-DBLEXT)**

Arquivos executáveis que ocultam a extensão real do arquivo de uma maneira suspeita. Esse método de camuflagem normalmente é usado por malwares.

O programa AntiVir reconhece "Arquivos com extensão dupla". Se a opção **Arquivos com extensão dupla (HEUR-DBLEXT)** estiver ativada com uma marca de verificação na configuração, em Categorias de ameaça estendidas, você receberá um alerta correspondente se o programa AntiVir detectar esses arquivos.

### **Phishing**

Phishing, também conhecido como *brand spoofing* (falsificação de marca), é uma forma mais inteligente de roubo de dados cujo objetivo são clientes ou possíveis clientes de provedores de serviços de Internet, bancos, serviços bancários on-line e autoridades de registro.

Ao enviar seu endereço de email pela Internet, preencher formulários on-line, acessar grupos de notícias ou sites, seus dados podem ser roubados por "rastreadores da Internet" e usados sem sua permissão para cometer fraudes e outros crimes.

O programa AntiVir reconhece "Phishing". Se a opção **Phishing** estiver ativada com uma marca de verificação na configuração, em Categorias de ameaça estendidas, você receberá um alerta correspondente se o programa AntiVir detectar esse comportamento.

### **Aplicativo (APPL)**

O termo APPL refere-se a um aplicativo que pode envolver um risco quando for usado ou é de origem duvidosa.

O programa AntiVir reconhece "Aplicativo (APPL)". Se a opção **Aplicativo (APPL)** estiver ativada com uma marca de verificação na configuração, em Categorias de ameaça estendidas, você receberá um alerta correspondente se o programa AntiVir detectar esse comportamento.

## 11.2 Vírus e outros malwares

### Adware

Adware é um software que apresenta anúncios de banner ou janelas pop-up através de uma barra que aparece na tela do computador. Esses anúncios normalmente não podem ser removidos e, por isso, estão sempre visíveis. Os dados de conexão fornecem várias conclusões quanto ao comportamento de uso e são problemáticos em termos de segurança de dados.

### Backdoors

Um backdoor pode obter acesso a um computador observando os mecanismos de segurança de acesso do computador.

Um programa que está sendo executado em segundo plano, em geral, concede ao invasor direitos quase ilimitados. Os dados pessoais do usuário podem ser vistos com a ajuda de um backdoor. Porém, são usados principalmente para instalar outros worms ou vírus de computador no sistema relevante.

### Vírus de inicialização

O setor mestre ou de inicialização dos discos rígidos é infectado principalmente através de vírus do setor de inicialização. Eles substituem informações importantes necessárias para a execução do sistema. Uma das consequências indesejáveis é que não é mais possível carregar o sistema do computador...

### Bot-Net

Um bot net é definido como uma rede remota de computadores (na Internet) que é composta por bots que se comunicam entre si. Um bot-net pode comprometer vários computadores invadidos por programas (mais conhecidos como worms, cavalos de Troia) executados sob um comando e uma infraestrutura de controle comuns. Os bot-nets possuem várias finalidades, entre elas, ataques de negação de serviço, muitas vezes, sem o conhecimento do usuário do PC afetado. O grande potencial dos bot-nets é que as redes podem alcançar o crescimento de milhares de computadores e o total de larguras de banda ultrapassa o acesso à Internet mais convencional.

### Exploit

Um exploit (lacuna de segurança) é um programa de computador ou script que se aproveita de um bug, glitch ou uma vulnerabilidade que leva ao escalonamento de privilégios ou negação de serviço em um sistema de computador. Por exemplo, um tipo de exploração são ataques na Internet com a ajuda de pacotes de dados manipulados. Os programas podem ser infiltrados para obter acesso de nível mais alto.

### Hoaxes

Há muitos anos, os usuários da Internet e outros usuários de rede têm recebido alertas sobre vírus disseminados intencionalmente por email. Esses alertas são difundidos via e-mail com a solicitação de que sejam enviados ao maior número possível de amigos e outros usuários para avisá-los do "perigo".

### Honeypot

Honeypot é um serviço (programa ou servidor) que é instalado em uma rede. Sua função é monitorar uma rede e registrar ataques. Um usuário legítimo da rede não tem conhecimento desse serviço, por isso ele nunca é avisado. Se um invasor examinar as falhas na rede e usar os serviços oferecidos por um honeypot, ele será registrado e será acionado um alerta.

### Vírus de macro

Os vírus de macro são pequenos programas escritos na linguagem de macro de um aplicativo (por exemplo, WordBasic no WinWord 6.0) que, em geral, só se propagam em documentos desse aplicativo. Por causa disso, eles também são chamados de vírus de documentos. Para se tornarem ativos, eles precisam que aplicativos correspondentes sejam ativados e que uma das macros infectadas seja executada. Diferentemente dos vírus "normais", os vírus de macro não atacam arquivos executáveis, mas atacam os documentos do aplicativo host correspondente.

### Pharming

Pharming é uma manipulação do arquivo de host dos navegadores para desviar as consultas para sites falsos. É mais um desenvolvimento do phishing clássico. Os vigaristas de pharming operam seus próprios farms de servidor enormes nos quais os sites falsos são armazenados. Pharming foi estabelecido como um termo geral para os diversos tipos de ataques de DNS. No caso da manipulação do arquivo de host, uma manipulação específico de um sistema é realizada como a ajuda de um cavalo de Troia ou vírus. Em resultado disso, o sistema agora só pode acessar sites falsos, mesmo se o endereço da Web correto for inserido.

### Phishing

Phishing significa pescar os dados pessoais do usuário da Internet. Os praticantes de phishing geralmente enviam para suas vítimas cartas aparentemente oficiais, como e-mails, cujo objetivo é levá-los a revelar informações confidenciais para os criminosos em boa fé, especialmente nomes de usuário e senhas ou PINs e TANs de contas bancárias online. Com os detalhes de acesso roubados, os fraudadores podem assumir a identidade de suas vítimas e realizar transações em nome delas. Obviamente, os bancos e as seguradoras nunca pedem números de cartão de crédito, PINs, TANs ou outros detalhes de acesso por e-mail, SMS ou telefone.

### Vírus polimorfos

Os vírus polimorfos são verdadeiros mestres do disfarce. Eles alteram seus próprios códigos de programação e, por isso, são muito difíceis de se detectar.

### **Vírus de programa**

Um vírus de computador é um programa capaz de se anexar a outros programas depois de ser executado e causar uma infecção. Os vírus se multiplicam diferentemente de bombas lógicas e cavalos de Troia. Ao contrário de um worm, um vírus sempre precisa de um programa como host, no qual ele deposita seu código infeccioso. Como regra, a execução do programa do host em si não é alterada.

### **Rootkit**

Um rootkit é uma coleção de ferramentas de softwares que são instaladas após o sistema do computador ser invadido para dissimular logins do invasor, ocultar processos e registrar dados – em outras palavras: ferramentas para deixar os invasores invisíveis. Eles tentam atualizar programas de espionagem já instalados e reinstalar spywares excluídos.

### **Vírus de script e worms**

Esses vírus são extremamente fáceis de programar e, se a tecnologia necessária estiver à disposição, podem se difundir por e-mail para o mundo inteiro em questão de horas.

Os vírus de script e worms usam uma das linguagens de script, como Javascript, VBScript e outras, para se infiltrar em novos scripts ou se propagar pela invocação de funções do sistema operacional. Isso acontece com frequência por e-mail ou através da troca de arquivos (documentos).

Um worm é um programa que se multiplica, mas não infecta o host. Consequentemente, os worms podem não fazer parte das sequências de outros programas. Muitas vezes, só eles são capazes de se infiltrar em algum tipo de programa nocivo em sistemas com medidas de segurança restritivas.

### **Spyware**

Spyware é o programa espião que intercepta ou assume o controle parcial da operação de um computador sem o consentimento informado do usuário. O spyware é criado para explorar computadores infectados para fins comerciais.

### **Cavalos de Troia**

Os cavalos de Troia são bastante comuns hoje em dia. Os cavalos de Troia incluem programas que parecem ter uma determinada função, mas mostram sua verdadeira imagem depois de serem executados, quando carregam uma função diferente, que, na maioria dos casos, é destrutiva. Os cavalos de Troia não podem se multiplicar, o que os diferencia dos vírus e worms. A maioria tem um nome interessante (SEXO.EXE ou EXECUTE.EXE) com a intenção de induzir o usuário a iniciar o cavalo de Troia. Logo depois da execução, eles se tornam ativos e podem, por exemplo, formatar o disco rígido. Um dropper é uma forma especial de cavalo de Troia que "solta" vírus, isto é, incorpora vírus no sistema do computador.

### **Zumbi**

Um computador zumbi é aquele infectado por programas de malware e que permite aos hackers invadirem as máquinas por controle remoto para fins ilegais. No comando, o computador afetado inicia, por exemplo, ataques DoS (Negação de serviço) ou envia spam e e-mails de phishing.

## 12 Informações e serviço

Este capítulo contém informações sobre como entrar em contato conosco.

consulte o Capítulo Endereço de contato

consulte o Capítulo Suporte técnico

consulte o Capítulo Arquivos suspeitos

consulte o Capítulo Registrar falsos-positivos

consulte o Capítulo Seus comentários para mais segurança

### 12.1 Endereço de contato

Se você tiver alguma dúvida ou desejar fazer alguma solicitação relacionada ao produto AntiVir, teremos prazer em ajudar. Para obter nossos endereços de contato, consulte o Centro de controle em Ajuda :: Sobre o Avira Premium Security Suite.

### 12.2 Suporte técnico

O Avira fornece assistência confiável para esclarecer suas dúvidas ou solucionar um problema técnico.

Todas as informações necessárias sobre nosso abrangente serviço de suporte podem ser obtidas em nosso site:

<http://www.avira.pt/premium-suite-support>

Para que possamos fornecer ajuda rápida e confiável, tenha as seguintes informações em mãos:

- **Informações da licença.** É possível encontrar a interface do programa no item de menu Ajuda :: Sobre o Avira Premium Security Suite :: Informações da licença
- **Informações da versão.** É possível encontrar a interface do programa no item de menu Ajuda :: Sobre o Avira Premium Security Suite:: Informações da versão.
- **Versão do sistema operacional** e os Service Packs instalados.
- **Pacotes de software instalados**, por exemplo, software antivírus de outros fornecedores.
- **Mensagens exatas** do programa ou do arquivo de relatório.

### 12.3 Arquivo suspeito

Os vírus que ainda não podem ser detectados ou removidos por nossos produtos ou os arquivos suspeitos podem ser enviados para nós. Você tem várias maneiras de fazer isso.

- Identifique o arquivo no Gerenciador de quarentena do Centro de controle, e selecione o item Enviar arquivo por meio do menu de contexto ou do botão correspondente.
- Envie o arquivo desejado compactado (WinZIP, PKZip, Arj etc.) como um anexo de e-mail para o seguinte endereço:  
SYMLINKDB  
Como alguns gateways de e-mail funcionam com software antivírus, você também deve fornecer o arquivo com uma senha (informe a senha para nós).

Você também pode enviar o arquivo suspeito através de nosso site: [http://www.avira.pt/sample\\_upload](http://www.avira.pt/sample_upload)

## 12.4 Registrando falso-positivos

Se você achar que o programa AntiVir registrou uma detecção em um arquivo que provavelmente está "limpo", envie o arquivo relevante compactado (WinZIP, PKZip, Arj etc.) como um anexo de e-mail para o seguinte endereço:

- SYMLINKDB

Como alguns gateways de e-mail funcionam com software antivírus, você também deve fornecer o arquivo com uma senha (informe a senha para nós).

## 12.5 Seus comentários para mais segurança

Na Avira, a segurança de nossos clientes é a nossa principal prioridade. Devido a isso, temos apenas uma equipe de especialistas interna que testa a qualidade e a segurança de todas as soluções da Avira GmbH antes do lançamento do produto. Além disso, damos grande importância às indicações feitas sobre lacunas de segurança significativas que podem se desenvolver de forma crítica.

Se você achar que detectou uma lacuna de segurança em um de nossos produtos, envie um e-mail para o seguinte endereço:

SYMLINKDB

## 13 Referência: opções de configuração

A referência de configuração documenta todas as opções de configuração disponíveis.

### 13.1 Scanner

A seção Scanner da Configuração é responsável pela configuração da verificação sob demanda.

#### 13.1.1 Fazer verificação

Aqui é possível definir o comportamento básico da rotina de uma verificação sob demanda. Se você selecionar alguns diretórios a serem verificados sob demanda, dependendo da configuração, o Scanner verificará:

- com uma determinada ordem de verificação (prioridade),
- também os setores de inicialização e a memória principal,
- alguns ou todos os setores de inicialização e a memória principal,
- alguns ou todos os arquivos do diretório.

##### **Arquivos**

O Scanner pode usar um filtro para verificar somente os arquivos com uma determinada extensão (tipo).

##### **Todos os arquivos**

Se essa opção for ativada, todos os arquivos serão verificados em busca de vírus ou programas indesejados, independentemente do conteúdo e da extensão do arquivo. O filtro não é usado.

##### **Nota**

Se Todos os arquivos for ativado, o botão **Extensões de arquivo** não poderá ser selecionado.

##### **Extensões inteligentes**

Se essa opção for ativada, a seleção dos arquivos verificados em busca de vírus ou programas indesejados será escolhida automaticamente pelo programa. Desse modo, o programa AntiVir decidirá se os arquivos devem ou não ser verificados com base em seu conteúdo. Esse procedimento é um pouco mais lento do que Usar lista de extensões de arquivo, porém é mais seguro visto que não é apenas a extensão do arquivo que é verificada. Essa opção é ativada como configuração padrão e é recomendada.

##### **Nota**

Se Extensões inteligentes for ativado, o botão **Extensões de arquivo** não poderá ser selecionado.

##### **Usar lista de extensões de arquivo**



Se essa opção for ativada, somente os arquivos com a extensão especificada serão verificados. Todos os tipos de arquivo que podem conter vírus e programas indesejados são predefinidos. A lista pode ser editada manualmente através do botão "**Extensão do arquivo**".

### **Nota**

Se essa opção for ativada e todas as entradas tiverem sido excluídas da lista com as extensões de arquivo, aparecerá a mensagem "Sem extensões de arquivo" no botão **Extensões de arquivo**.

### **Extensões de arquivo**

Quando esse botão é pressionado, uma caixa de diálogo é aberta na qual são exibidas todas as extensões de arquivo que são verificadas no modo "**Usar lista de extensões de arquivo**". As entradas padrão são definidas para as extensões, mas as entradas podem ser adicionadas ou excluídas.

### **Nota**

A lista padrão pode variar de acordo com a versão.

## **Configurações adicionais**

### **Fazer a varredura de setores de inicialização das unidades selecionadas**

Se essa opção for ativada, o Scanner verificará os setores de inicialização das unidades selecionadas para a verificação sob demanda. Essa opção é ativada como configuração padrão.

### **Fazer a varredura de setores de inicialização principais**

Se essa opção for ativada, o Scanner verificará os setores de inicialização principais dos discos rígidos usados no sistema.

### **Ignorar arquivos off-line**

Se essa opção for ativada, a verificação direta ignorará os arquivos off-line por completo durante uma verificação. Isso significa que esses arquivos não são verificados em busca de vírus e programas indesejados. Os arquivos off-line são arquivos que foram movidos fisicamente pelo chamado HSMS (Hierarchical Storage Management System, Sistema de gerenciamento de armazenamento hierárquico), por exemplo, do disco rígido para uma fita. Essa opção é ativada como configuração padrão.

### **Verificação da integridade dos arquivos de sistema**

Quando essa opção está ativada, os arquivos mais importantes do sistema Windows são submetidos a uma verificação particularmente segura das alterações realizadas por malwares durante cada verificação sob demanda. Se um arquivo corrigido for detectado, será registrado como suspeito. Essa função consome muita memória do computador. É por esse motivo que a opção é desativada como configuração padrão.

### **Importante**

Essa opção está disponível somente no Windows Vista e superior.

### **Observação**

Essa opção não deverá ser usada se você estiver usando ferramentas de terceiros que modificam arquivos do sistema e adaptam a tela de inicialização aos seus próprios requisitos. O Skinpacks, o TuneUp Utilities e o Vista Customization são exemplos dessas ferramentas.

### **Varredura otimizada**

Quando essa opção está ativada, a capacidade do processador é utilizada de modo ideal durante uma verificação do Scanner. Por razões de desempenho, a verificação utilizada é realizada somente no nível padrão.

### **Observação**

Essa opção está disponível somente em sistemas com vários processadores. Se

### **Seguir links simbólicos**

Se essa opção for ativada, o Scanner realizará uma verificação que segue todos os links simbólicos no perfil de verificação ou diretório selecionado e verifica os arquivos vinculados em busca de vírus e malwares. Essa opção não tem suporte no Windows 2000 e foi desativada.

### **Importante**

A opção não inclui nenhum atalho, mas faz referência exclusivamente a links simbólicos (gerados por mklink.exe) ou pontos de junção (gerados por junction.exe) que são transparentes no sistema de arquivos.

### **Pesquisar rootkits antes da varredura**

Se essa opção for ativado e uma verificação for iniciada, o Scanner verificará o diretório do sistema Windows em busca de rootkits ativos em um atalho conhecido. Esse processo não verifica seu computador em busca de rootkits ativos de modo tão abrangente quanto o perfil de verificação "**Verificar rootkits**", mas sua execução é significativamente mais rápida.

### **Importante**

A verificação de rootkit não está disponível para o Windows XP de 64 bits .

### **Fazer a varredura do registro**

Se essa opção for ativada, o registro será verificado quanto a referências de malware.

## **Processo da verificação**

### **Permitir interromper o Scanner**

Se essa opção for ativada, a verificação em busca de vírus ou programas indesejados poderá ser encerrada a qualquer momento com o botão "**Parar**" na janela "Luke Filewalker". Se essa configuração for desativada, o botão "**Parar**" na janela "Luke Filewalker" terá um fundo cinza. Desse modo, o encerramento prematuro de um processo de verificação não é permitido. Essa opção é ativada como configuração padrão.

### **Prioridade do mecanismo de varredura**

Com a verificação sob demanda, o Scanner diferencia os níveis de prioridade. Isso será útil somente se vários processos estiverem em execução simultaneamente na estação de trabalho. A seleção afeta a velocidade da verificação.

#### **Baixo**

O Scanner terá apenas o tempo de processador alocado pelo sistema operacional se nenhum outro processo exigir o tempo de computação, isto é, contanto que apenas o Scanner esteja em execução, a velocidade será máxima. Em tudo por tudo, o trabalho com outros programas é ideal: o computador responderá mais rapidamente se outros programas exigirem o tempo de computação enquanto o Scanner continua em execução em segundo plano. Essa opção é ativada como configuração padrão e é recomendada.

#### **Médio**

O Scanner é executado com prioridade normal. O sistema operacional aloca a mesma quantidade de tempo de processador para todos os processos. Em algumas circunstâncias, o trabalho com outros aplicativos pode ser afetado.

#### **Alto**

O Scanner tem a prioridade mais alta. O trabalho simultâneo com outros aplicativos é quase impossível. No entanto, o Scanner conclui sua verificação em velocidade máxima.

### 13.1.1.1. Ação para detecção

#### **Ação para detecção**

Você pode definir as ações a serem executadas pelo Scanner quando um vírus ou programa indesejado for detectado.

#### **Interativo**

Se essa opção for ativada, os resultados da verificação do Scanner serão exibidos em uma caixa de diálogo. Ao realizar uma verificação com o Scanner, um alerta será emitido com uma lista dos arquivos afetados no final da verificação. Você pode usar o menu sensível ao contexto para selecionar uma ação a ser executada para os diversos arquivos afetados. Você pode executar as ações padrão para todos os arquivos afetados ou cancelar o Scanner.

#### **Nota**

A ação Mover para quarentena é pré-selecionada por padrão na notificação do Scanner. Outras ações podem ser selecionadas em um menu de contexto.

Clique aqui para obter mais informações.

#### **Automático**

Se essa opção for ativada, nenhuma caixa de diálogo com uma detecção de vírus será exibida. O Scanner reage de acordo com as configurações predefinidas nesta seção como ação primária ou secundária.

#### **Mover backup para quarentena**

Se essa opção for ativada, o Scanner criará uma cópia de backup antes de realizar a ação primária ou secundária solicitada. A cópia de backup é salva na Quarentena, onde o arquivo poderá ser restaurado se tiver valor informativo. Você também pode enviar a cópia de backup para o Centro de pesquisa de malware da Avira para novas investigações.

#### **Ação primária**

Ação primária é a ação executada quando o Scanner encontra um vírus ou programa indesejado. Se a opção "**reparar**" for selecionada, mas não for possível reparar o arquivo afetado, a ação selecionada em "**Ação secundária**" será executada.

#### **Nota**

A opção **Ação secundária** só poderá ser selecionada se a configuração **reparar** tiver sido selecionada em **Ação primária**.

#### **Reparar**

Se essa opção for ativada, o Scanner reparará os arquivos afetados automaticamente. Se o Scanner não conseguir reparar um arquivo afetado, realizará a ação selecionada em Ação secundária.

#### **Nota**

Um reparo automático é recomendado, mas o Scanner modificará os arquivos na estação de trabalho.

#### **excluir**

Se essa opção for ativada, o arquivo será excluído. Esse processo é muito mais rápido do que "substituir e excluir".

#### **substituir e excluir**

Se essa opção for ativada, o Scanner substituirá o arquivo por um padrão e irá excluí-lo. Não é possível restaurá-lo.

#### **renomear**

Se essa opção for ativada, o Scanner renomeará o arquivo. Portanto, o acesso direto a esses arquivos (por exemplo, com clique duplo) não é mais possível. Os arquivos podem ser reparados posteriormente e voltar a ter seus nomes originais.

**Ignorar**

Se essa opção for ativada, o acesso ao arquivo será permitido e o arquivo não será alterado.

**Aviso**

O arquivo afetado permanece ativo em sua estação de trabalho. Isso pode causar danos graves à estação de trabalho.

**Quarentena**

Se essa opção for ativada, o Scanner moverá o arquivo para a quarentena. Esses arquivos podem ser reparados posteriormente ou, se necessário, enviados para o Centro de pesquisa de malware da Avira.

**Ação secundária**

A opção "**Ação secundária**" só poderá ser selecionada se a configuração **reparar** tiver sido selecionada em "**Ação primária**". Com essa opção, agora é possível decidir o que deve ser feito com o arquivo afetado caso não seja possível repará-lo.

**excluir**

Se essa opção for ativada, o arquivo será excluído. Esse processo é muito mais rápido do que "substituir e excluir".

**substituir e excluir**

Se essa opção for ativada, o Scanner substituirá o arquivo por um padrão e irá excluí-lo (apagá-lo). Não é possível restaurá-lo.

**renomear**

Se essa opção for ativada, o Scanner renomeará o arquivo. Portanto, o acesso direto a esses arquivos (por exemplo, com clique duplo) não é mais possível. Os arquivos podem ser reparados posteriormente e voltar a ter seus nomes originais.

**Ignorar**

Se essa opção for ativada, o acesso ao arquivo será permitido e o arquivo não será alterado.

**Aviso**

O arquivo afetado permanece ativo em sua estação de trabalho. Isso pode causar danos graves à estação de trabalho.

**Quarentena**

Se essa opção for ativada, o Scanner moverá o arquivo para a Quarentena. Esses arquivos podem ser reparados posteriormente ou, se necessário, enviados para o Centro de pesquisa de malware da Avira.

**Nota**

Se tiver selecionado **Excluir** ou **Substituir e excluir** como ação primária ou secundária, leve em consideração o seguinte: no caso de acessos heurísticos, os arquivos afetados não são excluídos, mas movidos para a quarentena.

Ao verificar arquivos compactados, o Scanner usa uma verificação recursiva: os arquivos do arquivamento também são descompactados e verificados quanto à presença de vírus e programas indesejados. Os arquivos são verificados, descompactados e verificados novamente.

**Fazer a varredura dos arquivamentos**

Se essa opção for ativada, os arquivamentos selecionados na lista serão verificados. Essa opção é ativada como configuração padrão.

### **Todos os tipos de arquivo**

Se essa opção for ativada, todos os tipos de arquivo da lista de arquivamentos serão selecionados e verificados.

### **Extensões inteligentes**

Se essa opção for ativada, o Scanner detectará se um arquivo está em um formato compactado (arquivo compactado), mesmo que a extensão seja diferente das extensões normais, e fará a verificação do arquivo compactado. No entanto, para isso, é necessário abrir cada arquivo, o que diminui a velocidade da verificação. Exemplo: Se um arquivo \*.zip tiver a extensão \*.xyz, o Scanner também descompactará e verificará esse arquivo. Essa opção é ativada como configuração padrão.

### **Nota**

Somente os tipos de arquivo marcados na lista são suportados.

### **Profundidade de recursão**

A descompactação e a verificação de arquivamentos recursivos podem consumir muito tempo e muitos recursos do computador. Se essa opção for ativada, a profundidade da verificação de arquivos com vários níveis de compactação será limitada a um determinado número de níveis de compactação (profundidade máxima de recursão). Isso economiza tempo e recursos do computador.

### **Nota**

Para encontrar um vírus ou programa indesejado em um arquivo, o Scanner deve fazer a verificação até o nível de recursão em que o vírus ou programa indesejado está localizado.

### **Profundidade máxima da recursão**

Para inserir a recursividade máxima, a opção Recursividade máxima deve ser ativada. Você pode inserir a profundidade de recursão solicitada diretamente ou usando a tecla de seta para a direita no campo de entrada. Os valores permitidos estão entre 1 e 99. O valor padrão (e recomendado) é 20.

### **Valores padrão**

O botão restaura os valores predefinidos para verificar os arquivamentos.

## **Arquivos**

Nessa área de exibição, é possível definir os arquivos compactados que devem ser verificados pelo Scanner. Para isso, você deve selecionar as entradas relevantes.

### 13.1.1.2. Exceções

#### **Objetos do arquivo a serem omitidos do Scanner**

A lista dessa janela contém arquivos e caminhos que não devem ser incluídos pelo Scanner na verificação em busca de vírus ou programas indesejados.

Insira o mínimo de exceções possível aqui e somente os arquivos que, por algum motivo, não devem ser incluídos em uma verificação normal. Recomendamos que você sempre verifique esses arquivos quanto à presença de vírus ou programas indesejados antes que eles sejam incluídos nessa lista.

### **Nota**

As entradas da lista devem ter no máximo 6000 caracteres no total.

**Aviso**

Esses arquivos não são incluídos em uma verificação.

**Nota**

Os arquivos incluídos nessa lista são registrados no arquivo de relatório. Verifique o arquivo de relatório periodicamente para observar se há algum arquivo não verificado, pois a causa que fez você excluir um arquivo aqui talvez não exista mais. Nesse caso, remova o nome desse arquivo dessa lista novamente.

**Caixa de entrada**

Nessa caixa de entrada, é possível inserir o nome do objeto de arquivo que não é incluído na verificação sob demanda. Nenhum objeto de arquivo é inserido como configuração padrão.



O botão abre uma janela na qual é possível selecionar o arquivo ou caminho desejado. Quando um nome de arquivo com seu caminho completo é inserido, somente o arquivo em questão não é verificado quanto à presença de infecção. Caso tenha inserido um nome de arquivo sem um caminho, todos os arquivos com esse nome (independentemente do caminho ou da unidade) não serão verificados.

**Adicionar**

Com esse botão, você pode adicionar o objeto de arquivo inserido na caixa de entrada à janela de exibição.

**Excluir**

O botão exclui uma entrada selecionada da lista. Esse botão estará desativado se nenhuma entrada for selecionada.

**Nota**

Se você adicionar uma partição completa à lista de objetos de arquivo, somente os arquivos salvos diretamente na partição serão excluídos da verificação; isso não se aplica aos arquivos nos subdiretórios da partição correspondente:

Exemplo: Objeto de arquivo a ser ignorado: D:\ = D:\file.txt será excluído da verificação do Scanner; D:\folder\file.txt não será excluído da verificação.

### 13.1.1.3. Heurística

Essa seção de configuração contém as configurações de heurística do mecanismo de verificação.

Os produtos AntiVir contêm uma heurística muito poderosa que pode detectar malwares desconhecidos de modo proativo, isto é, antes que uma assinatura de vírus especial para combater o elemento nocivo seja criada e antes que uma atualização de proteção contra vírus seja enviada. A detecção de vírus envolve uma análise abrangente e a investigação dos códigos afetados em busca de funções típicas de malware. Se o código que está sendo verificado apresentar esses recursos característicos, será considerado suspeito. Isso não significa necessariamente que o código é um malware genuíno. Falso-positivos também ocorrem às vezes. A decisão de como tratar o código afetado deve ser tomada pelo usuário, por exemplo, com base em seu conhecimento sobre a confiabilidade da origem do código.

**Heurística para vírus de macro**

**Heurística para vírus de macro**

O produto AntiVir contém uma heurística para vírus de macro muito poderosa. Se essa opção for ativada, todas as macros no documento em questão serão excluídas em caso de reparo. Por outro lado, os arquivos suspeitos são apenas relatados (por exemplo, você recebe um alerta). Essa opção é ativada como configuração padrão e é recomendada.

### **Detecção e análise heurística avançada (AHeAD)**

#### **ativar AHeAD**

O programa AntiVir contém uma heurística muito poderosa na forma da tecnologia AntiVir AHeAD, que também pode detectar malwares desconhecidos (novos). Se essa opção for ativada, você poderá definir até que ponto essa heurística deve ser "agressiva". Essa opção é ativada como configuração padrão.

#### **Nível de detecção baixo**

Se essa opção for ativada, malwares conhecidos serão detectados menos ligeiramente e o risco de alertas falsos é baixo nesse caso.

#### **Nível de detecção médio**

Essa opção será ativada como configuração padrão se você tiver selecionado o uso dessa heurística.

#### **Nível de detecção alto**

Se essa opção for ativada, uma quantidade consideravelmente maior de malwares desconhecidos será detectada, mas existe a possibilidade de aparecerem falso-positivos.

## 13.1.2 Relatório

O Scanner tem uma função de relatório abrangente. Com ela, você obtém informações precisas sobre os resultados de uma verificação sob demanda. O arquivo de relatório contém todas as entradas do sistema, bem como alertas e mensagens da verificação sob demanda.

### **Nota**

Para que você possa definir as ações que o Scanner executou quando vírus ou programas indesejados foram detectados, um arquivo de relatório sempre deve ser criado.

### **Relatório**

#### **Desligar**

Se essa opção for ativada, o Scanner não registrará as ações e os resultados da verificação sob demanda.

#### **Padrão**

Quando essa opção está ativada, o Scanner registra os nomes dos arquivos suspeitos e os caminhos correspondentes. Além disso, a configuração da verificação atual, as informações de versão e as informações sobre o usuário licenciado são gravadas no arquivo de relatório.

#### **Avançado**

Quando essa opção é ativada, o Scanner registra alertas e dicas além das informações padrão.

#### **Concluído**

Quando essa opção está ativada, o Scanner também registra todos os arquivos verificados. Além disso, todos os arquivos envolvidos, bem como os alertas e as dicas, são incluídos no arquivo de relatório.

**Nota**

Se precisar enviar um arquivo de relatório a qualquer momento (para solucionar problemas), crie esse arquivo nesse modo.

## 13.2 Guard

A seção Guard da configuração é responsável pela configuração da verificação durante o acesso.

### 13.2.1 Fazer verificação

Em geral, você quer monitorar seu sistema constantemente. Para fazer isso, use o Guard (= Scanner de acesso). Com ele, você pode verificar todos os arquivos que são copiados ou abertos no computador "imediatamente" em busca de vírus e programas indesejados.

**Modo de verificação**

Aqui é definida a hora em que será feita a verificação de um arquivo.

**Fazer varredura ao ler**

Se essa opção for ativada, o Guard verificará os arquivos antes que eles sejam lidos ou executados pelo aplicativo ou sistema operacional.

**Fazer varredura ao gravar**

Se essa opção for ativada, o Guard verificará o arquivo durante a gravação. Você só poderá acessar o arquivo novamente após a conclusão desse processo.

**Fazer varredura ao ler e gravar**

Se essa opção for ativada, o Guard verificará os arquivos quando forem abertos, lidos e executados e depois de serem gravados. Essa opção é ativada como configuração padrão e é recomendada.

**Arquivos**

O Guard pode usar um filtro para verificar somente os arquivos com uma determinada extensão (tipo).

**Todos os arquivos**

Se essa opção for ativada, todos os arquivos serão verificados em busca de vírus ou programas indesejados, independentemente do conteúdo e da extensão do arquivo.

**Nota**

Se Todos os arquivos for ativado, o botão **Extensões de arquivo** não poderá ser selecionado.

**Extensões inteligentes**



Se essa opção for ativada, a seleção dos arquivos verificados em busca de vírus ou programas indesejados será escolhida automaticamente pelo programa. Desse modo, o programa decidirá se os arquivos devem ou não ser verificados com base em seu conteúdo. Esse procedimento é um pouco mais lento do que Usar lista de extensões, porém é mais seguro visto que não é apenas a extensão que é verificada.

### **Nota**

Se Extensões inteligentes for ativado, o botão **Extensões de arquivo** não poderá ser selecionado.

### **Usar lista de extensões de arquivo**

Se essa opção for ativada, somente os arquivos com a extensão especificada serão verificados. Todos os tipos de arquivo que podem conter vírus e programas indesejados são predefinidos. A lista pode ser editada manualmente através do botão "**Extensões do arquivo**". Essa opção é ativada como configuração padrão e é recomendada.

### **Nota**

Se essa opção for ativada e todas as entradas tiverem sido excluídas da lista com as extensões de arquivo, aparecerá a mensagem "Sem extensões de arquivo" no botão **Extensões de arquivo**.

### **Extensões de arquivo**

Quando esse botão é pressionado, uma caixa de diálogo é aberta na qual são exibidas todas as extensões de arquivo que são verificadas no modo "**Usar lista de extensões de arquivo**". As entradas padrão são definidas para as extensões, mas as entradas podem ser adicionadas ou excluídas.

### **Nota**

A lista de extensões de arquivo pode variar de acordo com a versão.

## **Arquivos**

### **Fazer a varredura dos arquivamentos**

Se essa opção for ativada, os arquivamentos serão verificados. Os arquivos compactados são verificados, descompactados e verificados novamente. Essa opção é desativada por padrão. A verificação do arquivamento é restrita pela profundidade de recursão, pelo número de arquivos a serem verificados e pelo tamanho do arquivamento. É possível definir a profundidade de recursão máxima, o número de arquivos a serem verificados e o tamanho máximo do arquivo compactado.

### **Nota**

Essa opção é desativada por padrão, pois o processo consome muita memória do computador. Geralmente, é recomendado fazer a varredura dos arquivamentos com uma verificação sob demanda.

### **Profundidade máxima da recursão**

Ao verificar arquivos compactados, o Guard usa uma verificação recursiva: os arquivos do arquivamento também são descompactados e verificados quanto à presença de vírus e programas indesejados. É possível definir a profundidade de recursão. O valor padrão (e recomendado) para a profundidade de recursão é 1: todos os arquivos que estão localizados diretamente no arquivamento principal são verificados.

### **Número máximo de arquivos**

Ao verificar os arquivamentos, é possível limitar a verificação a um número máximo de arquivo. O valor padrão e recomendado para o número máximo de arquivos a serem verificados é 10.

### **Tamanho máximo (KB)**

Ao verificar os arquivamentos, é possível limitar a verificação a um tamanho máximo de arquivo a ser descompactado. O valor padrão de 1000 KB é recomendado.

### 13.2.1.1. Ação para detecção

#### **Ação para detecção**

Você pode definir as ações a serem executadas pelo Guard quando um vírus ou programa indesejado for detectado.

#### **Interativo**

Se essa opção for ativada, uma notificação de área de trabalho aparecerá quando o Guard detectar um vírus ou programa indesejado. Você pode remover o malware detectado ou acessar outras ações possíveis de tratamento de vírus através do botão "Detalhes". As ações são exibidas em uma caixa de diálogo. As ações serão exibidas em uma caixa de diálogo. Essa opção é ativada como configuração padrão.

Clique aqui para obter mais informações.

#### **Automático**

Se essa opção for ativada, nenhuma caixa de diálogo com uma detecção de vírus será exibida. O Guard reage de acordo com as configurações predefinidas nesta seção como ação primária ou secundária.

#### **Mover backup para quarentena**

Se essa opção for ativada, o Guard criará uma cópia de backup antes de realizar a ação primária ou secundária solicitada. A cópia de backup é salva na quarentena. Ela poderá ser restaurada através do Gerenciador de quarentena se tiver valor informativo. Você também pode enviar a cópia de backup para o Centro de pesquisa de malware da Avira. Dependendo do objeto, outras opções de seleção estarão disponíveis no Gerenciador de quarentena.

#### **Ação primária**

Ação primária é a ação executada quando o Guard encontra um vírus ou programa indesejado. Se a opção "**reparar**" for selecionada, mas não for possível reparar o arquivo afetado, a ação selecionada em "**Ação secundária**" será executada.

#### **Observação**

A opção Ação secundária só poderá ser selecionada se a configuração reparar tiver sido selecionada em Ação primária.

#### **reparar**

Se essa opção for ativada, o Guard reparará os arquivos afetados automaticamente. Se o Guard não conseguir reparar um arquivo afetado, realizará a ação selecionada em Ação secundária.

#### **Observação**

Um reparo automático é recomendado, mas o Guard modificará os arquivos na estação de trabalho.

#### **excluir**

Se essa opção for ativada, o arquivo será excluído. Esse processo é muito mais rápido do que "substituir e excluir".

#### **substituir e excluir**

Se essa opção for ativada, o Guard substituirá o arquivo por um padrão e irá excluí-lo. Não é possível restaurá-lo.

#### **renomear**

Se essa opção for ativada, o Guard renomeará o arquivo. Portanto, o acesso direto a esses arquivos (por exemplo, com clique duplo) não é mais possível. Os arquivos podem ser reparados posteriormente e voltar a ter seus nomes originais.

### **Ignorar**

Se essa opção for ativada, o acesso ao arquivo será permitido e o arquivo não será alterado.

### **Aviso**

O arquivo afetado permanece ativo em sua estação de trabalho. Isso pode causar danos graves à estação de trabalho.

### **Negar acesso**

Se essa opção for ativada, o Guard irá inserir a detecção no arquivo de relatório, se a função de registro estiver ativada. Além disso, o Guard grava uma entrada no Registro de eventos, se essa opção for ativada.

### **Quarentena**

Se essa opção for ativada, o Guard moverá o arquivo para a Quarentena. Os arquivos desse diretório podem ser reparados posteriormente ou, se necessário, enviados para o Centro de pesquisa de malware da Avira.

### **Ação secundária**

A opção "**Ação secundária**" só poderá ser selecionada se a opção "**Reparar**" tiver sido selecionada em "**Ação primária**". Com essa opção, agora é possível decidir o que deve ser feito com o arquivo afetado caso não seja possível repará-lo.

### **excluir**

Se essa opção for ativada, o arquivo será excluído. Esse processo é muito mais rápido do que "substituir e excluir".

### **substituir e excluir**

Se essa opção for ativada, o Guard substituirá o arquivo por um padrão e irá excluí-lo. Não é possível restaurá-lo.

### **renomear**

Se essa opção for ativada, o Guard renomeará o arquivo. Portanto, o acesso direto a esses arquivos (por exemplo, com clique duplo) não é mais possível. Os arquivos podem ser reparados posteriormente e voltar a ter seus nomes originais.

### **Ignorar**

Se essa opção for ativada, o acesso ao arquivo será permitido e o arquivo não será alterado.

### **Aviso**

O arquivo afetado permanece ativo em sua estação de trabalho. Isso pode causar danos graves à estação de trabalho.

### **Negar acesso**

Se essa opção for ativada, o Guard irá inserir a detecção no arquivo de relatório, se a função de registro estiver ativada. Além disso, o Guard grava uma entrada no Registro de eventos, se essa opção for ativada.

### **Quarentena**

Se essa opção for ativada, o Guard moverá o arquivo para a Quarentena. Os arquivos podem ser reparados posteriormente ou, se necessário, enviados para o Centro de pesquisa de malware da Avira.

**Observação**

Se tiver selecionado **Excluir** ou **Substituir e excluir** como ação primária ou secundária, leve em consideração o seguinte: no caso de acessos heurísticos, os arquivos afetados não são excluídos, mas movidos para a quarentena.

## 13.2.1.2. Mais ações

### Notificações

#### Registro de eventos

##### Usar registro de eventos

Se essa opção for ativada, uma entrada é adicionada ao registro de eventos do Windows para cada detecção. Os eventos podem ser chamados no visualizador de eventos do Windows. Essa opção é ativada como configuração padrão.

#### Início automático

##### Bloquear função de início automático

Quando essa opção está ativada, a execução da função Início automático do Windows é bloqueada em todas as unidades conectadas, incluindo pendrives, unidades de CD e DVD e unidades de rede. Com a função Início automático do Windows, os arquivos em mídias de dados ou unidades de rede são lidos imediatamente durante o carregamento ou a conexão e, assim, podem ser iniciados e copiados automaticamente. No entanto, essa funcionalidade tem um alto risco de segurança, pois malwares e programas indesejados podem ser instalados durante o início automático. A função Início automático é crítica especialmente para pendrives, pois os dados de um pendrive podem ser alterados a qualquer momento.

##### Excluir CDs e DVDs

Quando esta opção está ativada, a função Início automático é permitida em unidades de CD e DVD.

##### **Aviso**

Desative a função Início automático para unidades de CD e DVD somente se tiver certeza de que está usando mídias de dados confiáveis.

## 13.2.1.3. Exceções

Com essas opções, é possível configurar objetos de exceção para o Guard (verificação durante o acesso). Os objetos relevantes não são incluídos na verificação durante o acesso. O Guard pode ignorar os acessos do arquivo a esses objetos durante a verificação de acesso através da lista de processos a serem omitidos. Isso é útil, por exemplo, com soluções de backup ou bancos de dados.

Observe as informações a seguir ao especificar processos e objetos de arquivo a serem omitidos: A lista é processada de cima para baixo. Quanto maior a lista, mais tempo será necessário para processar a lista para cada acesso. Desse modo, mantenha a lista o menor possível.

### Processos a serem omitidos pelo Guard

Todos os acessos de arquivo dos processos dessa lista são excluídos do monitoramento do Guard.

#### **Caixa de entrada**

Neste campo, insira o nome do processo que deve ser ignorado pela varredura em tempo real. Nenhum processo é inserido como configuração padrão.

#### **Nota**

Você pode inserir até 128 processos.

#### **Nota**

Ao inserir o processo, os símbolos Unicode são aceitos. Você pode inserir processos ou nomes de diretório contendo símbolos especiais.

#### **Observação**

É possível excluir processos do monitoramento do Guard sem detalhes de caminho completos.

application.exe

No entanto, isso se aplica somente a processos em que os arquivos executáveis estão localizados nas unidades do disco rígido.

Não especifique todos as exceções dos processos em que os arquivos executáveis estão localizados nas unidades dinâmicas. Unidades dinâmicas são usadas para discos removíveis, como CDs, DVDs e memórias flash USB.

#### **Observação**

As informações da unidade devem ser inseridas da seguinte forma: [Letra da unidade]:\ O símbolo de dois-pontos (:) é somente usado para especificar unidades.

#### **Observação**

Ao especificar o processo, você poderá usar os caracteres curinga\* (qualquer número de caracteres) e ?? (um único caractere).

C:\Arquivos de programas\Application\application.exe

C:\Arquivos de programas\Aplicativos\applicationio?.exe

C:\Arquivos de programas\Application\applic\*.exe

C:\Arquivos de programas\Aplicativos\\*.exe

Para evitar que o processo seja excluído globalmente do monitoramento do Guard, as especificações que compreendem exclusivamente os seguintes caracteres são inválidas: \* (asterisco), ? (ponto de interrogação), / (barra), \ (barra invertida), . (ponto), : (dois-pontos).

#### **Nota**

O caminho e o nome de arquivo especificados do processo devem ter no máximo 255 caracteres. As entradas da lista devem ter no máximo 6000 caracteres no total.

#### **Aviso**

Todos os acessos de arquivo pelos processos registrados na lista são excluídos da verificação quanto a vírus e programas indesejados. O Windows Explorer e o sistema operacional propriamente dito não podem ser excluídos. Uma entrada correspondente na lista será ignorada.



O botão abre uma janela na qual é possível selecionar um arquivo executável.

#### **Processos**

O botão "**Processos**" abre a janela "*Seleção de processos*" na qual são exibidos os processos em execução.

#### **Adicionar**

Com esse botão, você pode adicionar o processo inserido na caixa de entrada à janela de exibição.

### **Excluir**

Com esse botão, é possível excluir um processo selecionado na janela de exibição.

## **Objetos a serem omitidos pelo Guard**

Todos os acessos de arquivo aos objetos dessa lista são excluídos do monitoramento do Guard.

### **Caixa de entrada**

Nessa caixa, é possível inserir o nome do objeto de arquivo que não é incluído na verificação durante o acesso. Nenhum objeto de arquivo é inserido como configuração padrão.

### **Observação**

Ao especificar os objetos de arquivo a serem omitidos, você poderá usar os caracteres curinga\* (qualquer número de caracteres) e ?? (um único caractere): Extensões de arquivo individuais também podem ser excluídas (inclusive curingas):

C:\Diretório\\*.mdb

\*.mdb

\*.md?

\*.xls\*

C:\Diretório\\*.log

### **Observação**

Os nomes de diretório devem terminar com uma barra invertida (\); caso contrário, será considerado um nome de arquivo.

### **Nota**

As entradas da lista devem ter no máximo 6000 caracteres no total.

### **Observação**

Se um diretório for excluído, todos os subdiretórios também serão excluídos automaticamente.

### **Nota**

Para cada unidade, é possível especificar no máximo 20 exceções inserindo o caminho completo (começando com a letra da unidade).

Por exemplo: C:\Arquivos de programas\Aplicativos\Nome.log

Podem existir no máximo 64 exceções sem um caminho completo.

Por exemplo: \*.log

### **Nota**

No caso das unidades dinâmicas que são montadas como um diretório em outra unidade, o alias do sistema operacional da unidade integrada na lista de exceções deve ser usado:

por exemplo, \Device\HarddiskDmVolumes\PhysicalDmVolumes\BlockVolume1\

No entanto, se você usar o ponto de montagem propriamente dito (por exemplo, C:\DynDrive), a unidade dinâmica será verificada. Você pode determinar o alias do sistema operacional a ser usado no arquivo de relatório do Guard.



O botão abre uma janela na qual é possível selecionar o objeto de arquivo a ser excluído.

### **Adicionar**

Com esse botão, você pode adicionar o objeto de arquivo inserido na caixa de entrada à janela de exibição.

### **Excluir**

Com esse botão, é possível excluir um objeto de arquivo selecionado da janela de exibição. Observe as informações adicionais ao especificar exceções:

### **Observação**

Para excluir também os objetos quando forem acessados com nomes curtos de arquivo DOS (convenção de nome DOS 8.3), o nome curto relevante do arquivo deve ser inserido na lista.

### **Nota**

Um nome de arquivo que contém caracteres curinga não pode terminar com uma barra invertida.

Por exemplo:

```
C:\Arquivos de programas\Application\applic*.exe\
```

Essa entrada não é válida e não é tratada como uma exceção.

### **Nota**

Você pode localizar o caminho usado pelo Guard para verificar os arquivos infectados no arquivo de relatório do Guard. Indique exatamente o mesmo caminho na lista de exceções. Proceda do seguinte modo: Defina a função de protocolo do Guard como **Concluído** na configuração em Guard::Relatório. Em seguida, acesse os arquivos, as pastas, as unidades montadas com o Guard ativado. Agora você pode ler o caminho a ser usado no arquivo de relatório do Guard. O arquivo de relatório pode ser acessado no Centro de controle em Proteção local::Guard.

### Exemplos de processos a serem excluídos:

- application.exe

O processo application.exe é excluído da verificação do Guard, independentemente do local em que a unidade do disco rígido está localizada e do diretório.

- C:\Arquivos de programas1\Application.exe

O processo do arquivo application.exe, localizado no caminho C:\Arquivos de programas1, é excluído da verificação do Guard.

- C:\Arquivos de programas1\\*.exe

Todos os processos dos arquivos executáveis localizados no caminho C:\Arquivos de programas1 são excluídos da verificação do Guard.

### Exemplos de arquivos a serem excluídos:

- \*.mdb

Todos os arquivos com a extensão “mdb” são excluídos da verificação do Guard

- \*.xls\*

Todos os arquivos com a extensão “xls” são excluídos da verificação do Guard, por exemplo os arquivos com as extensões .xls e .xlsx.

- C:\Diretório\\*.log

Todos arquivos de registro com a extensão “log”, localizados no caminho C:\Diretório, são excluídos da verificação do Guard.

### 13.2.1.4. Heurística

Essa seção de configuração contém as configurações de heurística do mecanismo de verificação.

Os produtos AntiVir contém uma heurística muito poderosa que pode detectar malwares desconhecidos de modo proativo, isto é, antes que uma assinatura de vírus especial para combater o elemento nocivo seja criada e antes que uma atualização de proteção contra vírus seja enviada. A detecção de vírus envolve uma análise abrangente e a investigação dos códigos afetados em busca de funções típicas de malware. Se o código que está sendo verificado apresentar esses recursos característicos, será considerado suspeito. Isso não significa necessariamente que o código é um malware genuíno. Falso-positivos também ocorrem às vezes. A decisão de como tratar o código afetado deve ser tomada pelo usuário, por exemplo, com base em seu conhecimento sobre a confiabilidade da origem do código.

#### **Heurística para vírus de macro**

##### **Heurística para vírus de macro**

O produto AntiVir contém uma heurística para vírus de macro muito poderosa. Se essa opção for ativada, todas as macros no documento em questão serão excluídas em caso de reparo. Por outro lado, os arquivos suspeitos são apenas relatados (por exemplo, você recebe um alerta). Essa opção é ativada como configuração padrão e é recomendada.

#### **Detecção e análise heurística avançada (AHeAD)**

##### **ativar AHeAD**

O programa AntiVir contém uma heurística muito poderosa na forma da tecnologia AntiVir AHeAD, que também pode detectar malwares desconhecidos (novos). Se essa opção for ativada, você poderá definir até que ponto essa heurística deve ser "agressiva". Essa opção é ativada como configuração padrão.

##### **Nível de detecção baixo**

Se essa opção for ativada, malwares conhecidos serão detectados menos ligeiramente e o risco de alertas falsos é baixo nesse caso.

##### **Nível de detecção médio**

Essa opção será ativada como configuração padrão se você tiver selecionado o uso dessa heurística.

##### **Nível de detecção alto**

Se essa opção for ativada, uma quantidade consideravelmente maior de malwares desconhecidos será detectada, mas existe a possibilidade de aparecerem falso-positivos.



### 13.2.2 ProActiv

O Avira AntiVir ProActiv protege você contra ameaças novas e desconhecidas para as quais não há nenhuma definição de vírus ou heurística disponível. A tecnologia ProActiv está integrada no componente Guard e observa e analisa as ações executadas do programa. O comportamento do programa é verificado com relação a padrões típicos de ação de malware: tipo de ação e sequências de ações. Se algum programa exibir um comportamento típico de malware, será tratado como uma detecção de vírus : você pode bloquear o programa ou ignorar a notificação e continuar usando o programa. É possível classificar o programa como confiável e adicioná-lo ao filtro de aplicativos para programas permitidos. Você também pode adicionar o programa ao filtro de aplicativos para programas bloqueados usando o comando *Sempre bloquear*.

O componente ProActiv usa conjuntos de regras desenvolvidos pelo Centro de pesquisa de malware da Avira para identificar o comportamento suspeito. Os conjuntos de regras são fornecidos pelos bancos de dados da Avira GmbH. O Avira AntiVir ProActiv envia informações sobre os programas suspeitos detectados para os bancos de dados da Avira a fim de que sejam registrados. Você pode desativar a transmissão de dados para os bancos de dados da Avira.

#### **Nota**

A tecnologia ProActiv ainda não está disponível para os sistemas de 64 bits. O Windows 2000 não é compatível com componentes ProActiv.

#### **Geral**

##### **Ativação do Avira AntiVir ProActiv.**

Se essa opção for ativada, os programas serão monitorados no sistema do seu computador e verificados quanto a ações suspeitas. Você receberá uma mensagem se algum comportamento típico de malware for detectado. Você pode bloquear o programa ou selecionar "*Ignorar*" para continuar usando o programa. O processo de monitoramento exclui: Programas classificados como confiáveis, programas confiáveis e assinados incluídos por padrão no filtro de aplicativos permitidos e todos os programas adicionados ao filtro de programas permitidos.

##### **A participação na comunidade do Avira AntiVir ProActiv aumenta a segurança do computador.**

Se essa opção for ativada, o Avira AntiVir ProActiv enviará dados de programas suspeitos e, em alguns casos, arquivos de programas suspeitos (arquivos executáveis) para o Centro de pesquisa de malware da Avira para verificação on-line avançada. Depois de serem avaliados, esses dados são adicionados aos conjuntos de regras de análise comportamental do ProActiv. Desse modo, você passa a fazer parte da comunidade do Avira ProActiv e contribui para o aprimoramento e o refinamento contínuos da tecnologia de segurança ProActiv. Nenhum dado será enviado se essa opção estiver desativada. Isso não afeta a funcionalidade do ProActiv.

##### **Clique aqui para obter mais informações.**

Com esse link, é possível acessar uma página da Web onde você pode obter informações detalhadas sobre a verificação on-line avançada. Todos os dados transmitidos durante uma verificação on-line avançada são incluídos na página da Internet.

### 13.2.2.1. Filtro de aplicativos: Aplicativos a serem bloqueados

Em *Filtro de aplicativos: Aplicativos a serem bloqueados*, é possível inserir os aplicativos classificados como prejudiciais que devem ser bloqueados pelo Avira AntiVir ProActiv por padrão. Os aplicativos adicionados não podem ser executados no sistema do seu computador. Você também pode adicionar programas ao filtro de aplicativos bloqueados através das notificações do Guard sobre programas com comportamento suspeito selecionando a opção *Sempre bloquear este programa*.

#### Aplicativos a serem bloqueados

##### Aplicativos

A lista contém todos os aplicativos classificados como prejudiciais que você inseriu através da configuração ou notificando o componente ProActiv. Os aplicativos da lista são bloqueados pelo Avira AntiVir ProActiv e não podem ser executados no sistema do seu computador. Uma mensagem do sistema operacional é exibida quando um programa bloqueado é iniciado. Os aplicativos a serem bloqueados são identificados pelo Avira AntiVir ProActiv com base no caminho especificado e no nome de arquivo, e são bloqueados independentemente de seu conteúdo.

##### Caixa de entrada

Insira o aplicativo que deseja bloquear nesta caixa. Para identificar o aplicativo, o caminho completo, o nome e a extensão do arquivo devem ser especificados. O caminho deve mostrar a unidade em que o aplicativo está localizado ou começar com uma variável de ambiente.



O botão abre uma janela na qual é possível selecionar o aplicativo a ser bloqueado.

##### Adicionar

Com o botão "**Adicionar**", é possível transferir o aplicativo especificado na caixa de entrada para a lista de aplicativos a serem bloqueados.

##### **Nota**

Não é possível adicionar os aplicativos necessários para a operação adequada do sistema operacional.

##### Excluir

O botão "**Excluir**" permite que você remova um aplicativo realçado da lista de aplicativos a serem bloqueados.

### 13.2.2.2. Filtro de aplicativos: Aplicativos permitidos

A seção *Filtro de aplicativos: Aplicativos permitidos* lista os aplicativos excluídos do monitoramento pelo componente ProActiv: programas assinados classificados como confiáveis e incluídos na lista por padrão, todos os aplicativos classificados como confiáveis e adicionados ao filtro de aplicativos: Você pode adicionar aplicativos permitidos à lista na Configuração. Você também pode adicionar aplicativos ao comportamento suspeito do programa através das notificações do Guard usando a opção **Programa confiável** na notificação do Guard.

### Aplicativos a serem ignorados

#### Aplicativos

A lista contém aplicativos excluídos do monitoramento pelo componente ProActiv. Nas configurações de instalação padrão, a lista contém aplicativos assinados de fornecedores confiáveis. Você pode adicionar os aplicativos que considera confiáveis através da configuração ou das notificações do Guard. O componente ProActiv identifica aplicativos usando o caminho, o nome do arquivo e o conteúdo. Recomendamos verificar o conteúdo, pois códigos de malware podem ser adicionados a um programa através de alterações como atualizações. Você pode determinar se uma verificação de conteúdo deve ser executada a partir do tipo especificado: para o tipo "Conteúdo", os aplicativos especificados por caminho e nome de arquivo são verificados quanto a alterações no conteúdo do arquivo antes de serem excluídos do monitoramento pelo componente ProActiv. Se o conteúdo do arquivo tiver sido modificado, o aplicativo será monitorado novamente pelo componente ProActiv. Para o tipo "Caminho", nenhuma verificação de conteúdo é executada antes de o aplicativo ser excluído do monitoramento pelo Guard. Para alterar o tipo de exclusão, clique no tipo exibido.

#### Aviso

Use o tipo *Caminho* somente em casos excepcionais. Códigos de malware podem ser adicionados a um aplicativo através de uma atualização. O aplicativo originalmente confiável agora é um malware.

#### Nota

Alguns aplicativos confiáveis, incluindo, por exemplo, todos os componentes de aplicativo do programa AntiVir, são excluídos por padrão do monitoramento pelo componente ProActiv, mesmo que não estejam incluídos na lista.

#### Caixa de entrada

Nesta caixa, insira o aplicativo a ser excluído do monitoramento pelo componente ProActiv. Para identificar o aplicativo, o caminho completo, o nome e a extensão do arquivo devem ser especificados. O caminho deve mostrar a unidade em que o aplicativo está localizado ou começar com uma variável de ambiente.



O botão abre uma janela na qual é possível selecionar o aplicativo a ser excluído.

#### Adicionar

Com o botão "**Adicionar**", é possível transferir o aplicativo especificado na caixa de entrada para a lista de aplicativos a serem excluídos.

#### Excluir

O botão "**Excluir**" permite que você remova um aplicativo realçado da lista de aplicativos a serem excluídos.

### 13.2.3 Relatório

O Guard inclui uma função de registro abrangente para fornecer ao usuário ou administrador observações exatas sobre o tipo e a maneira de uma detecção.

#### Relatório

Este grupo permite determinar o conteúdo do arquivo do relatório.

**Desligar**

Se essa opção for ativada, o Guard não criará um registro.

É recomendado desativar a função de registro somente em casos excepcionais, por exemplo, se você executar avaliações com vários vírus ou programas indesejados.

**Padrão**

Se essa opção for ativada, o Guard registrará informações importantes (sobre detecções, alertas e erros) no arquivo de relatório, e as informações menos importantes serão ignoradas para facilitar a compreensão. Essa opção é ativada como configuração padrão.

**Avançado**

Se essa opção for ativada, o Guard registrará informações menos importantes no arquivo de relatório também.

**Concluído**

Se essa opção for ativada, o Guard registrará todas as informações disponíveis no arquivo de relatório, incluindo o tamanho e o tipo de arquivo, a data etc.

**Limitar arquivo de relatório**

**Limitar tamanho a n MB**

Se essa opção for ativada, o arquivo de relatório poderá ser limitado a um determinado tamanho; possíveis valores: os valores permitidos devem estar entre 1 e 100 MB. São permitidos aproximadamente 50 KB de espaço extra ao limitar o tamanho do arquivo de relatório para minimizar o uso dos recursos do sistema. Se o tamanho do arquivo de registro ultrapassar o tamanho indicado em mais de 50 KB, as entradas antigas serão excluídas até que o tamanho indicado menos 50 KB seja atingido.

**Fazer backup do arquivo de relatório antes de reduzi-lo**

Se essa opção for ativada, o backup do arquivo de relatório será feito antes de sua redução.

**Gravar configuração no arquivo de relatório**

Se essa opção for ativada, a configuração da verificação durante o acesso será registrada no arquivo de relatório.

**Observação**

Se você não tiver especificado nenhuma restrição de arquivo de relatório, um novo arquivo de relatório será criado automaticamente quando o arquivo de relatório atingir 100MB. Um backup do arquivo de relatório antigo foi criado. Até três backups dos arquivos de relatório antigos foram salvos. Os backups mais antigos são excluídos primeiro.

## 13.3 MailGuard

A seção MailGuard da Configuração é responsável pela configuração do MailGuard.

### 13.3.1 Fazer verificação

Use o MailGuard para verificar emails de entrada em busca de vírus, malware e spam. Os emails de saída podem ser verificados quanto a vírus e malware pelo MailGuard. Os emails de saída que são spams enviados de um bot desconhecido em seu computador podem ser bloqueados pelo MailGuard para evitar spams.

#### **Fazer verificação**

##### **Ativar MailGuard**

Se essa opção for ativada, o tráfego de e-mails será monitorado pelo MailGuard. O MailGuard é o servidor proxy que verifica o tráfego de dados entre seu servidor de email e o programa cliente de email no sistema do computador: os e-mails de entrada podem ser verificados quanto a malware por padrão. Se essa opção for desativada, o serviço do MailGuard ainda será iniciado, mas o monitoramento do MailGuard será desativado.

##### **Fazer verificação nos e-mails de entrada**

Se essa opção for ativada, os emails de entrada serão verificados em busca de vírus, malware e spam. O MailGuard é compatível com os protocolos POP3 e IMAP. Ative o monitoramento do MailGuard para a conta da caixa de entrada usada por seu cliente de email para receber emails.

##### **Monitorar contas POP3**

Se essa opção for ativada, as contas POP3 serão monitoradas nas portas especificadas.

##### **Portas monitoradas**

Nesse campo, você deve inserir a porta a ser usada como caixa de entrada pelo protocolo POP3. Várias portas são separadas por vírgulas.

##### **Padrão**

Esse botão redefine a porta especificada como a porta POP3 padrão.

##### **Monitorar contas IMAP**

Se essa opção for ativada, as contas IMAP serão monitoradas nas portas especificadas.

##### **Portas monitoradas**

Nesse campo, você deve inserir a porta a ser usada como caixa de entrada pelo protocolo IMAP. Várias portas são separadas por vírgulas.

##### **Padrão**

Esse botão redefine a porta especificada como a porta IMAP padrão.

##### **Fazer verificação nos e-mails de saída (SMTP)**

Se essa opção for ativada, os e-mails de saída serão verificados em busca de vírus e malware. Os e-mails que são spams enviados por bots desconhecidos são bloqueados.

##### **Portas monitoradas**

Nesse campo, você deve inserir a porta a ser usada como caixa de saída pelo protocolo SMTP. Várias portas são separadas por vírgulas.

##### **Padrão**

Esse botão redefine a porta especificada como a porta SMTP padrão.

#### **Nota**

Para verificar os protocolos e portas usados, chame as propriedades de suas contas de e-mail em seu programa cliente de e-mail. Na maioria das vezes, as portas padrão são usadas.

### 13.3.1.1. Ação para detecção

Essa seção de configuração contém configurações para as ações realizadas quando o MailGuard encontra um vírus ou programa indesejado em um email ou anexo.

#### **Nota**

Essas ações são realizadas quando um vírus é detectado tanto em e-mails de entrada quanto em e-mails de saída.

#### **Ação para detecção**

##### **Interativo**

Se essa opção for ativada, uma caixa de diálogo aparecerá quando um vírus ou programa indesejado for detectado em um e-mail ou anexo, na qual você poderá especificar o que deve ser feito com o e-mail ou anexo em questão. Essa opção é ativada como configuração padrão.

##### **Mostrar barra de andamento**

Se essa opção for ativada, o MailGuard mostrará uma barra de andamento durante o download de emails. Essa opção só poderá ser ativada se a opção **Interativo** tiver sido selecionada.

##### **Automático**

Se essa opção for ativada, você não será mais notificado quando um vírus ou programa indesejado for encontrado. O MailGuard reage de acordo com as configurações definidas nesta seção.

##### **Ação primária**

A Ação primária é a ação executada quando o MailGuard encontra um vírus ou programa indesejado em um email. Se a opção "**Ignorar e-mail**" for selecionada, também será possível, em "**Anexos afetados**", selecionar o processo para lidar com um vírus ou programa indesejado detectado em um anexo.

##### **Excluir e-mail**

Se essa opção for ativada, o e-mail afetado será excluído automaticamente caso um vírus ou programa indesejado seja encontrado. O corpo do e-mail é substituído pelo texto padrão fornecido abaixo. O mesmo se aplica a todos os anexos incluídos; eles também são substituídos por um texto padrão.

##### **Isolar e-mail**

Se essa opção for ativada, o e-mail completo, incluindo todos os anexos, será colocado na Quarentena se um vírus ou programa indesejado for encontrado. Se necessário, ele poderá ser restaurado posteriormente. O e-mail afetado propriamente dito é excluído. O corpo do e-mail é substituído pelo texto padrão fornecido abaixo. O mesmo se aplica a todos os anexos incluídos; eles também são substituídos por um texto padrão.

##### **Ignorar e-mail**

Se essa opção for ativada, o e-mail afetado será ignorado apesar da detecção de um vírus ou programa indesejado. No entanto, você pode decidir o que deve ser feito com o anexo afetado:

##### **Anexos afetados**

A opção "**Anexos afetados**" só poderá ser selecionada se a configuração "**Ignorar e-mail**" tiver sido selecionada em "**Ação primária**". Com essa opção, é possível decidir o que deve ser feito se um vírus ou programa indesejado for encontrado em um anexo.

##### **excluir**

Se essa opção for ativada, o anexo afetado será excluído se um vírus ou programa indesejado for encontrado e substituído por um texto padrão.

### **Isolar**

Se essa opção for ativada, o anexo afetado será colocado na Quarentena e excluído (substituído por um texto padrão). Se necessário, os anexos afetados poderão ser restaurados posteriormente.

### **Ignorar**

Se essa opção for ativada, o anexo será ignorado apesar da detecção de um vírus ou programa indesejado e entregue.

### **Aviso**

Se essa opção for selecionada, você não terá nenhuma proteção do MailGuard contra vírus e programas indesejados. Selecione esse item somente se tiver certeza do que está fazendo. Desative a visualização em seu programa de e-mail. Nunca abra anexos clicando duas vezes neles.

## 13.3.1.2. Outras ações

Essa seção de configuração contém outras configurações para as ações realizadas quando o MailGuard encontra um vírus ou programa indesejado em um email ou anexo.

### **Nota**

Essas ações são realizadas exclusivamente quando um vírus é detectado nos e-mails de entrada.

### **Texto padrão para e-mails excluídos e movidos**

O texto dessa caixa é inserido no e-mail como uma mensagem em vez do e-mail afetado. Você pode editar essa mensagem. O texto pode ter no máximo 500 caracteres.

Você pode usar a seguinte combinação de teclas para formatação:

**Strg** + **Enter** Insere uma quebra de linha.

### **Padrão**

O botão insere um texto padrão predefinido na caixa de edição.

### **Texto padrão para anexos excluídos e movidos**

O texto dessa caixa é inserido no e-mail como uma mensagem em vez do anexo afetado. Você pode editar essa mensagem. O texto pode ter no máximo 500 caracteres.

Você pode usar a seguinte combinação de teclas para formatação:

**Strg** + **Enter** Insere uma quebra de linha.

### **Padrão**

O botão insere um texto padrão predefinido na caixa de edição.

## 13.3.1.3. Heurística

Essa seção de configuração contém as configurações de heurística do mecanismo de verificação.

Os produtos AntiVir contêm uma heurística muito poderosa que pode detectar malwares desconhecidos de modo proativo, isto é, antes que uma assinatura de vírus especial para combater o elemento nocivo seja criada e antes que uma atualização de proteção contra vírus seja enviada. A detecção de vírus envolve uma análise abrangente e a investigação dos códigos afetados em busca de funções típicas de malware. Se o código que está sendo verificado apresentar esses recursos característicos, será considerado suspeito. Isso não significa necessariamente que o código é um malware genuíno. Falso-positivos também ocorrem às vezes. A decisão de como tratar o código afetado deve ser tomada pelo usuário, por exemplo, com base em seu conhecimento sobre a confiabilidade da origem do código.

### **Heurística para vírus de macro**

#### **Ativar heurística para vírus de macro**

O produto AntiVir contém uma heurística para vírus de macro muito poderosa. Se essa opção for ativada, todas as macros no documento em questão serão excluídas em caso de reparo. Por outro lado, os arquivos suspeitos são apenas relatados (por exemplo, você recebe um alerta). Essa opção é ativada como configuração padrão e é recomendada.

### **Detecção e análise heurística avançada (AHeAD)**

#### **ativar AHeAD**

O programa AntiVir contém uma heurística muito poderosa na forma da tecnologia AntiVir AHeAD, que também pode detectar malwares desconhecidos (novos). Se essa opção for ativada, você poderá definir até que ponto essa heurística deve ser "agressiva". Essa opção é ativada como configuração padrão.

#### **Nível de detecção baixo**

Se essa opção for ativada, malwares conhecidos serão detectados menos ligeiramente e o risco de alertas falsos é baixo nesse caso.

#### **Nível de detecção médio**

Essa opção será ativada como configuração padrão se você tiver selecionado o uso dessa heurística. Essa opção é ativada como configuração padrão e é recomendada.

#### **Nível de detecção alto**

Se essa opção for ativada, uma quantidade consideravelmente maior de malwares desconhecidos será detectada, mas existe a possibilidade de aparecerem falso-positivos.

## **13.3.1.4. AntiBot**

A função AntiBot do MailGuard impede que seu computador faça parte da conhecida bot-net e seja usado para enviar emails de spam: Para enviar spam através de uma bot-net, o invasor normalmente infecta diversos computadores com um bot que, em seguida, se conecta a um servidor IRC, abre um canal específico e aguarda o comando para enviar os e-mails de spam. Para diferenciar emails de spam de um bot desconhecido de emails genuínos, o MailGuard verifica se algum email de saída do servidor SMTP e do remetente do email está incluído nas listas de servidores e remetentes permitidos. Caso não esteja, os e-mails de saída serão bloqueados, isto é, o e-mail não será enviado. O email bloqueado é exibido em uma caixa de diálogo.

#### **Nota**

A função AntiBot só poderá ser usada se a verificação de emails de saída do MailGuard estiver ativada (consulte a opção **Verificar nos emails de saída** em MailGuard :: Fazer verificação).



### **Servidores permitidos**

Todos os servidores dessa lista têm autorização para enviar emails do MailGuard: os emails enviados para esses servidores **não** são bloqueados pelo MailGuard. Se nenhum servidor estiver incluído na lista, o servidor SMTP usado para enviar os e-mails de saída não será verificado. Se a lista estiver preenchida, o MailGuard bloqueará os emails enviados para qualquer servidor SMTP não incluído na lista.

#### **Caixa de entrada**

Insira o nome do host ou o endereço IP do servidor SMTP usado para enviar seus e-mails nessa caixa.

#### **Nota**

Você pode encontrar detalhes do servidor SMTP usado por seu programa de e-mail para enviar mensagens em seu programa de e-mail na data em que a conta de usuário foi criada.

#### **Adicionar**

Você pode usar esse botão para incluir os servidores especificados na caixa de entrada na lista de servidores permitidos.

#### **Excluir**

Esse botão exclui uma entrada destacada da lista de servidores permitidos. Esse botão estará desativado se nenhuma entrada for selecionada.

#### **Limpar tudo**

Esse botão exclui todas as entradas da lista de servidores permitidos.

### **Remetentes permitidos**

Todos os remetentes dessa lista têm autorização para enviar emails do MailGuard: os emails enviados desse endereço de email **não** são bloqueados pelo MailGuard. Se nenhum remetente estiver incluído na lista, o endereço de e-mail usado para enviar os e-mails de saída não será verificado. Se a lista estiver preenchida, o MailGuard bloqueará os emails dos remetentes não incluídos na lista.

#### **Caixa de entrada**

Insira os endereços de e-mail dos remetentes nessa caixa.

#### **Adicionar**

Você pode usar esse botão para incluir os remetentes especificados na caixa de entrada na lista de remetentes permitidos.

#### **Excluir**

Esse botão exclui uma entrada destacada da lista de remetentes permitidos. Esse botão estará desativado se nenhuma entrada for selecionada.

#### **Limpar tudo**

Esse botão exclui todas as entradas da lista de remetentes permitidos.

## 13.3.2 Geral

### 13.3.2.1. Exceções




#### **Exceções de varredura**

Essa tabela mostra a lista de endereços de email excluídos da verificação do AntiVir MailGuard (lista de permissões).

**Nota**

A lista de exceções é usada exclusivamente pelo MailGuard com relação aos emails de entrada.

**Status**

Ícone	Descrição
	Esse endereço de e-mail não será mais verificado quanto a spam.
	Esse endereço de e-mail não será mais verificado quanto a malware.
	Esse endereço de e-mail não será verificado quanto a malware ou spam.

**Endereço de e-mail**

E-mail que não será mais verificado.

**Malware**

Quando essa opção é ativada, o endereço de e-mail não é mais verificado quanto a malware.

**Spam**

Quando essa opção é ativada, o endereço de e-mail não é mais verificado quanto a spam.

**Para cima**

Você pode usar esse botão para mover um endereço de e-mail destacado para uma posição superior. Se nenhuma entrada estiver destacada ou o endereço destacado estiver na primeira posição da lista, esse botão estará desativado.

**Para baixo**

Você pode usar esse botão para mover um endereço de e-mail destacado para uma posição inferior. Se nenhuma entrada estiver destacada ou o endereço destacado estiver na última posição da lista, esse botão estará desativado.

**Caixa de entrada**

Nessa caixa, é possível inserir o endereço de e-mail que deseja adicionar à lista de endereços de e-mail que não devem ser verificados. Dependendo das configurações, o endereço de email não será mais verificado futuramente pelo MailGuard.

**Nota**

Você pode usar caracteres curinga ao inserir endereços de e-mail: \* para qualquer número de caracteres e ? somente para um caractere. No entanto, os caracteres curinga podem ser usados exclusivamente para os endereços de e-mail que não são verificados quanto a spam. Uma mensagem de erro será exibida se você tentar excluir um endereço que contém caracteres curinga da verificação de malware marcando a caixa de listagem de exclusão **Malware**. Ao inserir endereços com caracteres curinga, a sequência de caracteres especificada deve condizer com a estrutura de um endereço de email (\*@\*.\*).

**Aviso**

Observe os exemplos fornecidos quanto ao uso de caracteres curinga. Use os caracteres curinga somente de modo seletivo e tome cuidado com os endereços de e-mail que contém caracteres curinga e estão incluídos na lista de permissões de spam.

Exemplos: Uso de caracteres curinga em endereços de e-mail (lista de permissões de spam)

- `virus@avira.*` / = todos os e-mails com esse endereço e qualquer domínio de nível superior: `virus@avira.de`, `virus@avira.com`, `virus@avira.net` etc.
- `*@avira.com` = todos os emails enviados do domínio **avira.com**:  
`info@avira.com`, `virus@avira.com`, `kontakt@avira.com`, `employee@avira.com`
- `info@*.com` = todos os endereços de e-mail com o domínio de nível superior **com** e o endereço **info**: o domínio de segundo nível pode ser qualquer coisa:  
`info@name1.com`, `info@name2.com`...

### **Adicionar**

Com esse botão, é possível adicionar o endereço de e-mail inserido na caixa de entrada à lista de endereços de e-mail que não devem ser verificados.

### **Excluir**

Esse botão exclui um endereço de e-mail destacado da lista.

### **Importar catálogo de endereços do Outlook**

Com esse botão, você importa os endereços de e-mail do catálogo de endereços do programa de e-mail MS Outlook para a lista de exceções. Os endereços de e-mail importados não são verificados quanto a spam.

### **Importar catálogo de endereços do Outlook Express**

Use esse botão para importar o endereço de e-mail do catálogo de endereços do programa de e-mail MS Outlook Express para a lista de exceções. Os endereços de e-mail importados não são verificados quanto a spam.

## 13.3.2.2. Cache

### **Cache**

O cache do MailGuard contém dados sobre os emails verificados que são exibidos como dados estatísticos no Centro de controle em MailGuard. Cópias dos e-mails de entrada também são armazenadas no cache. Os e-mails também podem ser usados para as funções de treinamento do módulo antispam (Bom e-mail – use para treinamento, Spam – use para treinamento).

### **Nota**

O módulo antispam deve ser ativado para que o backup dos e-mails de entrada seja feito no cache.

### **Número máximo de e-mails a serem armazenados no cache**

Esse campo é usado para definir o número máximo de emails que são armazenados pelo MailGuard no cache. Os emails mais antigos são excluídos primeiro.

### **Período máximo de armazenamento de um e-mail em dias**

O período máximo de armazenamento de um e-mail em dias é inserido nessa caixa. Após esse período, o email é removido do cache.

### **Esvaziar cache**

Clique nesse botão para excluir os e-mails armazenados no cache.

### 13.3.2.3. MailGuard

#### **AntiSpam**

O serviço do AntiVir MailGuard verifica emails e anexos em busca de vírus e programas indesejados. Além disso, ele pode proteger você contra e-mails de spam de modo confiável.

#### **AntiSpam**

##### **Ativar módulo AntiSpam**

A ativação dessa opção ativa a função antispam do MailGuard.

##### **Marcar assunto do e-mail**

Se essa opção for ativada, uma observação é adicionada à linha de assunto original quando um e-mail de spam é detectado.

##### **Simples**

Se o e-mail de spam ou phishing for recebido, a marca [SPAM] ou [Phishing] será adicionada. Essa opção é ativada como configuração padrão.

##### **Detalhado**

A linha de assunto de um e-mail de spam ou phishing tem uma marca no início que chama a atenção para a probabilidade da mensagem ser spam.

##### **Ativar registro**

Se essa opção for ativada, o MailGuard criará um arquivo de relatório antispam especial.

##### **Usar listas negras em tempo real**

Quando essa opção é ativada, a chamada "lista negra" é consultada em tempo real, fornecendo informações adicionais para classificar e-mail de origem duvidosa como spam.

##### **Tempo limite: n segundo(s)**

Se as informações da lista negra não forem disponibilizadas depois de n segundos, a tentativa de consultar a lista negra será cancelada.

##### **Limpar banco de dados de treinamento**

Clique no botão para excluir o banco de dados de treinamento.

##### **Adicionar automaticamente destinatários de e-mail de saída à lista branca**

Se essa opção for ativada, os endereços dos destinatários dos e-mails de saída serão adicionados automaticamente à lista de permissões de spam (lista dos e-mails não verificados em busca de spam, definida em **MailGuard:: Geral :: Exceções**). Os e-mails de entrada enviados dos endereços da lista de permissões de spam não são verificados em busca de spam. No entanto, eles são verificados quanto a vírus e malwares. Essa opção é desativada como configuração padrão.

#### **Nota**

Essa opção só poderá ser ativada se a verificação de e-mails de saída do MailGuard estiver ativada (consulte a opção **Fazer verificação nos emails de saída** em MailGuard :: Fazer verificação).

### 13.3.2.4. Rodapé

Em *Rodapé*, é possível configurar um rodapé de email que é exibido nos emails enviados. Essa função requer a ativação da verificação feita pelo MailGuard dos emails de saída (consulte a opção *Fazer varredura nos emails de saída (SMTP)* em Configuração::MailGuard::Fazer varredura) . Você pode usar o rodapé definido pelo AntiVir MailGuard para confirmar que o email enviado foi verificado por um programa de proteção contra vírus. Você também pode inserir um texto personalizado para um rodapé definido pelo usuário. Se você usar as duas opções de rodapé, o texto definido pelo usuário virá depois do rodapé do AntiVir MailGuard.

#### **Rodapé para emails a serem enviados**

##### **Anexar rodapé do AntiVir MailGuard**

Se essa opção for ativada, o rodapé do AntiVir MailGuard será exibido abaixo do texto da mensagem do email enviado. O rodapé do AntiVir MailGuard confirma que o email enviado foi verificado pelo AntiVir MailGuard quanto a vírus e programas indesejados e não se origina de um bot desconhecido. O rodapé do AntiVir MailGuard contém o seguinte texto: "Verificado com o AntiVir MailGuard [versão do produto] [iniciais e número da versão do mecanismo de pesquisa] [iniciais e número da versão do arquivo de definição de vírus]".

##### **Anexar este rodapé**

Se essa opção for ativada, o texto que você inseriu na caixa de entrada será exibido como rodapé nos emails enviados.

##### **Caixa de entrada**

Nessa caixa de entrada, você pode inserir um texto que é exibido como uma nota de rodapé em emails enviados.

### 13.3.3 Relatório

O MailGuard inclui uma função de registro abrangente para fornecer ao usuário ou administrador observações exatas sobre o tipo e a maneira de uma detecção.

#### **Relatório**

Este grupo permite determinar o conteúdo do arquivo do relatório.

##### **Desligar**

Se essa opção for ativada, o MailGuard não criará um registro.

É recomendado desativar a função de registro somente em casos excepcionais, por exemplo, se você executar avaliações com vários vírus ou programas indesejados.

##### **Padrão**

Se essa opção for ativada, o MailGuard registrará informações importantes (sobre detecções, alertas e erros) no arquivo de relatório, e as informações menos importantes serão ignoradas para facilitar a compreensão. Essa opção é ativada como configuração padrão.

##### **Avançado**

Se essa opção for ativada, o MailGuard registrará informações menos importantes no arquivo de relatório também.

##### **Concluído**

Se essa opção for ativada, o MailGuard registrará todas as informações no arquivo de relatório.

### **Limitar arquivo de relatório**

#### **Limitar tamanho a n MB**

Se essa opção for ativada, o arquivo de relatório poderá ser limitado a um determinado tamanho; possíveis valores: os valores permitidos devem estar entre 1 e 100 MB. São permitidos aproximadamente 50 KB de espaço extra ao limitar o tamanho do arquivo de relatório para minimizar o uso dos recursos do sistema. Se o tamanho do arquivo de registro ultrapassar o tamanho indicado em mais de 50 KB, as entradas antigas serão excluídas até que o tamanho indicado menos 50 KB seja atingido.

#### **Fazer backup do arquivo de relatório antes de reduzi-lo**

Se essa opção for ativada, o backup do arquivo de relatório será feito antes de sua redução.

#### **Gravar configuração no arquivo de relatório**

Se essa opção for ativada, a configuração do MailGuard será registrada no arquivo de relatório.

#### **Observação**

Se você não tiver especificado nenhuma restrição de arquivo de relatório, um novo arquivo de relatório será criado automaticamente quando o arquivo de relatório atingir 100MB. Um backup do arquivo de relatório antigo foi criado. Até três backups dos arquivos de relatório antigos foram salvos. Os backups mais antigos são excluídos primeiro.

## 13.4 Firewall

A seção Firewall da Configuração é responsável pela configuração do componente Avira Firewall.

### 13.4.1 Regras do adaptador

No Avira FireWall, um adaptador representa um dispositivo de hardware com simulação de software (por exemplo, miniporta, conexão tipo ponte etc.) ou um dispositivo de hardware real (por exemplo, placa de rede).

O Avira FireWall exibe as regras de todos os adaptadores existentes no seu computador para os quais um driver foi instalado.

Uma regra de adaptador predefinida depende do nível de segurança. Você pode alterar o nível de segurança no Proteção on-line :: Você pode alterar as configurações do FireWall no Centro de controle ou definir suas próprias regras do adaptador. Se tiver definido suas próprias regras do adaptador, na seção FireWall do Centro de controle, o nível de segurança será definido como personalizado.

#### **Nota**

A configuração padrão de nível de segurança para todas as regras predefinidas do Avira FireWall é **Médio**.

## Protocolo ICMP

O Protocolo de mensagem de controle de Internet (ICMP) é usado para trocar mensagens de erro e informações em redes. O protocolo também é usado para mensagens de status com ping ou rota de rastreamento.

Com essa regra, é possível definir os tipos de mensagem de entrada e saída que devem ser bloqueados, o comportamento em caso de inundação e a reação a pacotes ICMP fragmentados. Essa regra serve para evitar os conhecidos ataques de flooding de ICMP, que resultam no aumento da carga da CPU da máquina atacada à medida que ela responde a cada pacote.

### Regras predefinidas para o protocolo ICMP

Configuração: Baixo	Configuração: Médio	Configuração: Alto
Tipos de entrada bloqueados: <b>nenhum tipo</b> . Tipos de saída bloqueados: <b>nenhum tipo</b> . Assumir flooding se o atraso entre pacotes for menor do que <b>50 ms</b> . <b>Rejeitar</b> pacotes ICMP fragmentados.	Mesma regra do nível inferior.	Tipos de entrada bloqueados: <b>vários tipos</b> Tipos de saída bloqueados: <b>vários tipos</b> Assumir flooding se o atraso entre pacotes for menor do que <b>50 ms</b> . <b>Rejeitar</b> pacotes ICMP fragmentados.

### Tipos de entrada bloqueados: nenhum tipo/vários tipos

Com o mouse, clique no link para exibir uma lista de tipos de pacote ICMP. Nessa lista, especifique os tipos de mensagem ICMP de entrada que deseja bloquear.

### Tipos de saída bloqueados: nenhum tipo/vários tipos

Com o mouse, clique no link para exibir uma lista de tipos de pacote ICMP. Nessa lista, selecione os tipos de mensagem ICMP de saída que deseja bloquear.

### Inundação

Com o mouse, clique no link para exibir uma caixa de diálogo na qual é possível inserir o atraso máximo permitido de ICMP.

### Pacotes ICMP fragmentados

Com o mouse, clique no link para rejeitar ou não os pacotes ICMP fragmentados.

## Verificação da porta TCP

Com essa regra, é possível definir quando uma verificação da porta TCP é suposta pelo FireWall e o que deve ser feito nesse caso. Essa regra serve para evitar o conhecido ataque de verificação da porta TCP, que resulta na detecção de portas TCP abertas no seu computador. Esse tipo de ataque é usado para procurar os pontos fracos de um computador e geralmente é seguido por tipos de ataque mais perigosos.

### Regras predefinidas para a verificação da porta TCP

Configuração: Baixo	Configuração: Médio	Configuração: Alto
Assumirá a verificação da	Assumirá a verificação da	Mesma regra do nível intermediário.

<p>porta TCP se <b>50</b> ou mais portas tiverem sido verificadas em <b>5.000</b> milissegundos. Quando detectado, <b>registra</b> o IP do invasor e <b>não adiciona</b> a regra para bloquear o ataque.</p>	<p>porta TCP se <b>50</b> ou mais portas tiverem sido verificadas em <b>5.000</b> milissegundos. Quando detectado, <b>registra</b> o IP do invasor e <b>adiciona</b> a regra para bloquear o ataque.</p>
--	--

### Portas

Com o mouse, clique no link para exibir uma caixa de diálogo na qual é possível inserir o número de portas que devem ser verificadas para que uma verificação da porta TCP seja assumida.

### Janela de horário de verificação de porta

Com o mouse, clique neste link para exibir uma caixa de diálogo na qual é possível inserir o horário para um determinado número de verificações de porta para que uma verificação da porta TCP seja assumida.

### Arquivo de relatório

Com o mouse, clique no link para registrar ou não o endereço IP do invasor.

### Regra

Com o mouse, clique no link para adicionar ou não a regra para bloquear o ataque de verificação da porta TCP.

## Verificação da porta UDP

Com essa regra, é possível definir quando uma verificação da porta UDP é suposta pelo FireWall e o que deve ser feito nesse caso. Essa regra evita os conhecidos ataques de verificação da porta UDP, que resultam na detecção de portas UDP abertas no seu computador. Esse tipo de ataque é usado para procurar os pontos fracos de um computador e geralmente é seguido por tipos de ataque mais perigosos.

### Regras predefinidas para a verificação da porta UDP

<b>Configuração: Baixo</b>	<b>Configuração: Médio</b>	<b>Configuração: Alto</b>
<p>Assumirá a verificação da porta UDP se <b>50</b> ou mais portas tiverem sido verificadas em <b>5.000</b> milissegundos. Quando detectado, <b>registra</b> o IP do invasor e <b>não adiciona</b> a regra para bloquear o ataque.</p>	<p>Assumirá a verificação da porta UDP se <b>50</b> ou mais portas tiverem sido verificadas em <b>5.000</b> milissegundos. Quando detectado, <b>registra</b> o IP do invasor e <b>adiciona</b> a regra para bloquear o ataque.</p>	<p>Mesma regra do nível intermediário.</p>

### Portas

Com o mouse, clique no link para exibir uma caixa de diálogo na qual é possível inserir o número de portas que devem ser verificadas para que uma verificação da porta UDP seja assumida.

### Janela de horário de verificação de porta



Com o mouse, clique neste link para exibir uma caixa de diálogo na qual é possível inserir o horário para um determinado número de verificações de porta para que uma verificação da porta UDP seja assumida.

**Arquivo de relatório**

Com o mouse, clique no link para registrar ou não o endereço IP do invasor.

**Regra**

Com o mouse, clique no link para adicionar ou não a regra para bloquear o ataque de verificação da porta UDP.

### 13.4.1.1. Regras de entrada

As regras de entrada são definidas para controlar o tráfego de entrada do Avira FireWall.

**Nota**

Quando um pacote é filtrado, as regras correspondentes são aplicadas sucessivamente e, portanto, a ordem das regras é muito importante. Altere a ordem das regras somente se tiver certeza do que está fazendo.

#### Regras predefinidas para o monitoramento do tráfego dos dados TCP

Configuração: Baixo	Configuração: Médio	Configuração: Alto
Nenhum tráfego de dados de entrada é bloqueado pelo Avira FireWall.	<ul style="list-style-type: none"> <li>– Permitir conexões TCP estabelecidas em 135</li> </ul> <p><b>Permitirá</b> pacotes TCP do endereço <b>0.0.0.0</b> com a máscara <b>0.0.0.0</b> se houver portas locais em <b>{135}</b> e portas remotas em <b>{0-65535}</b>. Aplicar aos <b>pacotes de conexões existentes</b>. <b>Não registra</b> quando o pacote corresponde à regra. Avançado: descartar pacotes que possuem os seguintes bytes <b>&lt;vazio&gt;</b> com a máscara <b>&lt;vazio&gt;</b> no deslocamento <b>0</b>.</p>	<ul style="list-style-type: none"> <li>– Tráfego dos dados TCP estabelecido pelo monitor</li> </ul> <p><b>Permitirá</b> pacotes TCP do endereço <b>0.0.0.0</b> com a máscara <b>0.0.0.0</b> se houver portas locais em <b>{0-65535}</b> e portas remotas em <b>{0-65535}</b>. Aplicar aos <b>pacotes de conexões existentes</b>. <b>Não registra</b> quando o pacote corresponde à regra. Avançado: descartar pacotes que possuem os seguintes bytes <b>&lt;vazio&gt;</b> com a máscara <b>&lt;vazio&gt;</b> no deslocamento <b>0</b>.</p>

- Negar pacotes TCP em 135

Negará **pacotes TCP** do endereço **0.0.0.0** com a máscara **0.0.0.0** se houver portas locais em **{135}** e portas remotas em **{0-65535}**. Aplicar a **todos os pacotes**.

**Não registra** quando o pacote corresponde à regra.

Avançado:

Descartar pacotes que possuem os seguintes bytes **<vazio>** com a máscara **<vazio>** no deslocamento **0**.

- Monitorar tráfego de dados de integridade TCP

**Permitirá** pacotes TCP do endereço **0.0.0.0** com a máscara **0.0.0.0** se houver portas locais em **{0-65535}** e portas remotas em **{0-65535}**. Aplicar ao **início da conexão e aos pacotes de conexão existentes**.

**Não registra** quando o pacote corresponde à regra.

Avançado:  
descartar pacotes

	<p>que possuem os seguintes bytes <b>&lt;vazio&gt;</b> com a máscara <b>&lt;vazio&gt;</b> no deslocamento <b>0</b>.</p> <p>– Negar todos os pacotes TCP</p> <p>Negar <b>pacotes TCP</b> do endereço <b>0.0.0.0</b> com a máscara <b>0.0.0.0</b> se as portas locais estiverem no intervalo <b>{0-65535}</b> e a porta remota estiver no intervalo <b>{0-65535}</b>. Aplicar a <b>todos os pacotes</b>. <b>Não registra</b> quando o pacote corresponde à regra. Avançado: descartar pacotes que possuem os seguintes bytes <b>&lt;vazio&gt;</b> com a máscara <b>&lt;vazio&gt;</b> no deslocamento <b>0</b>.</p>	
--	--	--

#### **Aceitar/rejeitar pacotes TCP**

Com o mouse, clique no link para permitir ou negar pacotes TCP de entrada com definição especial.

#### **Endereço IP**

Ao clicar neste link com o mouse, uma caixa de diálogo será exibida na qual é possível inserir o endereço IP obrigatório.

#### **Máscara IP**

Ao clicar neste link com o mouse, uma caixa de diálogo será exibida na qual é possível inserir a máscara IP obrigatória.

#### **Portas locais**

Com o mouse, clique neste link para exibir uma caixa de diálogo na qual é possível definir o número das portas locais ou intervalos de porta completos.

#### **Portas remotas**

Com o mouse, clique neste link para exibir uma caixa de diálogo na qual é possível definir o número das portas remotas ou intervalos de porta completos.

**Método de aplicação**

Com o mouse, clique neste link para aplicar a regra ao início da conexão e aos pacotes de conexão existentes, somente aos pacotes de conexões existentes ou a todos os pacotes.

**Arquivo de relatório**

Ao clicar no link com o mouse, você pode decidir se gravará ou não um arquivo de relatório caso o pacote esteja em conformidade com a regra.

O **recurso avançado** ativa a filtragem do conteúdo. Por exemplo, os pacotes podem ser rejeitados se tiverem alguns dados específicos em um determinado deslocamento. Se não desejar usar essa opção, não selecione um arquivo ou escolha um arquivo vazio.

**Conteúdo filtrado: dados**

Com o mouse, clique no link para exibir uma caixa de diálogo na qual é possível selecionar um arquivo que contém o buffer específico.

**Conteúdo filtrado: máscara**

Com o mouse, clique no link para exibir uma caixa de diálogo na qual é possível selecionar a máscara específica.

**Conteúdo filtrado: deslocamento**

Com o mouse, clique no link para exibir uma caixa de diálogo na qual é possível definir o deslocamento do conteúdo filtrado. O deslocamento é calculado a partir do final do cabeçalho TCP.

**Regras predefinidas para o monitoramento do tráfego dos dados UDP**

Configuração: Baixo	Configuração: Médio	Configuração: Alto
-	<ul style="list-style-type: none"> <li>Monitorar tráfego de dados aceito de UDP</li> </ul> <p><b>Permitirá</b> pacotes UDP do endereço <b>0.0.0.0</b> com a máscara <b>0.0.0.0</b> se a porta local estiver em <b>{0-65535}</b> e a porta remota estiver em <b>{0-65535}</b>. Aplicar regra às <b>portas abertas</b>. <b>Não registra</b> quando o pacote corresponde à regra. Avançado: descartar pacotes que possuem os seguintes bytes</p>	<p>UDP estabelecido pelo monitor tráfego</p> <p>Permitirá <b>pacotes UDP</b> do endereço <b>0.0.0.0</b> com a máscara <b>0.0.0.0</b> se a porta local estiver no intervalo <b>{0-65535}</b> e a porta remota estiver no intervalo <b>{53, 67, 68, 123}</b>. Aplicar regra às <b>portas abertas</b>. <b>Não registra</b> quando o pacote corresponde à regra. Avançado: descartar pacotes que possuem os seguintes bytes <b>&lt;vazio&gt;</b> com a máscara <b>&lt;vazio&gt;</b> no deslocamento <b>0</b>.</p>

	<p><b>&lt;vazio&gt;</b> com a máscara <b>&lt;vazio&gt;</b> no deslocamento <b>0</b>.</p> <p>– Negar todos os pacotes UDP</p> <p>Negará <b>pacotes UDP</b> do endereço <b>0.0.0.0</b> com a máscara <b>0.0.0.0</b> se as portas locais estiverem no intervalo <b>{0-65535}</b> e a porta remota estiver no intervalo <b>{0-65535}</b>.</p> <p>Aplicar a <b>todas as portas</b>. <b>Não registra</b> quando o pacote corresponde à regra.</p> <p>Avançado: descartar pacotes que possuem os seguintes bytes <b>&lt;vazio&gt;</b> com a máscara <b>&lt;vazio&gt;</b> no deslocamento <b>0</b>.</p>	
--	---	--

#### **Aceitar/rejeitar pacotes UDP**

Com o mouse, clique no link para permitir ou negar pacotes UDP de entrada com definição especial.

#### **Endereço IP**

Ao clicar neste link com o mouse, uma caixa de diálogo será exibida na qual é possível inserir o endereço IP obrigatório.

#### **Máscara IP**

Ao clicar neste link com o mouse, uma caixa de diálogo será exibida na qual é possível inserir a máscara IP obrigatória.

#### **Portas locais**

Com o mouse, clique neste link para exibir uma caixa de diálogo na qual é possível definir o número das portas locais ou intervalos de porta completos.

#### **Portas remotas**

Com o mouse, clique neste link para exibir uma caixa de diálogo na qual é possível definir o número das portas remotas ou intervalos de porta completos.

**Método de aplicação**

Com o mouse, clique neste link para aplicar esta regra a todas as portas ou somente a todas as portas abertas.

**Arquivo de relatório**

Ao clicar no link com o mouse, você pode decidir se gravará ou não um arquivo de relatório caso o pacote esteja em conformidade com a regra.

O **recurso avançado** ativa a filtragem do conteúdo. Por exemplo, os pacotes podem ser rejeitados se tiverem alguns dados específicos em um determinado deslocamento. Se não desejar usar essa opção, não selecione um arquivo ou escolha um arquivo vazio.

**Conteúdo filtrado: dados**

Com o mouse, clique no link para exibir uma caixa de diálogo na qual é possível selecionar um arquivo que contém o buffer específico.

**Conteúdo filtrado: máscara**

Com o mouse, clique no link para exibir uma caixa de diálogo na qual é possível selecionar a máscara específica.

**Conteúdo filtrado: deslocamento**

Com o mouse, clique no link para exibir uma caixa de diálogo na qual é possível definir o deslocamento do conteúdo filtrado. O deslocamento é calculado a partir do final do cabeçalho UDP.

**Regras predefinidas para o monitoramento do tráfego dos dados ICMP**

<b>Configuração: Baixo</b>	<b>Configuração: Médio</b>	<b>Configuração: Alto</b>
-	<ul style="list-style-type: none"> <li>- Não descartar ICMP com base em endereço IP</li> </ul> <p><b>Permitir</b> pacotes ICMP do endereço <b>0.0.0.0</b> com a máscara <b>0.0.0.0</b>.</p> <p><b>Não registra</b> quando o pacote corresponde à regra.</p> <p>Avançado: descartar pacotes que possuem os seguintes bytes <b>&lt;vazio&gt;</b> com a máscara <b>&lt;vazio&gt;</b> no deslocamento <b>0</b>.</p>	Mesma regra do nível intermediário.

**Aceitar/rejeitar pacotes ICMP**

Com o mouse, clique no link para permitir ou negar pacotes ICMP de entrada com definição especial.

### Endereço IP

Ao clicar neste link com o mouse, uma caixa de diálogo será exibida na qual é possível inserir o endereço IP obrigatório.

### Máscara IP

Ao clicar neste link com o mouse, uma caixa de diálogo será exibida na qual é possível inserir a máscara IP obrigatória.

### Arquivo de relatório

Ao clicar no link com o mouse, você pode decidir se gravará ou não um arquivo de relatório caso o pacote esteja em conformidade com a regra.

O **recurso avançado** ativa a filtragem do conteúdo. Por exemplo, os pacotes podem ser rejeitados se tiverem alguns dados específicos em um determinado deslocamento. Se não desejar usar essa opção, não selecione um arquivo ou escolha um arquivo vazio.

### Conteúdo filtrado: dados

Com o mouse, clique no link para exibir uma caixa de diálogo na qual é possível selecionar um arquivo que contém o buffer específico.

### Conteúdo filtrado: máscara

Com o mouse, clique no link para exibir uma caixa de diálogo na qual é possível selecionar a máscara específica.

### Conteúdo filtrado: deslocamento

Com o mouse, clique no link para exibir uma caixa de diálogo na qual é possível definir o deslocamento do conteúdo filtrado. O deslocamento é calculado a partir do final do cabeçalho ICMP.

## Regras predefinidas para os pacotes IP

Configuração: Baixo	Configuração: Médio	Configuração: Alto
-	-	Negar todos os pacotes IP  Negar <b>pacotes IP</b> do endereço <b>0.0.0.0</b> com a máscara <b>0.0.0.0</b> . <b>Não registra</b> quando o pacote corresponde à regra.

### Aceitar/negar pacotes IP

Ao clicar no link com o mouse, você pode decidir se aceitará ou rejeitará pacotes IP com definição especial.

### Endereço IP

Ao clicar neste link com o mouse, uma caixa de diálogo será exibida na qual é possível inserir o endereço IP obrigatório.

### Máscara IP

Ao clicar neste link com o mouse, uma caixa de diálogo será exibida na qual é possível inserir a máscara IP obrigatória.

### Arquivo de relatório

Ao clicar no link com o mouse, você pode decidir se gravará ou não um arquivo de relatório caso o pacote esteja em conformidade com a regra.

### Possíveis regras para monitorar pacotes IP com base em protocolos IP

#### Pacotes IP

Ao clicar no link com o mouse, você pode decidir se aceitará ou rejeitará pacotes IP com definição especial.

#### Endereço IP

Ao clicar neste link com o mouse, uma caixa de diálogo será exibida na qual é possível inserir o endereço IP obrigatório.

#### Máscara IP

Ao clicar neste link com o mouse, uma caixa de diálogo será exibida na qual é possível inserir a máscara IP obrigatória.

#### Protocolo

Ao clicar neste link com o mouse, uma caixa de diálogo será exibida na qual é possível inserir o protocolo IP obrigatório.

#### Arquivo de relatório

Ao clicar no link com o mouse, você pode decidir se gravará ou não um arquivo de relatório caso o pacote esteja em conformidade com a regra.

## 13.4.1.2. Regras de saída

As regras de saída são definidas para controlar o tráfego de saída do Avira Firewall. Você pode definir uma regra de saída para um dos seguintes protocolos: IP, ICMP, UDP e TCP.

#### **Nota**

Quando um pacote é filtrado, as regras correspondentes são aplicadas sucessivamente e, portanto, a ordem das regras é muito importante. Altere a ordem das regras somente se tiver certeza do que está fazendo.

#### **Botões**

Botão	Descrição
Adicionar	Permite criar uma nova regra. Se pressionar esse botão, a caixa de diálogo " <b>Adicionar nova regra</b> será aberta". Nessa caixa de diálogo, é possível selecionar novas regras.
Remover	Remove a regra selecionada.
Regra abaixo	Move a regra selecionada uma linha para baixo, isto é, diminui a prioridade da regra.
Regra acima	Move a regra selecionada uma linha para cima, isto é, aumenta a prioridade da regra.
Renomear	Permite dar outro nome à regra selecionada.



### Nota

Você pode adicionar novas regras para adaptadores individuais ou para todos os adaptadores presentes no computador. Para adicionar uma regra para todos os adaptadores, selecione **Computador** na hierarquia de adaptadores exibida e clique no botão **Adicionar**.

### Nota

Para alterar a posição de uma regra, você também pode usar o mouse para arrastar a regra até a posição desejada.

## 13.4.2 Regras de aplicativo

### Regras de aplicativo para o usuário

Esta lista contém todos os usuários do sistema. Se estiver conectado como administrador, você poderá selecionar o usuário a quem deseja aplicar as regras. Caso não seja um usuário com privilégios, você poderá ver apenas o usuário conectado no momento.

### Lista de aplicativos

Esta tabela mostra a lista dos aplicativos para os quais as regras são definidas. A lista de aplicativos contém as configurações de cada aplicativo que foi executado e tinha uma regra salva desde que o Avira FireWall foi instalado.

#### Visualização normal

	<b>Descrição</b>
Aplicativo	Nome do aplicativo.
Modo	Exibe o modo de regra de aplicativo selecionado : no modo <b>filtrado</b> , as regras do adaptador são verificadas e executadas após a execução da regra do aplicativo. No modo <i>com privilégios</i> , as regras do adaptador são ignoradas. Clique no link para alternar para um modo diferente.
Ação	Mostra a ação que o Avira FireWall executará automaticamente quando o aplicativo estiver usando a rede, independentemente do tipo de uso de rede. Com o mouse, clique no link para alternar para outro tipo de ação. Os tipos de ação são <b>Perguntar</b> , <b>Permitir</b> ou <b>Negar</b> . <b>Perguntar</b> é a ação padrão.

#### Configuração estendida

Se o acesso de um aplicativo à rede exigir regras individuais, você poderá criar as regras do aplicativo com base nos filtros de pacote, da mesma maneira como as regras do adaptador foram criadas. Para alterar para a configuração estendida das regras do aplicativo, primeiro ative o modo de especialista. Em seguida, altere a configuração de regras do aplicativo na seção FireWall::Configurações: ative a opção **Configurações estendidas** e salve a configuração clicando em **Aceitar** ou **OK**. Na configuração do firewall, selecione a seção **FireWall::Regras de aplicativo**: Uma coluna adicional com o cabeçalho *Filtragem* com a entrada *Simples* é exibida na lista de regras de aplicativo. Agora você tem uma **Filtragem** adicional: a opção *Avançado - Ação: regras*, que permite selecionar a configuração estendida.

	<b>Descrição</b>
Aplicativo	Nome do aplicativo.
Modo	Exibe o modo de regra de aplicativo selecionado : no modo <b>filtrado</b> , as regras do adaptador são verificadas e executadas após a execução da regra do aplicativo. No modo <i>com privilégios</i> , as regras do adaptador são ignoradas. Clique no link para alternar para um modo diferente.
Ação	Mostra a ação que o Avira FireWall executará automaticamente quando o aplicativo estiver usando a rede, independentemente do tipo de uso de rede. Se você escolher <i>Filtragem - Simples</i> , poderá clicar no link para selecionar outro tipo de ação. Os valores são <b>Perguntar</b> , <b>Permitir</b> , <b>Negar</b> ou <i>Estendido</i> . Se você escolher <i>Filtragem - Avançado</i> , o tipo de ação <i>Regras</i> será exibido. O link <b>Regras</b> abre a janela <b>Regras de aplicativo</b> , na qual é possível inserir regras específicas para o aplicativo.
Filtragem	Mostra o tipo de filtragem. Você pode selecionar outro tipo de filtragem clicando no link. <i>Simples</i> : na filtragem simples, a ação especificada é realizada em todas as atividades de rede executadas pelo software. <i>Avançado</i> : com esse tipo de filtragem, as regras que foram adicionadas à configuração estendida são aplicadas.

Se desejar criar regras específicas para um aplicativo, selecione a entrada **Avançado** em *Filtragem*. A entrada *Regras* é exibida na coluna **Ação**. Clique em **Regras** para abrir a janela e criar regras específicas do aplicativo.

**Regras de aplicativo especificadas na configuração estendida**

As regras de aplicativo especificadas permitem que você aceite ou negue o tráfego de dados especificado para o aplicativo ou aceite ou negue a escuta passiva de portas individuais. As seguintes opções estão disponíveis:

Permitir ou negar injeção de código

Injeção de código é uma técnica para introduzir o código no espaço de endereço de outro processo para executar ações, forçando esse processo a carregar uma biblioteca de links dinâmicos (DLL). A injeção de código é usada por malwares para, entre outras coisas, executar o código com a fachada de outro programa. Desse modo, o acesso à Internet na frente do FireWall pode ser ocultado. No modo padrão, a injeção de código é ativada para todos os aplicativos assinados.

Permitir ou negar a escuta passiva do aplicativo nas portas

Permitir ou negar tráfego de dados

Permitir ou negar pacotes IP de entrada e/ou saída

Permitir ou negar pacotes TCP de entrada e/ou saída

Permitir ou negar pacotes UDP de entrada e/ou saída

Você pode criar quantas regras quiser para cada aplicativo. As regras de aplicativo são executadas na sequência mostrada (Mais informações estão disponíveis ).

### Nota

Se você alterar a filtragem *Avançado* de uma regra de aplicativo, as regras de aplicativo já existentes na configuração estendida serão simplesmente desativadas, e não excluídas de modo permanente. Se você selecionar a filtragem *Avançado* novamente, as regras de aplicativo já existentes serão reativadas e exibidas na configuração estendida da janela de regras de aplicativo.

### Detalhes do aplicativo

Nesta caixa, é possível ver os detalhes do aplicativo selecionado na caixa de listagem de aplicativos.

	Descrição
Nome	Nome do aplicativo.
Caminho	Caminho completo até o arquivo executável.

### Botões

Botão	Descrição
Adicionar aplicativo	Permite criar uma nova regra de aplicativo. Se pressionar esse botão, uma caixa de diálogo será aberta. Aqui, é possível selecionar o aplicativo necessário para criar uma nova regra.
Remover regra	Remove a regra de aplicativo selecionada.
Recarregar	Recarrega a lista de aplicativos e, ao mesmo tempo, descarta as alterações que acabaram de ser feitas nas regras de aplicativo.

## 13.4.3 Fornecedores confiáveis

Uma lista de fabricantes de software confiáveis é exibida em *Fornecedores confiáveis*. Você pode adicionar ou remover fabricantes da lista usando a opção *Sempre confiar neste fornecedor* na janela pop-up *Evento de rede*. Para permitir o acesso à rede dos aplicativos que são assinados pelos fornecedores listados por padrão, ative a opção **Permitir aplicativos automaticamente dos fornecedores confiáveis**.

### Fornecedores confiáveis para usuário

Esta lista contém todos os usuários do sistema. Se estiver conectado como administrador, você poderá selecionar o usuário cuja lista de fornecedores confiáveis deseja visualizar ou atualizar. Caso não seja um usuário com privilégios, você poderá ver apenas o usuário atual conectado.

**Permitir aplicativos automaticamente criados por fornecedores confiáveis**

Se essa opção for ativada, o aplicativo fornecido com a assinatura de um fornecedor conhecido e confiável receberá permissão automaticamente para acessar a rede. A opção é ativada como configuração padrão.

**Fornecedores**

A lista mostra todos os fornecedores classificados como confiáveis.

**Botões**

Botão	Descrição
Remover	A entrada destacada é removida da lista de fornecedores confiáveis. Para remover o fornecedor selecionado permanentemente da lista, clique em <b>Aceitar</b> ou <b>OK</b> na janela de configuração.
Recarregar	As alterações feitas são desfeitas. A última lista salva é carregada.

**Nota**

Se você remover fornecedores da lista e, em seguida, selecionar **Aplicar**, os fornecedores serão removidos permanentemente da lista. A alteração não pode ser desfeita com a opção *Recarregar*. No entanto, você pode usar a opção *Sempre confiar neste fornecedor* na janela pop-up *Evento de rede* para adicionar um fornecedor à lista de fornecedores confiáveis novamente.

**Nota**

O FireWall prioriza as regras de aplicativo antes de criar entradas na lista de fornecedores confiáveis: se você tiver criado uma regra de aplicativo e o fornecedor estiver relacionado na lista de fornecedores confiáveis, a regra de aplicativo será executada.

## 13.4.4 Configurações

**Opções avançadas**

**Ativar FireWall:**

Se essa opção for ativada, o Avira FireWall será ativado e protegerá seu computador dos riscos da Internet e de outras redes.

**Interromper o Windows Firewall na inicialização**

Se essa opção for ativada, o Windows Firewall será desativado quando o computador for reiniciado. Essa opção é ativada como configuração padrão.

**O arquivo de hosts do Windows (não) está bloqueado.**

Se essa opção for definida como BLOQUEADO, o arquivo de hosts do Windows será protegido contra gravação. A manipulação não é mais permitida. Por exemplo, o malware não pode redirecionar você para sites indesejados. Por padrão, o estado dessa opção é NÃO BLOQUEADO.

### **Tempo limite de regra automática**

#### **Bloquear sempre**

Se essa opção for ativada, uma regra que tenha sido criada automaticamente, por exemplo, durante uma verificação de porta será retida.

#### **Remover regra após n segundos**

Se essa opção for ativada, uma regra que tenha sido criada automaticamente, por exemplo, durante uma verificação de porta será removida novamente após o tempo definido. Essa opção é ativada como configuração padrão.

### **Notificações**

As notificações definem os eventos sobre os quais você deseja receber uma notificação de área de trabalho do FireWall.

#### **Varredura de porta**

Se a opção for ativada, você receberá uma notificação de área de trabalho quando uma verificação de porta for detectada pelo FireWall.

#### **Inundação**

Se a opção for ativada, você receberá uma notificação de área de trabalho quando um ataque de flooding for detectado pelo FireWall.

#### **Aplicativos bloqueados**

Se a opção for ativada, você receberá uma notificação de área de trabalho quando o FireWall negar, isto é, bloquear a atividade de rede de um aplicativo.

#### **IP bloqueado**

Se a opção for ativada, você receberá uma notificação de área de trabalho quando o FireWall negar, isto é, bloquear o tráfego de dados de um endereço IP.

### **Regras de aplicativo**

As opções de regras de aplicativo são usadas para definir as opções de configuração das regras de aplicativo na seção FireWall::Regras de aplicativo.

#### **Opções avançadas**

Se essa opção for ativada, você poderá ajustar acessos de rede diferentes de um aplicativo individualmente.

#### **Configurações básicas**

Se essa opção for ativada, somente uma ação poderá ser definida para diferentes acessos de rede do aplicativo.

## 13.4.5 Configurações de pop-up

### **Configurações de pop-up**

#### **Inspecionar pilha de inicialização de processo**

Se essa opção for ativada, a inspeção da pilha de processo permitirá um controle mais preciso. O FireWall presumirá que nenhum dos processos não confiáveis da pilha poderá ser o que realmente está acessando a rede através de seu processo filho. Desse modo, uma janela pop-up diferente será aberta para cada processo não confiável na pilha de processo. Essa opção é desativada como configuração padrão.

#### **Permitir vários pop-ups por processo**

Se essa opção for ativada, um pop-up será acionado sempre que um aplicativo estabelecer conexão de rede. Se preferir, você pode ser notificado somente na primeira tentativa de conexão. Essa opção é desativada como configuração padrão.

#### **Desativar notificações de pop-up automaticamente no modo Jogo**

Se essa opção for ativada, o modo de jogo do Avira FireWall será ativado automaticamente quando um aplicativo for executado no modo de tela inteira no seu computador. No modo de jogo, todas as regras definidas de adaptador e aplicativo são aplicadas. Os aplicativos para os quais nenhuma regra é definida com as ações "Permitir" ou "Negar" podem acessar temporariamente a rede, de modo que nenhuma janela pop-up aparecerá com perguntas sobre o evento de rede.

### **Lembrar ação para este aplicativo**

#### **Sempre ativado**

Quando essa opção é ativada, a opção "**Lembrar ação para este aplicativo**" da caixa de diálogo "**Evento de rede**" é ativada como configuração padrão. Essa opção é ativada como configuração padrão.

#### **Sempre desativado**

Quando essa opção é ativada, a opção "**Lembrar ação para este aplicativo**" da caixa de diálogo "**Evento de rede**" é desativada como configuração padrão.

#### **Permitir aplicativo assinado**

Quando essa opção é ativada, a opção "**Lembrar ação para este aplicativo**" da caixa de diálogo "**Evento de rede**" é ativada automaticamente durante o acesso à rede por parte dos aplicativos assinados. Os fabricantes são: Microsoft, Mozilla, Opera, Yahoo, Google, Hewlett Packard, Sun, Skype, Adobe, Lexmark, Creative Labs, ATI e nVidia.

#### **Lembrar último estado usado**

Quando essa opção é ativada, a opção "**Lembrar ação para este aplicativo**" da caixa de diálogo "**Evento de rede**" é ativada da mesma maneira em que foi ativada no último evento de rede. Se a opção "**Lembrar ação para este aplicativo**" tiver sido ativada, essa opção será ativada no próximo evento de rede. Se a opção "**Lembrar ação para este aplicativo**" tiver sido desativada para o último evento de rede, essa opção também será desativada no próximo evento de rede.

### **Mostrar detalhes**

Neste grupo de opções de configuração, você pode configurar a exibição de informações detalhadas na janela **Evento de rede**.

#### **Mostrar detalhes sob demanda**

Se essa opção for ativada, as informações detalhadas serão exibidas somente na janela "Evento de rede" mediante solicitação, isto é, as informações detalhadas serão exibidas quando você clicar no botão "**Mostrar detalhes**" na janela "Evento de rede".

### **Sempre mostrar detalhes**

Se essa opção for ativada, as informações detalhadas sempre serão exibidas na janela "Evento de rede".

### **Lembrar último estado usado**

Se essa opção for ativada, a exibição das informações detalhadas será gerenciada da mesma maneira em que foi no evento de rede anterior. Se as informações detalhadas tiverem sido exibidas ou acessadas durante o último evento de rede, elas serão exibidas no próximo evento de rede. Se as informações detalhadas tiverem sido ocultadas e não exibidas durante o último evento de rede, elas não serão exibidas no próximo evento de rede.

## **Permitir com privilégios**

Neste grupo de opções de configuração, você pode definir o status da opção *Permitir com privilégios* na janela **Evento de rede**.

### **Sempre ativado**

Se essa opção for ativada, a opção "*Permitir com privilégios*" será ativada como configuração padrão na janela "Evento de rede".

### **Sempre desativado**

Se essa opção for ativada, a opção "*Permitir com privilégios*" será desativada como configuração padrão na janela "Evento de rede".

### **Lembrar último estado usado**

Se essa opção for ativada, o status da opção "*Permitir com privilégios*" será tratado da mesma forma em que foi no evento de rede anterior na janela "Evento de rede": Se a opção "*Permitir com privilégios*" tiver sido ativada para execução do último evento de rede, ela será ativada por padrão no próximo evento de rede. Se a opção "*Permitir com privilégios*" tiver sido desativada para execução do último evento de rede, ela será desativada como configuração padrão no próximo evento de rede.

## 13.5 WebGuard

A seção WebGuard da Configuração é responsável pela configuração do WebGuard.

### 13.5.1 Fazer verificação

O WebGuard protege você contra vírus ou malwares que atingem seu computador a partir de páginas da Web carregadas em seu navegador a partir da Internet. A opção *Fazer verificação* pode ser usada para definir o comportamento do componente WebGuard.

#### **Fazer verificação**

##### **Ativar o WebGuard**

Se essa opção for ativada, as páginas da Web solicitadas com um navegador serão verificadas quanto a vírus e malware. O WebGuard monitora os dados transferidos da Internet usando o protocolo HTTP nas portas 80, 8080 e 3128. Se alguma página da Web afetada for detectada, o carregamento das páginas da Web será bloqueado. Se essa opção for desativada, o serviço do WebGuard ainda será iniciado, mas a verificação em busca de vírus e malwares será desativada.

**Nota**

Para usar a função de controle dos pais, ative o WebGuard.

**Proteção da unidade**

A proteção da unidade permite que você defina configurações para bloquear I-Frames, também conhecidos como quadros internos. I-Frames são elementos HTML, isto é, elementos de páginas da Internet que delimitam uma área de uma página da Web. Os I-Frames podem ser usados para carregar e exibir conteúdos da Web diferentes (normalmente outros URLs) como documentos independentes em uma subjanela do navegador. Na maioria das vezes, os I-Frames são usados para anúncios em banner. Em alguns casos, os I-Frames são usados para ocultar malwares. Nesses casos, a área do I-Frame fica total ou parcialmente invisível no navegador. A opção *Bloquear I-frames suspeitos* permite verificar e bloquear o carregamento de I-Frames.

**Bloquear I-frames suspeitos**

Se essa opção for ativada, os I-Frames das páginas da Web solicitadas serão verificados de acordo com determinados critérios. Se houver I-Frames suspeitos em uma página da Web solicitada, o I-Frame será bloqueado. Uma mensagem de erro será exibida na janela do I-Frame.

**Padrão**

Se essa opção for ativada, os I-Frames com conteúdo suspeito serão bloqueados.

**Avançado**

Se essa opção for ativada, os I-Frames com conteúdo suspeito e os I-Frames usados de forma suspeita serão bloqueados. O uso de I-Frames será considerado suspeito se o I-Frame for muito pequeno e, portanto, invisível ou quase invisível no navegador ou se o I-Frame for colocado em uma posição incomum na página da Web.

### 13.5.1.1. Ação para detecção

**Ação para detecção**

Você pode definir as ações a serem executadas pelo WebGuard quando um vírus ou programa indesejado for detectado.

**Interativo**

Se essa opção for ativada, uma caixa de diálogo aparecerá quando um vírus ou programa indesejado for detectado durante uma verificação sob demanda, na qual você poderá especificar o que deve ser feito com o arquivo afetado. Essa opção é ativada como configuração padrão.

Clique aqui para obter mais informações.

**Mostrar barra de andamento**



Se essa opção for ativada, uma notificação será exibida na área de trabalho com uma barra de andamento de download se o download de um conteúdo do site ultrapassar o tempo limite de 20 segundos. Essa notificação foi criada especialmente para o download de sites com volumes de dados maiores: se estiver navegando com o WebGuard, o conteúdo do site não será baixado de modo incremental no navegador, pois ele será verificado quanto à presença de vírus e malware antes de ser exibido no navegador. Essa opção é desativada como configuração padrão.

### **Automático**

Se essa opção for ativada, nenhuma caixa de diálogo com uma detecção de vírus será exibida. O WebGuard reage de acordo com as configurações predefinidas nesta seção como ação primária ou secundária.

### **Ação primária**

A Ação primária é a ação executada quando o WebGuard encontra um vírus ou programa indesejado.

### **Negar acesso**

O site solicitado do servidor da Web e/ou todos os dados ou arquivos transferidos não são enviados para seu navegador. Uma mensagem de erro para notificar que o acesso foi negado é exibida no navegador. O WebGuard registrará a detecção no arquivo de relatório se a função de registro for ativada.

### **Isolar**

Caso um vírus ou malware seja detectado, o site solicitado do servidor da Web e/ou os dados e arquivos transferidos serão movidos para a quarentena. O arquivo afetado pode ser recuperado do Gerenciador de quarentena se tiver um valor informativo ou, se necessário, enviado para o Centro de pesquisa de malware da Avira.

### **Ignorar**

O site solicitado do servidor da Web e/ou os dados e arquivos que foram transferidos são encaminhados pelo WebGuard para seu navegador. O acesso ao arquivo é permitido e o arquivo é ignorado.

### **Aviso**

O arquivo afetado permanece ativo em sua estação de trabalho. Isso pode causar danos graves à estação de trabalho.

## 13.5.1.2. Solicitações bloqueadas

Em **Solicitações bloqueadas**, é possível especificar os tipos de arquivo e os tipos MIME (tipos de conteúdo para os dados transferidos) a serem bloqueados pelo WebGuard. O filtro da Web permite que você bloqueie URLs conhecidos de phishing e malware. O WebGuard impede a transferência de dados da Internet para seu computador.

### **Tipos de arquivo/tipos MIME a serem bloqueados pelo WebGuard (definido pelo usuário)**

Todos os tipos de arquivo e tipos MIME (tipos de conteúdo para os dados transferidos) na lista são bloqueados pelo WebGuard.

### **Caixa de entrada**

Nessa caixa, insira os nomes dos tipos MIME e dos tipos de arquivo que devem ser bloqueados pelo WebGuard. Para tipos de arquivo, insira a extensão do arquivo, por exemplo, **.htm**. Para tipos MIME, indique o tipo de mídia e, quando aplicável, o subtipo. As duas instruções são separadas uma da outra por uma única barra, por exemplo, **video/mpeg** ou **audio/x-wav**.

**Nota**

No entanto, os arquivos que já estão armazenados em seu computador como arquivos de Internet temporários e bloqueados pelo WebGuard podem ser baixados localmente da Internet pelo navegador do computador. Arquivos de Internet temporários são arquivos salvos em seu computador pelo navegador para que os sites possam ser acessados mais rapidamente.

**Nota**

A lista de tipos de arquivo e MIME bloqueados será ignorada se os tipos forem inseridos na lista de tipos de arquivo e MIME excluídos em WebGuard::Fazer varredura::Exceções.

**Nota**

Nenhum caractere curinga (\* para qualquer número de caracteres ou ? para um único caractere) pode ser usado ao inserir os tipos de arquivo e os tipos MIME.

Tipos MIME: exemplos para tipos de mídia:

- text = para arquivos de texto
- image = para arquivos gráficos
- video = para arquivos de vídeo
- audio = para arquivos de som
- application = para arquivos vinculados a um programa específico

Exemplos: tipos de arquivo e MIME excluídos

- application/octet-stream = os arquivos de tipo MIME application/octet-stream (arquivos executáveis \*.bin, \*.exe, \*.com, \*.dll, \*.class) são bloqueados pelo WebGuard.
- application/olescript = os arquivos de tipo MIME application/olescript (arquivos de script ActiveX \*.axs) são bloqueados pelo WebGuard.
- .exe = todos os arquivos com a extensão .exe (arquivos executáveis) são bloqueados pelo WebGuard.
- .msi = todos os arquivos com a extensão .msi (arquivos do Windows Installer) são bloqueados pelo WebGuard.

**Adicionar**

O botão permite copiar os tipos MIME e de arquivo do campo de entrada na janela de exibição.

**Excluir**

O botão exclui uma entrada selecionada da lista. Esse botão estará desativado se nenhuma entrada for selecionada.

**Filtro da Web**

O filtro da Web baseia-se em um banco de dados interno, atualizado diariamente, que classifica os URLs de acordo com o conteúdo.

**Ativar filtro da Web**

Quando a opção está ativada, todos os URLs que correspondem às categorias selecionadas na lista de filtro da Web são bloqueados.

**Lista de filtro da Web**

Na lista de filtro da Web, é possível selecionar as categorias de conteúdo cujos URLs devem ser bloqueados pelo WebGuard.

**Nota**

O filtro da Web é ignorado para as entradas na lista de URLs excluídos em WebGuard::Fazer varredura::Exceções.

**Nota**

URLs de spam são URLs enviados com e-mails de spam. A categoria Fraude e enganação abrange as páginas da Web com “Validade de assinatura” e outras ofertas de serviços cujos custos são ocultados pelo fornecedor.

### 13.5.1.3. Exceções

Essas opções permitem definir exceções com base nos tipos MIME (tipos de conteúdo para os dados transferidos) e nos tipos de arquivo para URLs (endereços da Internet) para a verificação realizada pelo WebGuard. Os tipos MIME e os URLs especificados são ignorados pelo WebGuard, isto é, os dados não são verificados em busca de vírus e malwares quando são transferidos para seu computador.

#### Tipos MIME ignorados pelo WebGuard

Nesse campo, é possível selecionar os tipos MIME (tipos de conteúdo para os dados transferidos) a serem ignorados pelo WebGuard durante a verificação.

#### Tipos de arquivo/tipos MIME ignorados pelo WebGuard (definido pelo usuário)

Todos os tipos MIME (tipos de conteúdo para os dados transferidos) na lista são ignorados pelo WebGuard durante a verificação.

##### Caixa de entrada

Nessa caixa, é possível inserir o nome dos tipos MIME e dos tipos de arquivo a serem ignorados pelo WebGuard durante a verificação. Para tipos de arquivo, insira a extensão do arquivo, por exemplo, **.htm**. Para tipos MIME, indique o tipo de mídia e, quando aplicável, o subtipo. As duas instruções são separadas uma da outra por uma única barra, por exemplo, **video/mpeg** ou **audio/x-wav**.

**Nota**

Nenhum caractere curinga (\* para qualquer número de caracteres ou ? para um único caractere) pode ser usado ao inserir os tipos de arquivo e os tipos MIME.

**Aviso**

Todos os tipos de arquivo e tipos de conteúdo na lista de exclusão são baixados do navegador da Internet sem nenhuma verificação do acesso bloqueado (lista de tipos de arquivos e MIME a serem bloqueados em WebGuard::Fazer verificação::Acesso bloqueado) ou do WebGuard: Para todas as entradas na lista de exclusão, as entradas na lista de tipos de arquivo e MIME a serem bloqueados são ignoradas. Nenhuma verificação quanto a vírus e malwares é executada.

Tipos MIME: exemplos para tipos de mídia:

- text = para arquivos de texto
- image = para arquivos gráficos
- video = para arquivos de vídeo
- audio = para arquivos de som
- application = para arquivos vinculados a um programa específico

Exemplos: tipos de arquivo e MIME excluídos

- `audio/` = Todos os arquivos de tipo de mídia de áudio são excluídos das verificações do WebGuard
- `video/quicktime` = Todos os arquivos de vídeo do subtipo Quicktime (\*.qt, \*.mov) são excluídos das verificações do WebGuard
- `.pdf` = Todos os arquivos Adobe PDF são excluídos das verificações do WebGuard.

**Adicionar**

O botão permite copiar os tipos MIME e de arquivo do campo de entrada na janela de exibição.

**Excluir**

O botão exclui uma entrada selecionada da lista. Esse botão estará desativado se nenhuma entrada for selecionada.

**URLs ignorados pelo WebGuard**

Todos os URLs dessa lista são excluídos das verificações do WebGuard.

**Caixa de entrada**

Nessa caixa, é possível inserir os URLs (endereços da Internet) a serem excluídos das verificações do WebGuard, por exemplo, **www.domainname.com**. Você pode especificar partes do URL, usando pontos no início e no final para indicar o nível do domínio: `.domainname.com` para todas as páginas e todos os subdomínios do domínio. Indique os sites com qualquer domínio de nível superior (`.com` ou `.net`) com um ponto no final: `domainname.`. Se você indicar uma string sem um ponto no início ou no final, a string será interpretada como um domínio de nível superior, como **net**, para todos os domínios NET (`www.domain.net`).

**Nota**

Você também pode usar o caractere curinga \* para qualquer número de caracteres ao especificar os URLs. Os pontos no início ou no final também podem ser usados junto com os caracteres curinga para indicar o nível do domínio:

`.domainname.*`

`*.domainname.com`

`*nome*.com` (válido, mas não recomendado)

As especificações sem pontos, como `*nome*`, são interpretadas como parte de um domínio de nível superior e não são recomendadas.

**Aviso**

Todos os sites na lista de URLs excluídos são baixados no navegador da Internet sem serem verificados pelo filtro da Web ou WebGuard: Para todas as entradas na lista de URLs excluídos, as entradas no filtro da Web (consulte WebGuard::Fazer varredura::Acesso bloqueado) são ignoradas. Nenhuma verificação quanto a vírus e malwares é executada. Desse modo, somente os URLs confiáveis devem ser excluídos das verificações do WebGuard.

**Adicionar**

O botão permite copiar o URL inserido no campo de entrada (endereço da Internet) na janela do visualizador.

**Excluir**

O botão exclui uma entrada selecionada da lista. Esse botão estará desativado se nenhuma entrada for selecionada.

### Exemplos: URLs ignorados

– `www.avira.com` -OU- `www.avira.com/*`

= Todos os URLs com o domínio “www.avira.com” são excluídos das verificações do WebGuard: `www.avira.com/en/pages/index.php`, `www.avira.com/en/support/index.html`, `www.avira.com/en/download/index.html` etc.

Os URLs com o domínio “www.avira.de” não são excluídos das verificações do WebGuard.

– `avira.com` -OU- `*.avira.com`

= Todos os URLs com o domínio de nível superior e de segundo nível “avira.com” são excluídos das verificações do WebGuard: a especificação implica todos os subdomínios existentes para “.avira.com”: `www.avira.com`, `www.avira.de`, `forum.avira.com` etc.

– `avira.` -OU- `*.avira.*`

= Todos os URLs com o domínio de segundo nível “avira” são excluídos das verificações do WebGuard: A especificação implica todos os domínios de nível superior ou subdomínios existentes para “.avira”: `www.avira.com`, `www.avira.de`, `forum.avira.com` etc.

– `.*domínio*.*`

Todos os URLs que contêm um domínio de segundo nível com a string “domínio” são excluídos das verificações do WebGuard: `www.domínio.com`, `www.novo-domínio.de`, `www.exemplo-domínio1.de`, ...

– `net` -OU- `*.net`

= Todos os URLs com o domínio de nível superior “net” são excluídos das verificações do WebGuard: `www.nome1.net`, `www.nome2.net` etc.

### **Aviso**

Insira os URLs que deseja excluir da verificação do WebGuard com a maior precisão possível. Evite especificar um domínio de nível superior inteiro ou partes de um domínio de segundo nível, pois as páginas da Internet que distribuem malwares e programas indesejados serão excluídas da verificação do WebGuard através das especificações globais em Exclusões. É recomendado especificar pelo menos o domínio de segundo nível completo e o domínio de nível superior: `domainname.com`

### 13.5.1.4. Heurística

Essa seção de configuração contém as configurações de heurística do mecanismo de verificação.

Os produtos AntiVir contêm uma heurística muito poderosa que pode detectar malwares desconhecidos de modo proativo, isto é, antes que uma assinatura de vírus especial para combater o elemento nocivo seja criada e antes que uma atualização de proteção contra vírus seja enviada. A detecção de vírus envolve uma análise abrangente e a investigação dos códigos afetados em busca de funções típicas de malware. Se o código que está sendo verificado apresentar esses recursos característicos, será considerado suspeito. Isso não significa necessariamente que o código é um malware genuíno. Falso-positivos também ocorrem às vezes. A decisão de como tratar o código afetado deve ser tomada pelo usuário, por exemplo, com base em seu conhecimento sobre a confiabilidade da origem do código.

### **Heurística para vírus de macro**

#### **Heurística para vírus de macro**

O produto AntiVir contém uma heurística para vírus de macro muito poderosa. Se essa opção for ativada, todas as macros no documento em questão serão excluídas em caso de reparo. Por outro lado, os arquivos suspeitos são apenas relatados (por exemplo, você recebe um alerta). Essa opção é ativada como configuração padrão e é recomendada.

### **Detecção e análise heurística avançada (AHeAD)**

#### **ativar AHeAD**

O programa AntiVir contém uma heurística muito poderosa na forma da tecnologia AntiVir AHeAD, que também pode detectar malwares desconhecidos (novos). Se essa opção for ativada, você poderá definir até que ponto essa heurística deve ser "agressiva". Essa opção é ativada como configuração padrão.

#### **Nível de detecção baixo**

Se essa opção for ativada, malwares conhecidos serão detectados menos ligeiramente e o risco de alertas falsos é baixo nesse caso.

#### **Nível de detecção médio**

Essa opção será ativada como configuração padrão se você tiver selecionado o uso dessa heurística.

#### **Nível de detecção alto**

Se essa opção for ativada, uma quantidade consideravelmente maior de malwares desconhecidos será detectada, mas existe a possibilidade de aparecerem falso-positivos.

## **13.5.2 Relatório**

O WebGuard inclui uma função de registro abrangente para fornecer ao usuário ou administrador observações exatas sobre o tipo e a maneira de uma detecção.

### **Relatório**

Este grupo permite determinar o conteúdo do arquivo do relatório.

#### **Desligar**

Se essa opção for ativada, o WebGuard não criará um registro.

É recomendado desativar a função de registro somente em casos excepcionais, por exemplo, se você executar avaliações com vários vírus ou programas indesejados.

### **Padrão**

Se essa opção for ativada, o WebGuard registrará informações importantes (sobre detecções, alertas e erros) no arquivo de relatório, e as informações menos importantes serão ignoradas para facilitar a compreensão. Essa opção é ativada como configuração padrão.

### **Avançado**

Se essa opção for ativada, o WebGuard registrará informações menos importantes no arquivo de relatório também.

### **Concluído**

Se essa opção for ativada, o WebGuard registrará todas as informações disponíveis no arquivo de relatório, incluindo o tamanho e o tipo de arquivo, a data etc.

## **Limitar arquivo de relatório**

### **Limitar tamanho a n MB**

Se essa opção for ativada, o arquivo de relatório poderá ser limitado a um determinado tamanho; possíveis valores: os valores permitidos devem estar entre 1 e 100 MB. São permitidos aproximadamente 50 KB de espaço extra ao limitar o tamanho do arquivo de relatório para minimizar o uso dos recursos do sistema. Se o tamanho do arquivo de registro ultrapassar o tamanho indicado em mais de 50 KB, as entradas antigas serão excluídas até que o tamanho indicado seja reduzido em 20% .

### **Fazer backup do arquivo de relatório antes de reduzi-lo**

Se essa opção for ativada, o backup do arquivo de relatório será feito antes de sua redução.

### **Gravar configuração no arquivo de relatório**

Se essa opção for ativada, a configuração da verificação durante o acesso será registrada no arquivo de relatório.

### **Observação**

Se você não tiver especificado nenhuma restrição de arquivo de relatório, as entradas mais antigas serão excluídas automaticamente quando o arquivo de relatório atingir 100MB. As entradas são excluídas até o tamanho do arquivo de relatório atingir 80MB.

## 13.6 Controles parentais

O programa AntiVir tem uma função de controle dos pais para filtrar conteúdo da Internet indesejável ou ilegal e limitar as durações de uso da Internet. A função de controles dos pais faz parte do componente WebGuard. É possível atribuir funções aos usuários do computador. Uma função de usuário é configurável e inclui um conjunto de regras com os seguintes critérios:

- URLs (endereços da Internet) proibidos ou permitidos
- Categorias de conteúdo proibido
- Duração do uso da Internet e, se necessário, períodos de uso permitidos durante a semana

Quando o conteúdo da Internet é bloqueado de acordo com categorias específicas, listas de filtros avançados de URL são usadas; nessas listas, os URLs são classificados em grupos de conteúdo com base no conteúdo das páginas da Internet. As listas de filtro de URL são atualizadas, adaptadas e expandidas por hora. As funções de crianças, adolescentes e adultos são pré-configuradas com as categorias proibidas relevantes.

Os registros de uso da Internet baseiam-se em solicitações da Internet que duram pelo menos 5 minutos.

Se o controle dos pais for ativado, todas as páginas da Web solicitadas pelo usuário enquanto navega na Internet serão verificadas com base na função do usuário. Se as páginas da Web forem proibidas, serão bloqueadas e uma mensagem será exibida no navegador. Se a duração do uso permitido for ultrapassada ou se o uso ocorrer fora do período permitido, os sites solicitados serão bloqueados. Uma mensagem é exibida no navegador.

#### **Aviso**

Para usar a função de controles dos pais, é necessário ativar o serviço do WebGuard.

#### **Aviso**

Proteja a configuração do programa AntiVir com uma senha ao ativar o controle dos pais. Se a configuração não for protegida por uma senha, todos os usuários do computador poderão alterar ou desativar as configurações de controle dos pais. A proteção por senha é ativada em Geral::Senha.

Se você tiver definido uma senha para o controle dos pais, a configuração do controle dos pais será ocultada e o botão *Protegido por senha* será exibido.

#### **Protegido por senha**

Para ativar a configuração do controle dos pais, pressione o botão "**Protegido por senha**" e insira a senha de controle dos pais na janela "*Inserir senha*".

#### **Ativar controle parental**

Se essa opção for ativada, todas as páginas da Web solicitadas pelo usuário enquanto navega na Internet serão verificadas com base na função atribuída ao usuário registrado na função de controle dos pais. As páginas da Web solicitadas serão bloqueadas se tiverem sido classificadas como proibidas na função atribuída.

#### **Nota**

Quando o controle dos pais está ativado, os usuários *padrão* do computador que não receberam nenhuma função quando o controle dos pais foi configurado são designados com a função de *criança*. É possível alterar a função do usuário padrão. Após a instalação, as funções de criança, adolescente e adulto são criadas. A restrição do tempo de uso da Internet é desativada para funções pré-configuradas.

### **Seleção do usuário**

#### **Lista de funções de usuário**

A lista mostra todos os usuários adicionados e suas respectivas funções. Quando um usuário é adicionado, o programa atribui a função de *criança* por padrão. Com o mouse, clique na função exibida para alternar para outra função.

#### **Usuário**

A lista contém todos os usuários do sistema.

#### **Adicionar**

O botão pode ser usado para adicionar o usuário selecionado à lista de usuários protegidos.

#### **Excluir**



O botão exclui uma entrada selecionada da lista.

### **Nota**

O usuário padrão não pode ser excluído.

## **Funções**

### **Lista**

A lista mostra todas as funções adicionadas. Clique duas vezes em uma função exibida para abrir a caixa de diálogo que permite definir a função.

### **Caixa de entrada**

Nesse campo, é possível inserir o nome da função que deseja adicionar às funções de usuário.

### **Alterar**

O botão "Editar" pode ser usado para configurar a função selecionada. Uma caixa de diálogo é exibida na qual é possível definir os URLs proibidos e permitidos para a função e o conteúdo da Web proibido selecionado por categoria.

### **Adicionar**

Com esse botão, é possível adicionar a função inserida na caixa de entrada à lista de funções disponíveis.

### **Excluir**

O botão exclui uma função realçada da lista.

### **Nota**

As funções que já foram atribuídas a um usuário não podem ser excluídas.

### **Propriedades de função**

O botão *Editar* permite acessar a caixa de diálogo *Propriedades de função* em que é possível definir a função de usuário com URLs proibidos e permitidos, bem como conteúdo da Web proibido. As seguintes opções estão disponíveis:

- Proibir acesso a URLs
- Permitir acesso a URLs
- Bloquear conteúdo da Web: Bloquear conteúdo da Web. Você pode selecionar categorias para o conteúdo da Web a ser bloqueado.
- Limitar tempo de uso da Internet: você pode definir um tempo de uso permitido (por dia, semana, mês). É possível ativar períodos de uso exatos durante a semana.

## 13.7 Backup

A seção Backup da Configuração é responsável pela configuração do componente Avira Backup.

### 13.7.1 Configurações

Em **Configurações**, é possível configurar o comportamento do componente Backup.

#### **Configurações**

### **Fazer backup somente dos arquivos modificados**

Se essa opção for ativada, um backup incremental será criado: Somente os arquivos que foram modificados desde o último backup são salvos no perfil de backup. Se essa opção for desativada, um backup completo será criado para cada perfil de backup salvo: todos os arquivos são salvos no perfil de backup. Essa opção é ativada como configuração padrão e é recomendada, pois os backups incrementais podem ser criados mais rapidamente e consomem menos recursos do que os backups de dados completos.

### **Fazer a verificação quanto a vírus e programas indesejados antes do backup**

Se essa opção for ativada, os arquivos que estão sendo salvos serão verificados quanto a vírus e malware durante o backup. Os arquivos infectados não são salvos. Essa opção é ativada como configuração padrão e é recomendada.

## 13.7.2 Exceções

Em Exceções, é possível especificar quais objetos e tipos de arquivo são salvos, e quais não são salvos no backup.

### **Arquivos ignorados no backup**

A lista dessa janela contém os arquivos e os caminhos que não são salvos no backup.

#### **Nota**

As entradas da lista devem ter no máximo 6000 caracteres no total.

#### **Nota**

Os arquivos incluídos nessa lista são registrados no Arquivo de relatório.

### **Caixa de entrada**

Insira os nomes dos objetos de arquivo que não devem ser salvos nessa caixa. O caminho do diretório temporário das configurações locais do usuário conectado é inserido como padrão.



O botão abre uma janela na qual é possível selecionar o arquivo ou caminho desejado. Se tiver o nome completo e o caminho do arquivo, você poderá isolar um arquivo específico do backup. Caso tenha inserido um nome ou caminho de arquivo, todos os arquivos com esse nome (independentemente do caminho ou da unidade) não serão salvos.

### **Adicionar**

Com esse botão, você pode adicionar o objeto de arquivo inserido na caixa de entrada à janela de exibição.

### **Excluir**

O botão exclui uma entrada selecionada da lista. Esse botão estará desativado se nenhuma entrada for selecionada.

### **Redefinir lista**

Esse botão restaura os valores padrão predefinidos.

Leve em consideração o seguinte:

- O nome do arquivo pode conter somente os caracteres curinga \* (qualquer número de caracteres) e ? (um único caractere).
- A lista é processada de cima para baixo.
- Se um diretório for excluído, todos os subdiretórios também serão excluídos automaticamente.

- Extensões de arquivo individuais também podem ser excluídas (inclusive curingas).
- Para excluir também os objetos quando forem acessados com nomes curtos de arquivo DOS (convenção de nome DOS 8.3), o nome curto relevante do arquivo deve ser inserido na lista.

### **Nota**

Um nome de arquivo que contém caracteres curinga não pode terminar com uma barra invertida.

Por exemplo:

```
C:\Arquivos de programas\Application\applic*.exe\
```

Essa entrada não é válida e não é tratada como uma exceção.

### Exemplos:

```
application.exe
```

```
\Arquivos de programas\
```

```
C:\*.*
```

```
C:\*
```

```
*.exe
```

```
*.xl?
```

```
*.*
```

```
C:\Arquivos de programas\Application\application.exe
```

```
C:\Arquivos de programas\Application\applic*.exe
```

```
C:\Arquivos de programas\Application\applic*
```

```
C:\Arquivos de programas\Application\applic?????.e*
```

```
C:\Arquivos de programas\
```

```
C:\Arquivos de programas
```

```
C:\Arquivos de programas\Application\*.mdb
```

## **Listas de extensões de arquivo**

### **Considerar todas as extensões de arquivo**

Se essa opção for ativada, todos os arquivos do perfil de backup serão salvos.

### **Ativar backup de extensões de arquivo ignoradas**

Se essa opção for ativada, todos os arquivos do perfil de backup serão salvos, exceto os arquivos cujas extensões tenham sido inseridas na lista de extensões de arquivo excluídas.

### **Extensões de arquivo**

Esse botão abre uma caixa de diálogo que exibe todas as extensões de arquivo não salvas durante um backup quando a opção "**Extensões de arquivo excluídas**" está ativada. As entradas padrão são definidas para as extensões, mas as entradas podem ser adicionadas ou excluídas.

### **Ativar backup das listas de extensões de arquivo consideradas**

Se essa opção for ativada, somente os arquivos cujas extensões tenham sido inseridas na lista de extensões de arquivo a serem consultadas serão salvos.

### **Extensões de arquivo**

Esse botão abre uma caixa de diálogo que exibe todas as extensões de arquivo salvas durante um backup quando a opção "**Extensões de arquivo incluídas**" está ativada. As entradas padrão são definidas para as extensões, mas as entradas podem ser adicionadas ou excluídas.

### 13.7.3 Relatório

O componente Backup inclui uma abrangente função de registro.

#### **Relatório**

Este grupo permite determinar o conteúdo do arquivo do relatório.

#### **Desligar**

Se essa opção for ativada, o componente Backup não criará um registro. Desative a função de registro somente em casos excepcionais.

#### **Padrão**

Se essa opção for ativada, o componente Backup registrará informações importantes (detecções de vírus, alertas e erros ao salvar) no arquivo de relatório, e as informações menos importantes serão ignoradas para facilitar a compreensão. Essa opção é ativada como configuração padrão.

#### **Avançado**

Se essa opção for ativada, o componente Backup incluirá informações menos importantes no arquivo de relatório.

#### **Concluído**

Se essa opção for ativada, o componente Backup incluirá todas as informações sobre o processo de backup e a verificação de vírus no arquivo de relatório.

## 13.8 Atualizar

Na seção *Atualizar*, é possível configurar o recebimento automático de atualizações. Você pode especificar vários intervalos de atualização e ativar ou desativar a atualização automática.

### **Atualização automática**

#### **Ativar**

Se essa opção for ativada, as atualizações automáticas serão executadas para os eventos ativados no intervalo especificado.

#### **Atualização automática a cada n dias/horas/minutos**

Nesta caixa, é possível especificar o intervalo em que a atualização automática é realizada. Para alterar o intervalo de atualização, realce uma das opções de tempo na caixa e altere-a usando a tecla de seta à direita da caixa de entrada.

#### **Iniciar trabalho ao conectar-se à Internet (discada)**

Se essa opção for ativada, além do intervalo de atualização especificado, o trabalho de atualização é realizado sempre que uma conexão com a Internet é estabelecida.

#### **Repetir trabalho se o tempo já tiver expirado**

Se essa opção for ativada, os trabalhos de atualização antigos que não foram realizados, por exemplo, porque o computador foi desligado serão realizados.

## 13.8.1 Iniciar atualização do produto

Em **Atualização do produto**, configure como as atualizações do produto ou a notificação das atualizações devem ser tratadas.

### **Atualizações de produto**

#### **Baixar e instalar as atualizações do produto automaticamente**

Se essa opção for ativada, as atualizações do produto serão baixadas e instaladas automaticamente pelo componente Atualizador assim que forem disponibilizada. As atualizações do arquivo de definição de vírus e do mecanismo de verificação são realizadas independentemente dessa configuração. As condições para essa opção são: configuração completa da atualização e uma conexão aberta com um servidor de download.

#### **Baixar atualizações do produto. Se for necessário reiniciar, instalar a atualização após o reinício do sistema; caso contrário, instalar imediatamente.**

Se essa opção for ativada, as atualizações do produto serão baixadas assim que forem disponibilizadas. Se não for necessário reiniciar, a atualização será instalada automaticamente após o arquivo de atualização ser baixado. Se uma atualização do produto exigir a reinicialização do computador, ela será executada na próxima reinicialização do sistema controlada pelo usuário e não imediatamente depois do download do arquivo de atualização. Desse modo, a reinicialização não é realizada enquanto os usuários estão trabalhando nos computadores, o que é uma vantagem. As atualizações do arquivo de definição de vírus e do mecanismo de verificação são realizadas independentemente dessa configuração. As condições para essa opção são: configuração completa da atualização e uma conexão aberta com um servidor de download.

#### **Notificação quando houver novas atualizações do produto disponíveis**

Se essa opção for ativada, você receberá uma notificação por e-mail quando novas atualizações do produto forem disponibilizadas. As atualizações do arquivo de definição de vírus e do mecanismo de verificação são realizadas independentemente dessa configuração. As condições para essa opção são: configuração completa da atualização e uma conexão aberta com um servidor de download. Você receberá notificações através de uma janela pop-up da área de trabalho e através de um alerta do Atualizador no Centro de controle em Visão geral::Eventos.

#### **Notificar mais uma vez após n dia(s)**

Se a atualização do produto não tiver sido instalada após a notificação inicial, insira nesta caixa o número de dias que devem passar para você receber uma notificação novamente sobre a disponibilidade de atualizações do produto.

#### **Não fazer o download de atualizações de produto**

Se essa opção for ativada, nenhuma atualização do produto automática ou notificação das atualizações disponíveis do Atualizador será executada. As atualizações do arquivo de definição de vírus e do mecanismo de pesquisa são realizadas independentemente dessa configuração.

### **Importante**

Uma atualização do arquivo de definição de vírus e do mecanismo de pesquisa é realizada durante cada processo de atualização, independentemente das configurações da atualização do produto (consulte o Capítulo Atualizações).

### Observação

Se tiver ativado uma opção de atualização automática do produto, você poderá configurar outras opções de cancelamento e reinicialização de notificações em Reiniciar configurações.

## 13.8.2 Reiniciar configurações

Quando uma atualização do produto é realizada pelo programa AntiVir, talvez seja necessário reiniciar o sistema do computador. Se tiver selecionado atualizações automáticas do produto em Geral::Atualizar::Atualização do produto, você poderá escolher entre as diferentes opções de cancelamento e notificação de reinicialização em **Reiniciar configurações**.

### Nota

As configurações de reinicialização permitem escolher entre duas opções para executar uma atualização do produto que requer a reinicialização do computador na configuração em Geral::Atualizar::Atualização do produto.

Execução automática da atualização do produto com a reinicialização obrigatória do computador quando a atualização está disponível: A atualização e a reinicialização são realizadas enquanto os usuários estão trabalhando nos computadores. Se você tiver ativado essa opção, talvez seja útil selecionar rotinas de reinicialização com uma opção de cancelamento ou função de lembrete.

Execução da atualização do produto quando uma reinicialização do computador é obrigatória após a próxima reinicialização do sistema: a atualização e a reinicialização são realizadas depois que os usuários ligam os computadores e fazem login. As rotinas de reinicialização automática são recomendadas para essa opção.

### Reiniciar configurações

#### Reiniciar o computador após n segundos

Se essa opção for ativada, a reinicialização que é necessária será realizada **automaticamente** depois que uma atualização do produto for executada no intervalo especificado. Uma contagem regressiva aparece sem nenhuma opção para cancelar a reinicialização do computador.

#### Mensagem de lembrete para reiniciar a cada n segundos

Se essa opção for ativada, a reinicialização que é necessária **não** será realizada automaticamente depois que uma atualização do produto for executada. No intervalo especificado, você receberá notificações de reinicialização sem opções de cancelamento. Essas notificações permitem que você confirme a reinicialização do computador ou selecione a opção "**Lembrar-me novamente**".

#### Consultar se o computador deve ser reiniciado

Se essa opção for ativada, a reinicialização que é necessária **não** será realizada automaticamente depois que uma atualização do produto for executada. Você receberá apenas uma mensagem, que oferecerá a opção para realizar uma reinicialização diretamente ou cancelar a rotina de reinicialização.

#### Reiniciar o computador sem consulta

Se essa opção for ativada, a reinicialização que é necessária será realizada **automaticamente** depois que uma atualização do produto for executada. Você não receberá nenhuma notificação.

A atualização pode ser realizada diretamente através de um servidor da Web na Internet.

### **Conexão do servidor da Web**

#### **Usar conexão já existente (rede)**

Essa configuração é exibida quando sua conexão é usada por meio de uma rede.

#### **Usar a seguinte conexão:**

Essa configuração é exibida quando sua conexão é definida individualmente.

O Atualizador detecta automaticamente as opções de conexão que estão disponíveis. As opções de conexão que não estão disponíveis aparecem desativadas e não podem ser ativadas. Uma conexão discada pode ser estabelecida manualmente, por exemplo, através de uma entrada do catálogo de telefones do Windows.

- **Usuário:** Insira o nome de usuário da conta selecionada.
- **Senha:** Insira a senha dessa conta. Por motivos de segurança, os caracteres reais digitados neste espaço são substituídos por asteriscos (\*).

#### **Nota**

Caso tenha esquecido o nome de usuário ou a senha de uma conta da Internet existente, entre em contato com seu provedor de serviços de Internet.

#### **Nota**

A discagem automática do atualizador através das chamadas ferramentas de discagem (por exemplo, SmartSurfer, Oleco etc.) ainda não está disponível no momento.

#### **Encerrar uma conexão discada que foi configurada para a atualização**

Se essa opção for ativada, a conexão RDT estabelecida para a atualização será interrompida automaticamente mais uma vez assim que o download tiver sido concluído.

#### **Nota**

Essa opção não está disponível no Windows Vista. No Windows Vista, a conexão discada aberta para a atualização sempre é encerrada assim que o download é executado.

## 13.9 Geral

### 13.9.1 Categorias de ameaça

#### **Seleção de categorias de ameaça**

Seu produto AntiVir protege seu computador contra vírus.

Além disso, você pode fazer a verificação de acordo com as seguintes categorias de ameaça estendidas.

- Clientes back-door (BDC)
- Discador (DIALER)

- Jogos (GAMES)
- Piadas (JOKES)
- Risco de privacidade de segurança (SPR)
- Adware/Spyware (ADSPY)
- Compactadores de tempo de execução incomuns (PCK)
- Arquivos com extensão dupla (HEUR-DBLEXT)
- Phishing
- Aplicativo (APPL)

Quando você clica na caixa relevante, o tipo selecionado é ativado (marca de verificação definida) ou desativado (sem marca de verificação).

**Selecionar tudo**

Se essa opção for ativada, todos os tipos serão ativados.

**Valores padrão**

Esse botão restaura os valores padrão predefinidos.

**Nota**

Se um tipo for desativado, os arquivos reconhecidos como sendo arquivos do tipo de programa relevante não serão mais indicados. Nenhuma entrada é criada no arquivo de relatório.

## 13.9.2 Senha

Você pode proteger o programa AntiVir em diferentes áreas com uma senha. Se uma senha for criada, você terá que inseri-la sempre que desejar abrir a área protegida.

**Senha**

**Digitar senha**

Insira a senha solicitada aqui. Por motivos de segurança, os caracteres reais digitados neste espaço são substituídos por asteriscos (\*). A senha pode ter no máximo 20 caracteres. Depois que a senha é criada, o programa negará o acesso se uma senha incorreta for inserida. Uma caixa vazia significa "Sem senha".

**Confirmar senha**

Confirme a senha inserida acima inserindo-a aqui novamente. Por motivos de segurança, os caracteres reais digitados neste espaço são substituídos por asteriscos (\*).

**Nota**

A senha diferencia maiúsculas de minúsculas.

### Áreas protegidas por senha

Seu programa AntiVir pode proteger áreas individuais com uma senha. Ao clicar na caixa relevante, a solicitação da senha poderá ser desativada ou reativada para áreas individuais conforme necessário.

Área protegida por senha	Função
Centro de controle	Se essa opção for ativada, a senha predefinida



		será necessária para iniciar o Centro de controle.
	Ativar/desativar o Guard	Se essa opção for ativada, a senha predefinida será necessária para ativar ou desativar o AntiVir Guard.
	Ativar/desativar o MailGuard	Se essa opção for ativada, a senha predefinida será necessária para ativar/desativar o MailGuard.
	Ativar/desativar o FireWall	Se essa opção for ativada, a senha predefinida será necessária para ativar/desativar o FireWall.
	Ativar/desativar o WebGuard	Se essa opção for ativada, a senha predefinida será necessária para ativar/desativar o WebGuard.
	Ativar/desativar o controle dos pais	Se essa opção for ativada, a senha predefinida será necessária para ativar/desativar o controle dos pais.
<b>Quarentena</b>		Se essa opção for ativada, todas as áreas do gerenciador de quarentena protegidas por senha serão ativadas. Ao clicar na caixa relevante, a solicitação da senha poderá ser desativada ou reativada para áreas individuais.
	Restaurar objetos afetados	Se essa opção for ativada, a senha predefinida será necessária para restaurar um objeto.
	Nova verificação dos objetos afetados	Se essa opção for ativada, a senha predefinida será necessária para verificar novamente um objeto.
	Propriedades do objeto afetado	Se essa opção for ativada, a senha predefinida será necessária para exibir as propriedades de um objeto.
	Excluir objetos afetados	Se essa opção for ativada, a senha predefinida será necessária para excluir um objeto.
	Enviar email para a Avira	Se essa opção for ativada, a senha predefinida será necessária para enviar um objeto para o Centro de pesquisa de malware da Avira para análise.
	Copiando objetos afetados	Se essa opção for ativada, a senha predefinida será necessária para copiar o objeto afetado.
	Adicionar e modificar tarefas	Se essa opção for ativada, a senha predefinida será necessária ao adicionar e modificar trabalhos no Programador.
	Iniciar atualizações do produto	Se essa opção for ativada, a senha predefinida será necessária para iniciar as atualizações do produto no menu Atualização.
<b>Configuração</b>		Se essa opção for ativada, a configuração do programa só poderá ser feita depois que a

	senha predefinida for inserida.
Ativar modo de especialista	Se essa opção for ativada, a senha predefinida será necessária para ativar o modo de especialista.
<b>Instalação/Desinstalação</b>	Se essa opção for ativada, a senha predefinida será necessária para a instalação ou desinstalação do programa.

### 13.9.3 Segurança

#### Atualizar

##### **Alerta se a última atualização for mais antiga que n dia(s)**

Nessa caixa, você pode inserir o número máximo de dias que podem transcorrer desde a última atualização. Se esse número de dias tiver passado, um ícone vermelho será exibido para o status de atualização em Status no Centro de controle.

##### **Mostrar aviso se o arquivo de definição de vírus estiver desatualizado**

Se essa opção for ativada, um alerta será exibido se o arquivo de definição de vírus estiver desatualizado. Com a ajuda da opção de alerta, você pode configurar o intervalo de tempo para um alerta caso a última atualização tenha mais de n dia(s).

#### Proteção do produto

##### **Observação**

As opções de proteção do produto não estarão disponíveis se o Guard não tiver sido instalado usando a opção de instalação definida pelo usuário.

##### **Proteger os processos de um encerramento indesejado**

Se essa opção for ativada, todos os processos do programa serão protegidos contra o encerramento indesejado acionado por vírus e malwares ou contra o encerramento “não controlado” acionado pelo usuário, por exemplo, através do Gerenciador de tarefas. Essa opção é ativada como configuração padrão.

##### **Proteção de processo avançada**

Se essa opção for ativada, todos os processos do programa serão protegidos com opções avançadas em relação ao encerramento indesejado. A proteção de processo avançada consome uma quantidade significativamente maior de recursos do computador do que a proteção simples com senha. A opção é ativada como configuração padrão. Para desativar essa opção, é necessário reiniciar o computador.

##### **Importante**

A proteção por senha não está disponível para o Windows XP de 64 bits !

##### **Aviso**

Se a proteção dos processos for ativada, poderão ocorrer problemas de interação com outros softwares. Nesses casos, desative a proteção dos processos.

##### **Proteger os arquivos e as entradas do registro contra manipulação**

Se essa opção for ativada, todas as entradas do registro do programa e todos os arquivos de programa (arquivos binários e de configuração) serão protegidos contra manipulação. A proteção contra manipulação impede o acesso de gravação, exclusão e, em alguns casos, leitura às entradas do registro ou aos arquivos de programa de usuários ou programas externos. Para ativar essa opção, é necessário reiniciar o computador.

### **Aviso**

Se essa opção estiver desativada,

### **Observação**

Quando essa opção está ativada, as alterações podem ser feitas apenas na configuração, incluindo alterações nas solicitações de verificação ou atualização por meio da interface de usuário.

### **Importante**

A proteção de arquivos e entradas de registro não está disponível para o Windows XP de 64 bits .

## 13.9.4 WMI

### **Suporte para Instrumentação de gerenciamento do Windows**

A Instrumentação de gerenciamento do Windows é uma técnica de administração básica do Windows que usa linguagens de script e programação para permitir o acesso de leitura e gravação, local e remoto, às configurações dos sistemas Windows. O programa AntiVir oferece suporte para WMI e fornece dados (informações de status, dados estatísticos, relatórios, solicitações planejadas etc.), bem como eventos em uma interface. O WMI fornece a você a condição de baixar dados operacionais do programa

#### **Ativar suporte para WMI**

Quando essa opção está ativada, é possível baixar dados operacionais do programa via WMI.

## 13.9.5 Proxy

### **Servidor proxy**

#### **Não use um servidor proxy**

Se essa opção for ativada, sua conexão com o servidor da Web não será estabelecido por meio de um servidor proxy.

#### **Usar configurações do sistema Windows**

Quando a opção está ativada as configurações atuais do sistema Windows são usadas para a conexão com o servidor da Web através de um servidor proxy. Defina as configurações do sistema Windows para usar um servidor proxy em **Painel de controle::Opções da Internet::Conexões::Configurações da LAN**. Você também pode acessar as opções da Internet no menu Extras no Internet Explorer.

**Aviso**

Se você estiver usando um servidor proxy que requer autenticação, insira todos os dados necessários na opção *Usar este servidor proxy*. A opção *Usar configurações do sistema Windows* poderá ser usada somente para servidores proxy sem autenticação.

**Use este servidor proxy**

Se sua conexão com o servidor da Web for configurada através de um servidor proxy, você poderá inserir as informações relevantes aqui.

**Endereço**

Insira o nome do computador ou o endereço IP do servidor proxy que deseja usar para estabelecer conexão com o servidor da Web.

**Porta**

Insira o número da porta do servidor proxy que deseja usar para estabelecer conexão com o servidor da Web.

**Nome de login**

Insira seu nome de usuário para fazer login no servidor.

**Senha de login**

Insira a senha relevante para fazer login no servidor proxy aqui. Por motivos de segurança, os caracteres reais digitados neste espaço são substituídos por asteriscos (\*).

*Exemplos:*

Endereço:	proxy.domain.com	Porta:	8080
Endereço:	192.168.1.100	Porta:	3128

## 13.9.6 Diretórios

**Caminho temporário**

Nesta caixa de entrada, insira o caminho onde o programa armazenará seus arquivos temporários.

**Usar configurações padrão do sistema**

Se essa opção for ativada, as configurações do sistema serão usadas para manipular arquivos temporários.

**Nota**

Você pode ver onde o sistema (por exemplo, o Windows XP) salva os arquivos temporários em: Iniciar/Configurações/Painel de controle/Sistema/Indexar placa "Avançado"/Botão "Variáveis de ambiente". As variáveis temporárias (TEMP, TMP) do usuário registrado atualmente e as variáveis de sistema (TEMP, TMP) são exibidas aqui com os valores relevantes.

**Usar o seguinte diretório**

Se essa opção for ativada, o caminho exibido na caixa de entrada será usado.



O botão abre uma janela na qual é possível selecionar o caminho temporário desejado.

**Padrão**

O botão restaura o diretório predefinido para o caminho temporário.

## 13.9.7 Eventos

### **Limitar tamanho do banco de dados de eventos**

#### **Limitar número máximo de eventos a n entradas**

Se essa opção for ativada, o número máximo de eventos listados no banco de dados de eventos poderá ser limitado a um determinado tamanho; os possíveis valores são: de 100 a 10.000 entradas. Se o número de entradas inseridas for ultrapassado, as entradas mais antigas serão excluídas.

#### **Excluir eventos mais antigos que n dia(s)**

Se essa opção for ativada, os eventos listados no banco de dados de eventos serão excluídos depois de um determinado período; os valores possíveis são: de 1 a 90 dias. Essa opção é ativada como configuração padrão, com um valor de 30 dias.

#### **Não limitar o tamanho do banco de dados de eventos (excluir eventos manualmente)**

Quando essa opção é ativada, o tamanho do banco de dados de eventos não é limitado. No entanto, são exibidas no máximo 20.000 entradas na interface do programa em Eventos.

## 13.9.8 Limitar relatórios

Limitar número de relatórios

#### **Limitar o número a n unidades**

Quando essa opção é ativada, o número máximo de relatórios pode ser limitado a um valor específico. São permitidos os valores entre 1 e 300. Se o número especificado for ultrapassado, o relatório mais antigo no momento será excluído.

#### **Excluir todos os relatórios com mais de n dia(s)**

Se essa opção for ativada, os relatórios serão excluídos automaticamente depois de um número de dias específico. Os valores permitidos são: de 1 a 90 dias. Essa opção é ativada como configuração padrão, com um valor de 30 dias.

#### **Não limitar o número de relatórios (excluir relatórios manualmente)**

Se essa opção for ativada, o número de relatórios não será restrito.

## 13.9.9 Alertas acústicos

### **Alerta acústico**

Quando um vírus ou malware é detectado pelo Scanner ou Guard, um alerta acústico é emitido no modo de ação interativa. Agora você pode desativar ou ativar o alerta acústico e selecionar um arquivo wave alternativo como o alerta.

#### **Observação**

O modo de ação do Scanner é definido na configuração em Scanner::Fazer varredura::Ação para detecção. O modo de ação do Guard é definido na configuração em Guard::Fazer varredura::Ação para detecção.

#### **Nenhum aviso**

Quando essa opção for ativada, nenhum alerta acústico será emitido quando um vírus for detectado pelo Scanner ou pelo Guard.

**Usar os alto-falantes do PC (apenas no modo interativo)**

Se essa opção for ativada, um alerta acústico com o sinal padrão será emitido quando um vírus for detectado pelo Scanner ou pelo Guard. O alerta acústico é emitido no alto-falante interno do computador.

**Usar o arquivo WAVE a seguir (apenas no modo interativo)**

Se essa opção for ativada, um alerta acústico com o arquivo Wave selecionado será emitido quando um vírus for detectado pelo Scanner ou pelo Guard. O arquivo Wave selecionado é reproduzido em um alto-falante externo conectado.

**Arquivo wave**

Nessa caixa de entrada, é possível inserir o nome e o caminho associado ao arquivo de áudio escolhido. O sinal acústico padrão do programa é inserido como padrão.



O botão abre uma janela na qual é possível selecionar o arquivo desejado com a ajuda do explorador de arquivos.

**Testar**

Esse botão é usado para testar o arquivo wave selecionado.

## 13.9.10 Avisos

O programa AntiVir gera as chamadas telas deslizantes, notificações de área de trabalho para eventos específicos, que fornecem informações sobre sequências do programa bem-sucedidas ou não, como as atualizações. Em *Avisos*, é possível ativar ou desativar as notificações para eventos específicos.

Com as notificações de área de trabalho, você pode desativar a notificação diretamente na tela deslizante. Você pode reativar a notificação em *Avisos*.

### **Avisos**

**sobre as conexões discadas usadas**

Se essa opção for ativada, será emitido um alerta de notificação de área de trabalho se um discador criar uma conexão discada no seu computador através da rede telefônica ou ISDN. Pode existir o risco de a conexão ter sido criada por um discador desconhecido e indesejado e de a conexão ser cobrada. (consulte Vírus e mais::Categorias de ameaça: Discador).

**sobre os arquivos atualizados com êxito**

Se essa opção for ativada, você receberá uma notificação de área de trabalho sempre que uma atualização for realizada e os arquivos forem atualizados.

**sobre falha na atualização**

Se essa opção for ativada, você receberá uma notificação de área de trabalho sempre que uma atualização falhar: nenhuma conexão com o servidor de download pode ser criada ou os arquivos de atualização não podem ser instalados.

**que nenhuma atualização é necessária**

Se essa opção for ativada, você receberá uma notificação de área de trabalho sempre que uma atualização for iniciada, mas a instalação dos arquivos não for necessária porque seu programa está atualizado.



Este manual foi elaborado com extremo cuidado. Mesmo assim, é impossível garantir que não haja erros em forma e conteúdo. É proibida a reprodução desta publicação ou de partes dela em qualquer meio ou forma sem autorização prévia por escrito da Avira Operations GmbH & Co. KG.

Edição Q3-2011

Nomes de marcas e produtos são marcas comerciais ou marcas registradas de seus respectivos proprietários. Marcas comerciais protegidas não são identificadas como tal neste manual. Mas isso não significa que elas possam ser utilizadas livremente.



live free.™