

Avira Professional Security

Manual do usuário

Marcas comerciais e direitos autorais

Marcas comerciais

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

O código concedido por fornecedores terceiros foi usado para o Avira Professional Security. Agradecemos os detentores dos direitos autorais por disponibilizar o código para nós.

Para obter informações detalhadas sobre direitos autorais, consulte "Licenças de terceiros" na ajuda do Programa Avira Professional Security.

Sumário:

1. Introdução	8
1.1 Ícones e ênfases.....	8
2. Informações do produto	10
2.1 Escopo da entrega	10
2.2 Requisitos do sistema	11
2.3 Licença e atualização	12
2.3.1 Gerenciador de licença	12
3. Instalação e desinstalação	14
3.1 Visão geral	14
3.1.1 Tipos de instalação.....	14
3.2 Pré-instalação	15
3.3 Instalação expressa	16
3.4 Instalação personalizada	18
3.5 Assistente de configuração	20
3.6 Alterar instalação	22
3.7 Módulos de instalação.....	22
3.8 Desinstalação.....	23
3.9 Instalação e desinstalação na rede.....	24
3.9.1 Parâmetros de linha de comando para o programa de instalação.....	25
4. Visão geral do Avira Professional Security	30
4.1 Interface de usuário e operação	30
4.1.1 Centro de controle	30
4.1.2 Iniciando e fechando o Centro de controle	31
4.1.3 Operar o Centro de controle	32
4.1.4 Visão geral do Centro de controle	32
4.1.5 Configuração	33
4.1.6 Acessando a Configuração.....	34
4.1.7 Operação de configuração.....	35
4.1.8 Perfis de configuração.....	36
4.1.9 Ícone de bandeja.....	38

4.1.10	Entradas do menu de contexto.....	38
4.2	Como...?	39
4.2.1	Ativar licença	39
4.2.2	Executar atualização automática	40
4.2.3	Iniciar uma atualização manual	41
4.2.4	uso de um perfil de verificação para verificar a presença de vírus e malwares.....	42
4.2.5	Verificar presença de vírus e malwares com o método de arrastar e soltar	44
4.2.6	Verificar presença de vírus e malwares através do menu de contexto	44
4.2.7	Verificar presença de vírus e malwares automaticamente	44
4.2.8	Verificação direcionada de rootkits e malware ativo	46
4.2.9	Reação aos vírus e malwares detectados	46
4.2.10	Manipulação de arquivos em quarentena (*.qua)	52
4.2.11	Restaurar os arquivos em quarentena.....	54
4.2.12	Mover arquivos suspeitos para quarentena.....	56
4.2.13	Perfil da verificação: Corrigir ou excluir tipo de arquivo em um perfil de verificação	56
4.2.14	Criar atalho na área de trabalho para o perfil de verificação	57
4.2.15	Filtrar eventos.....	57
4.2.16	Excluir endereços de email da verificação.....	58
4.2.17	Selecionar o nível de segurança para o FireWall	58
5.	System Scanner	60
6.	Atualizações	61
7.	Firewall.....	63
8.	Perguntas frequentes, dicas.....	64
8.1	Ajuda no caso de um problema	64
8.2	Atalhos	69
8.2.1	Nas caixas de diálogo.....	69
8.2.2	Na ajuda.....	70
8.2.3	No Centro de controle.....	71
8.3	Central de segurança do Windows	73
8.3.1	Geral.....	73
8.3.2	A Central de segurança do Windows e o produto Avira	74

9. Vírus e mais	81
9.1 Categorias de ameaça	81
9.2 Vírus e outros malwares	84
10. Informações e serviço	89
10.1 Endereço de contato.....	89
10.2 Suporte técnico	89
10.3 Arquivo suspeito	90
10.4 Registrando falso-positivos	90
10.5 Seus comentários para mais segurança.....	90
11. Referência: opções de configuração	91
11.1 System Scanner	91
11.1.1 Fazer verificação.....	91
11.1.2 Relatório.....	103
11.2 Realtime Protection.....	104
11.2.1 Fazer verificação	104
11.2.2 ProActiv.....	117
11.2.3 Relatório.....	120
11.3 Variáveis: Exceções da Realtime Protection e do System Scanner.....	121
11.4 Atualizar	122
11.4.1 Atualização do produto.....	124
11.4.2 Reiniciar configurações.....	125
11.4.3 Servidor de arquivos	126
11.4.4 Servidor da Web.....	127
11.5 Firewall.....	130
11.5.1 Regras do adaptador	130
11.5.2 Regras de aplicativo.....	142
11.5.3 Fornecedores confiáveis.....	145
11.5.4 Configurações	146
11.5.5 Configurações de pop-up	147
11.6 Firewall no SMC.....	149
11.6.1 Configurações gerais	149
11.6.2 Regras de entrada	154
11.6.3 Lista de aplicativos	163
11.6.4 Fornecedores confiáveis.....	164
11.6.5 Outras configurações	165

11.6.6	Configurações de exibição.....	166
11.7	Proteção para a web.....	168
11.7.1	Fazer verificação.....	168
11.7.2	Relatório.....	177
11.8	Proteção de e-mail.....	178
11.8.1	Fazer verificação.....	178
11.8.2	Geral.....	183
11.8.3	Relatório.....	186
11.9	Geral.....	187
11.9.1	Categorias de ameaça.....	187
11.9.2	Senha.....	188
11.9.3	Segurança.....	191
11.9.4	WMI.....	193
11.9.5	Configurações de proxy.....	193
11.9.6	Alertas.....	194
11.9.7	Eventos.....	207
11.9.8	Relatórios.....	207
11.9.9	Diretórios.....	208

1. Introdução

O produto Avira 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.com/pt-br>

No site da Avira, você pode:

- acessar informações sobre outros programas de desktop da Avira
- fazer download dos programas de desktop da Avira mais recentes
- fazer download dos manuais de produto mais recentes no formato PDF
- fazer download das 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

1.1 Ícones e ênfases

Os seguintes ícones são usados:

Ícone/designação	Explicação
✓	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.
Aviso	Colocado antes de um aviso quando há a possibilidade de perigo de perda de dados críticos.

Observação	Colocado antes de um link para informações especialmente importantes ou uma dica que facilita o uso do produto Avira.
-------------------	---

As seguintes ênfases são usadas:

Ênfase	Explicação
<i>Itálico</i>	Dados do nome de arquivo ou do caminho.
	Elementos exibidos da interface do software (por exemplo, seção da janela ou mensagem de erro).
Negrito	Elementos clicáveis na interface do software (por exemplo, item de menu, área de navegação, caixa de opção ou botão)

2. Informações do produto

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

- consulte o Capítulo: [Escopo da entrega](#)
- consulte o Capítulo: [Requisitos do sistema](#)
- consulte o Capítulo: [Licença e atualização](#)
- consulte o Capítulo: [Gerenciador de licença do Avira](#)

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

- ▶ Observe estas informações:

Observação

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.

Observação

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

2.1 Escopo da entrega

O produto Avira 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
- System 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.
- Realtime Protection (verificação durante 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)
- Scanner do Mail Protection (POP3, IMAP Scanner e SMTP Scanner) para a verificação constante de emails em busca de vírus e malware. Os anexos de email também são verificados
- Web Protection com monitoramento de dados e arquivos transferidos da Internet usando o protocolo HTTP (monitoramento das portas 80, 8080, 3128)
- 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 ou de uma intranet
- 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.

2.2 Requisitos do sistema

Os requisitos do sistema são os seguintes:

- Computador Pentium ou superior, com pelo menos 1 GHz
- Sistema operacional
 - Windows XP, SP2 (32 ou 64 bits) ou
 - Windows Vista (32 ou 64 bits, SP1) ou
 - 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 512 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](#))

2.3 Licença e atualização

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

A licença é emitida através de um código de licença digital na forma do arquivo *hbedv.key*. Esse código de licença digital é a chave de sua licença pessoal. Ele contém detalhes exatos sobre os programas que foram licenciados para você e por quanto tempo. Obviamente, um código de licença digital também pode conter a licença de mais de um produto.

Se tiver adquirido o produto Avira na Internet ou por meio do CD/DVD do programa, o código de licença digital será enviado a você por email. É possível carregar a chave de licença durante a instalação do programa ou instalá-lo posteriormente no Gerenciador de licença.

Observação

Se seu produto Avira for gerenciado sob AMC, seu administrador executará a atualização. Você deve salvar os dados e reiniciar o computador; do contrário, seu sistema não estará seguro.

2.3.1 Gerenciador de licença

O Gerenciador de licenças do Avira Professional Security oferece uma maneira muito simples para instalar a licença do Avira Professional Security.

Gerenciador de licenças do Avira Professional Security



Você pode instalar a licença selecionando o arquivo de licença no gerenciador de arquivos ou clicando duas vezes no email de ativação e seguindo as instruções relevantes na tela.

Observação

O Gerenciador de licenças do Avira Professional Security copia automaticamente a licença correspondente na pasta relevante do produto. Se uma licença já existir, será exibida uma nota perguntando se o arquivo de licença existente deve ser substituído. Nesse caso, o arquivo existente é substituído pelo novo arquivo de licença.

3. Instalação e desinstalação

3.1 Visão geral

Este capítulo contém informações relacionadas à instalação e desinstalação do produto Avira.

- consulte o Capítulo: [Pré-instalação](#): Requisitos, preparação do computador para instalação
- consulte o Capítulo: [Instalação expressa](#): Instalação padrão de acordo com as configurações padrão
- consulte o Capítulo: [Instalação personalizada](#): Instalação configurável
- consulte o Capítulo: [Assistente de configuração](#)
- consulte o Capítulo: [Alterar instalação](#)
- consulte o Capítulo: [Módulos de instalação](#)
- consulte o Capítulo: [Desinstalação](#): Desinstalar
- consulte o Capítulo: [Instalação e desinstalação na rede](#)

3.1.1 Tipos de instalação

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

Expresso

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

Personalizar

- 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 produto Avira e inicia uma verificação rápida do sistema que é executada automaticamente após a instalação.

3.2 Pré-instalação

Observação

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 produto Avira.

Observação

Ao instalar em um sistema operacional de servidor, a Realtime Protection e a proteção de arquivos não estará disponível.

Pré-instalação

- ✓ Feche seu programa de email. 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.
 - O produto Avira pesquisará uma possível incompatibilidade de software em seu computador.
 - Se um software possivelmente incompatível for detectado, o Avira gerará uma lista desses programas.
 - Recomenda-se remover esses softwares a fim de não colocar em risco a estabilidade de seu computador.
- ▶ Marque a caixa de seleção dos programas que devem ser removidos automaticamente de seu computador e clique em **Avançar**.
- ▶ É necessário confirmar manualmente a desinstalação de alguns programas. Selecione os programas e clique em **Avançar**.
 - A desinstalação de um ou mais programas selecionados exige a reinicialização do computador. Após a reinicialização, a instalação continuará.

Aviso

Seu computador não estará protegido até a conclusão da instalação do produto Avira.

Observação

Se o produto Avira em seu computador for administrado pelo AMC (Avira Management Console) você não receberá uma solicitação para remoção de softwares incompatíveis.

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.
- ▶ 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)
 - Quando apropriado, realize uma atualização do após o término da instalação
 - ▶ Salve o arquivo de licença *hbedv.key* no sistema do computador se desejar ativar o produto Avira.

Observação

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. Esse processo garante a instalação de seu produto Avira 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 produto Avira está disponível para a instalação feita com um pacote. Recomendamos que você realize uma atualização do arquivo de definição de vírus após a instalação.

3.3 Instalação expressa

Instalar seu produto Avira:

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 tela **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 seu produto Avira 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. A janela **Download** fecha quando o download termina.

Instalação com um pacote de instalação

- A janela **Preparar a instalação** é exibida.
- O arquivo de instalação é extraído. A rotina de instalação é iniciada.
- A caixa de diálogo **Selecionar tipo de instalação** é exibida.

Observação

Por padrão, a instalação Expressa é predefinida. Todos os componentes padrão serão instalados e não será possível configurá-los. Se você quiser executar uma instalação personalizada, consulte o capítulo: [Instalação > Instalação personalizada](#).

- ▶ Você pode participar na *Comunidade do Avira ProActiv* ([Configuração > Realtime Scanner > ProActiv](#)).
- ▶ Confirme que você aceita o **Contrato de Licença de Usuário Final**. Para ler o texto detalhado do **Contrato de Licença de Usuário Final**, clique no link **EULA**.
- ▶ Clique em **Avançar**.
- ▶ Se você optou por participar da Comunidade Avira ProActiv, a janela de informações da **Comunidade do Avira ProActiv** será exibida. Você pode obter mais detalhes sobre a verificação on-line expandida.
- ▶ Clique em **Avançar**.
 - O **Assistente de licença** é aberto e ajuda você a ativar seu produto.
 - Aqui, você tem a oportunidade de configurar um servidor Proxy.
- ▶ Clique em **Configurações proxy** para realizar as configurações e confirmá-las com **OK**.
 - Se você já tiver recebido uma chave de ativação, selecione **Ativar produto**. Como alternativa, clique em **Já tenho um arquivo de licença HBEDV.KEY** válido.
 - A caixa de diálogo **Abrir arquivo**.
- ▶ Selecione seu *HBEDV.KEY* e clique em **Abrir**.

- O código de ativação é copiado para o Assistente de licença.
- ▶ Clique em **Avançar**.
 - O progresso da instalação é exibido por uma barra verde.
- ▶ Clique em **Concluir** para encerrar o processo de instalação e fechar o **Assistente de licença**.
 - O Ícone de bandeja do Avira é colocado na barra de tarefas.
 - Para garantir a proteção efetiva para seu computador, o módulo **Atualizador** pesquisará por possíveis atualizações.
 - A janela **Luke Filewalker** será aberta e uma pequena verificação do sistema será realizada. O status da verificação e os resultados serão exibidos.
- ▶ Se após a verificação você receber uma solicitação de reinicialização de seu computador, clique em **Sim** para garantir que seu sistema esteja totalmente protegido.

Após a instalação, recomendamos que você verifique se o programa está atualizado no campo **Status** do Centro de controle.

- ▶ Se seu produto Avira mostrar que seu computador não está protegido, clique em **Corrigir problema**.
 - A caixa de diálogo **Restaurar a proteção** é aberta.
- ▶ Ative as opções predefinidas a fim de maximizar a segurança de seu sistema.
- ▶ Se for apropriado, realize em seguida uma verificação completa do sistema.

3.4 Instalação personalizada

Instalar seu produto Avira:

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 tela **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 seu produto Avira 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. A janela **Download** fecha quando o download termina.

Instalação com um pacote de instalação

- A janela **Preparar a instalação** é exibida.
- O arquivo de instalação é extraído. A rotina de instalação é iniciada.
- A caixa de diálogo **Selecionar tipo de instalação** é exibida.

Observação

Por padrão, a instalação Expressa é predefinida. Todos os componentes padrão serão instalados e não será possível configurá-los. Se você quiser executar uma instalação Expressa, consulte o capítulo: [Instalação > Instalação expressa](#).

- ▶ Escolha **Personalizar** para instalar os componentes individuais do programa.
- ▶ Confirme que você aceita o **Contrato de Licença de Usuário Final**. Para ler o texto detalhado do **Contrato de Licença de Usuário Final**, clique no link **EULA**.
- ▶ Clique em **Avançar**.
 - A janela **Escolher pasta de destino** é exibida.
 - A pasta padrão será *C:\Arquivos de programas\Avira\AntiVir Desktop*.
- ▶ Clique em **Avançar** para continuar.

-OU-

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

 - A caixa de diálogo **Instalar componentes** é exibida:
- ▶ Marque ou desmarque os componentes da lista e confirme com **Avançar** para prosseguir.
 - Se você optou por instalar o componente ProActiv, a janela da **comunidade do Avira ProActiv** será exibida.

Você pode confirmar a participação na comunidade do Avira ProActiv: Se essa opção estiver ativada, o Avira 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.
- ▶ Se a caixa de diálogo **Comunidade do Avira ProActiv** tiver sido exibida, ative ou desative a participação na comunidade do Avira 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**.

- Os recursos do programa serão instalados. O progresso da instalação é exibido na caixa de diálogo.
- A caixa de diálogo **Instalar licença** é exibida:
- ▶ Vá ao diretório no qual salvou o arquivo de licença, leia a mensagem na caixa de diálogo e confirme clicando em **Avançar**.
 - O arquivo de licença é copiado e os componentes são instalados e iniciados.
 - Os recursos do programa serão instalados. O progresso da instalação é exibido na caixa de diálogo.
- ▶ Clique em **Concluir** para encerrar o processo de instalação.
 - O **Assistente de instalação** é fechado e o **Assistente de configuração** é exibido.

3.5 Assistente de configuração

Ao final de uma instalação definida pelo usuário, o assistente de configuração é aberto. O assistente de configuração permite que você defina configurações personalizadas para o produto Avira.

- ▶ 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 o System Scanner (verificação sob demanda) e pela Realtime Protection (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 produto Avira 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 Avira FireWall, a caixa de diálogo **Regras padrão para acessar a rede e usar recursos de rede** será 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 da Realtime Protection da Avira, a caixa de diálogo **Modo de inicialização da Realtime Protection** será exibida. Você pode estipular a hora de início da Realtime Protection. Em cada reinicialização do computador, a Realtime Protection será iniciada no modo de inicialização especificado.

Observação

O modo de inicialização da Realtime Protection especificado é salvo no registro e não pode ser alterado na Configuração.

Observação

Quando o modo de inicialização padrão para a Realtime Protection (inicialização Normal) tiver sido escolhido e o processo de login na inicialização for executado rapidamente, os programas configurados para iniciar automaticamente na inicialização não serão verificados, pois podem estar em execução antes de a Realtime Protection ser inicializada completamente.

- ▶ Ative a opção necessária e continue a configuração clicando em **Avançar**.
 - ↳ Na próxima caixa de diálogo, **Selecionar configurações de email**, você pode definir as configurações do Servidor para o envio de emails. O produto Avira usa SMTP para enviar emails e enviar alertas de email.
- ▶ Quando apropriado, faça os ajustes necessários nas configurações do servidor e continue a configuração clicando em **Avançar**.
 - ↳ 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**
 - ↳ 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.
- ▶ Se após a verificação você receber uma solicitação de reinicialização de seu computador, clique em **Sim** para garantir que seu sistema esteja totalmente protegido.

Após a instalação, recomendamos que você verifique se o programa está atualizado no campo **Status do Centro de controle**.

- ▶ Se seu produto Avira mostrar que seu computador não está protegido, clique em **Corrigir problema**.
 - ↳ A caixa de diálogo **Restaurar a proteção** é aberta.
- ▶ Ative as opções predefinidas a fim de maximizar a segurança de seu sistema.
- ▶ Se for apropriado, realize em seguida uma verificação completa do sistema.

3.6 Alterar instalação

Você pode adicionar ou remover componentes individuais do programa da instalação atual do produto Avira (consulte o [Capítulo Instalação e desinstalação > Módulos de instalação](#)).

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

Selecione seu produto Avira e clique em **Alterar**. Na caixa de diálogo **Bem-vindo**, selecione a opção **Modificar**. Você será orientado pelas alterações de instalação.

3.7 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.

- **Avira Professional Security**
Esse módulo contém todos os componentes necessários para uma instalação bem-sucedida do produto Avira.
- **Realtime Protection da Avira**
A Realtime Protection da Avira executa 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 produto Avira verifica o arquivo automaticamente. A renomeação de um arquivo não aciona uma verificação da Realtime Protection da Avira.
- **Avira ProActiv**
O componente Avira 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 à Realtime Protection da Avira.
- **Mail Protection da Avira**
A Mail Protection é a interface entre seu computador e o servidor de email do qual seu programa de email (cliente de email) baixa emails. A Mail Protection é conectada como um proxy entre o programa e o servidor de email. Todos os emails recebidos passam por esse proxy, verificados quanto a vírus e programas indesejados e encaminhados ao seu programa de email. Dependendo da configuração, o programa processa os emails afetados automaticamente ou solicita alguma ação para o usuário.
- **Avira Web Protection**
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 pela Realtime Protection da Avira não é permitida. Isso

poderia permitir o acesso de vírus e programas indesejado ao sistema do seu computador. A Web Protection é conhecida 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.
- **Avira Rootkits Protection**
O *Avira* Rootkits 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 do shell**
A extensão do Shell gera a entrada **Verificar os arquivos selecionados com o Avira** no menu de contexto do Windows Explorer (botão direito do mouse). Com essa entrada, é possível verificar arquivos ou diretórios diretamente.

3.8 Desinstalação

Se você quiser remover o produto Avira de seu computador, use a opção **Adicionar ou remover programas** para **Alterar/remover** programas no Painel de controle do Windows.

Para desinstalar o produto Avira (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 seu produto Avira 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 produto Avira está desinstalado e todos os diretórios, arquivos e entradas de registro do programa são excluídos quando o computador é reiniciado.

3.9 Instalação e desinstalação na rede

Para simplificar a instalação dos produtos Avira em uma rede com vários computadores cliente para o administrador do sistema, o produto Avira tem um procedimento especial para a instalação inicial e de alteração.

Para a instalação automática, o programa de instalação trabalha com o arquivo de controle *setup.inf*. O programa de instalação (*presetup.exe*) está contido no pacote de instalação do programa. A instalação é iniciada com um arquivo de script ou lote e todas as informações necessárias são obtidas a partir do arquivo de controle. Os comandos de scripts substituem as entradas manuais normais durante a instalação.

Observação

Um arquivo de licença é obrigatório para a instalação inicial na rede.

Observação

É necessário ter um pacote de instalação do produto Avira para executar a instalação através de uma rede. Não é possível usar um arquivo de instalação para a instalação baseada na Internet.

Os produtos Avira podem ser compartilhados com facilidade na rede com um script de login do servidor ou via SMS.

Para obter informações sobre instalação e desinstalação na rede:

- consulte o Capítulo: [Parâmetros de linha de comando para o programa de instalação](#)
- consulte o Capítulo: [Parâmetro do arquivo *setup.inf*](#)
- consulte o Capítulo: [Instalação na rede](#)
- consulte o Capítulo: [Desinstalação na rede](#)

Observação

O Avira Management Console fornece outra opção fácil para a instalação e desinstalação dos produtos Avira na rede. O Avira Management Console permite a instalação remota e a manutenção dos produtos Avira na rede. Para obter mais informações, acesse nosso site.

<http://www.avira.com/pt-br>.

A instalação pode ser controlada por script no modo de lote.

A configuração é adequada para as seguintes instalações:

- Instalação inicial através da rede (instalação autônoma)
- Instalação em computadores com um único usuário

▶ Alterar instalação e atualização

Observação

Recomendamos que você teste a instalação automática antes que a rotina de instalação seja implementada na rede.

Observação

Ao instalar em um sistema operacional de servidor, a Realtime Protection e a proteção de arquivos não estará disponível.

Para instalar o produto Avira na rede automaticamente:

- ✓ Você deve ter direitos de administrador (também necessários no modo de lote)
- ▶ Configure o parâmetro do arquivo *setup.inf* e salve o arquivo.
- ▶ Inicie a instalação com o parâmetro */inf* ou integre o parâmetro no script de login do servidor.

Exemplo: `presetup.exe /inf="c:\temp\setup.inf"`

→ A instalação é iniciada automaticamente.

Para desinstalar os produtos Avira na rede automaticamente:

- ✓ Você deve ter direitos de administrador (também necessários no modo de lote)
- ▶ Inicie a desinstalação com o parâmetro */remsilent* ou */remsilentaskreboot* ou integre o parâmetro no script de login do servidor.

Você também pode especificar o parâmetro para o registro de desinstalação.

Exemplo: `presetup.exe /remsilent /unsetuplog="c:\logfile\unsetup.log"`

→ A desinstalação é iniciada automaticamente.

Observação

O programa de configuração para a desinstalação deve ser iniciado no PC no qual o produto Avira será desinstalado; não inicie o programa de configuração a partir de uma unidade de rede.

3.9.1 Parâmetros de linha de comando para o programa de instalação

Observação

Os parâmetros que contêm caminhos ou nomes de arquivo precisam estar em

aspas duplas (Exemplo:

```
InstallPath="%PROGRAMFILES%\Avira\AntiVir Server\").
```

O parâmetro a seguir é permitido para instalação:

- /inf

O programa de instalação começa com o script mencionado e recupera todos os parâmetros necessários.

Exemplo: `presetup.exe /inf="c:\temp\setup.inf"`

Os parâmetros a seguir são permitidos para a desinstalação:

- /remove

O programa de instalação desinstala o produto Avira.

Exemplo: `presetup.exe /remove`

- /remsilent

O programa de instalação desinstala o produto Avira sem exibir caixas de diálogo. O computador é reiniciado após a desinstalação.

Exemplo: `presetup.exe /remsilent`

- /remsilentaskreboot

O programa de instalação desinstala o produto Avira sem exibir caixas de diálogo e solicita a reinicialização do computador após a desinstalação.

Exemplo: `presetup.exe /remsilentaskreboot`

O parâmetro a seguir está disponível como uma opção para o registro de desinstalação:

- /unsetuplog

Todas as ações realizadas durante a desinstalação são registradas.

Exemplo: `presetup.exe /remsilent`

`/unsetuplog="c:\logfile\unsetup.log"`

No arquivo de controle *setup.inf*, é possível definir os seguintes parâmetros no campo [DATA] para a instalação automática do produto Avira. A sequência dos parâmetros não importa. Se uma configuração de parâmetro estiver faltando ou for incorreta, a rotina de instalação será interrompida e uma mensagem de erro será exibida.

Observação

Os parâmetros que contêm caminhos ou nomes de arquivo precisam estar em aspas duplas (Exemplo:

```
InstallPath="%PROGRAMFILES%\Avira\AntiVir Server\").
```

- DestinationPath

Caminho de destino no qual o programa é instalado. Deve ser incluído no script. A instalação inclui o nome da empresa e o nome do produto automaticamente.

Variáveis de ambiente podem ser usadas.

Exemplo: DestinationPath=%PROGRAMFILES%
produz o caminho de instalação C:\Program Files\Avira\AntiVir Desktop

- ProgramGroup

Cria um grupo de programa para todos os usuários do computador no menu Iniciar do Windows.

1: Criar grupo de programa

0: Não criar grupo de programa

Exemplo: ProgramGroup=1

- DesktopIcon

Cria um ícone do atalho na área de trabalho para todos os usuários do computador na área de trabalho.

1: Criar ícone na área de trabalho

0: Não criar ícone na área de trabalho

Exemplo: DesktopIcon=1

- ShellExtension

Registra a extensão do shell no registro. Com a extensão do shell, os arquivos ou diretórios podem ser verificados quanto à presença de vírus e malwares através do menu de contexto exibido ao clicar com o botão direito do mouse.

1: Registrar extensão do shell

0: Não registrar extensão do shell

Exemplo: ShellExtension=1

- Guard

Instala a Realtime Protection da Avira (scanner de acesso).

1: Instalar a Realtime Protection da Avira

0: Não instalar a Realtime Protection da Avira

Exemplo: Guard=1

- MailScanner

Instala a Mail Protection da Avira.

1: Instalar a Mail Protection da Avira

0: Não instalar a Mail Protection da Avira

Exemplo: MailScanner=1

- KeyFile

Especifica o caminho para o arquivo de licença que é copiado durante a instalação. Para instalação inicial: obrigatório. O nome do arquivo deve ser especificado por completo (totalmente qualificado). (Para uma instalação de alteração: opcional.

Exemplo: KeyFile=D:\inst\license\hbedv.key

- ShowReadMe

Exibe o arquivo *readme.txt* após a instalação.

1: Exibir arquivo

0: Não exibir arquivo

Exemplo: ShowReadMe=1

- `RestartWindows`

Reinicia o computador após a instalação. Essa entrada tem uma prioridade maior do que `ShowRestartMessage`.

1: Reiniciar o computador
0: Não reiniciar o computador
Exemplo: `RestartWindows=1`
- `ShowRestartMessage`

Exibe informações durante a instalação antes de realizar uma reinicialização automática.

0: Não exibir informações
1: Exibir informações
Exemplo: `ShowRestartMessage=1`
- `SetupMode`

Não obrigatório para a instalação inicial. O programa de instalação sabe se uma instalação inicial foi executada. Especifica o tipo de instalação. Se uma instalação já estiver disponível, deverá ser indicado no `SetupMode` se essa instalação é somente uma atualização, uma instalação de alteração (reconfiguração) ou uma desinstalação.

`Update`: atualiza uma instalação existente. Nesse caso, os parâmetros de configuração (por exemplo, `Guard`) são ignorados.
`Modify`: modifica (reconfigura) uma instalação existente. No processo, nenhum arquivo é copiado no caminho de destino.
`Remove`: desinstala o produto Avira do sistema.
Exemplo: `SetupMode=Update`
- `AVWinIni` (optional)

Especifica o caminho de destino do arquivo de configuração que pode ser copiado durante a instalação. O nome do arquivo deve ser especificado por completo (totalmente qualificado).

Exemplo: `AVWinIni=d:\inst\config\avwin.ini`
- `Password`

Essa opção atribui a senha que foi definida para a instalação (modificação) e desinstalação como a rotina de instalação. A entrada só é verificada pela rotina de instalação quando uma senha é definida. Se uma senha tiver sido definida e o parâmetro de senha estiver faltando ou incorreto, a rotina de instalação será interrompida.

Exemplo: `Password>Password123`
- `WebGuard`

Instala a Web Protection da Avira.

1: Instala a Proteção para web da Avira
0: Não instalar a Proteção para web da Avira
Exemplo: `WebGuard=1`
- `RootKit`

Instala o módulo do Avira Rootkits Protection. Sem o Avira Rootkits Protection, o System scanner não consegue verificar rootkits no sistema.

1: Instalar o Avira Rootkits Protection

0: Não instalar o Avira Rootkits Protection

Exemplo: `RootKit=1`

- `ProActiv`

Instala o componente Avira ProActiv. O Avira ProActiv é uma tecnologia de detecção baseada em modelo que permite que malwares ainda desconhecidos sejam detectados.

1: Instalar o ProActiv

0: Não instalar o ProActiv

Exemplo: `ProActiv=1`

- `FireWall`

Instala o componente Avira FireWall. O Avira FireWall monitora e controla o tráfego de dados recebidos e enviados no seu sistema de computador para verificar a presença de ameaças originada da Internet ou de outros ambientes de rede.

1: Instalar o FireWall

0: Não instalar o FireWall

Exemplo: `FireWall=1`

4. Visão geral do Avira Professional Security

Este capítulo contém uma visão geral da funcionalidade e da operação do produto Avira.

- consulte o Capítulo [Interface e operação](#)
- Consulte o Capítulo Como...?

4.1 Interface de usuário e operação

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

- [Centro de controle](#): monitorar e controlar o produto Avira
- [Configuração](#): configurar o produto Avira
- [Ícone de bandeja](#) do sistema na barra de tarefas: abre o Centro de controle e outras funções

4.1.1 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 produto Avira.



A janela Centro de controle é dividida em três áreas: a **Barra de menus**, a **Barra de navegação** e a janela de detalhes **Status**:

- **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: Atividade *Proteção local* - Seção **Realtime Protection**.
- **Status:** 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.

4.1.2 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 produto Avira.

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

4.1.3 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.

Observação

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 **Enter**, 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.

4.1.4 Visão geral do Centro de controle

- **Status:** Na tela **Status**, você encontrará todas as seções com as quais é possível monitorar o funcionamento do produto Avira.
 - A seção **Status** permite ver rapidamente quais módulos do programa estão ativos e fornece informações sobre a última atualização realizada. Também é possível ver se você possui uma licença válida.
- **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 Realtime Protection exibe informações sobre arquivos verificados, além de outros dados de estatística que podem ser redefinidos a qualquer momento e permite o acesso ao arquivo de relatório. É possível obter informações mais detalhadas sobre o último vírus ou programa indesejado detectado "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 Mail Protection mostra todos os emails verificados pela Mail Protection, suas propriedades e outros dados estatísticos.

A seção Web Protection exibe informações sobre URLs verificados e vírus detectados, além de outros dados de estatística, que podem ser redefinidos a qualquer momento e permite o acesso ao arquivo de relatório. É possível obter informações mais detalhadas sobre o último vírus ou programa indesejado detectado "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.

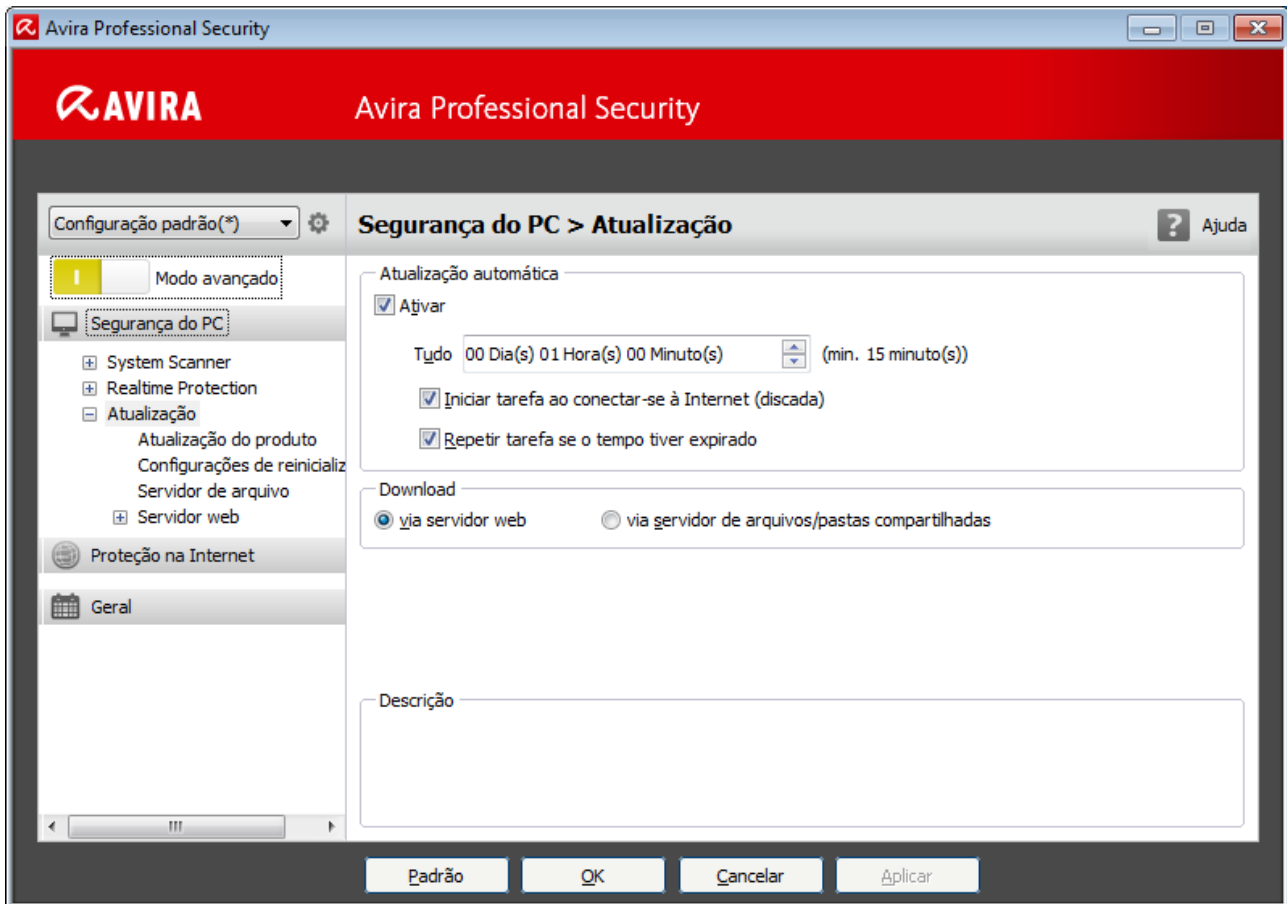
- **Gerenciamento:** Em **Gerenciamento**, você encontrará ferramentas para isolar e gerenciar arquivos suspeitos ou infectados e para planejar tarefas recorrentes.

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, e adaptar ou excluir os trabalhos existentes.

4.1.5 Configuração

Você pode definir as configurações do produto Avira na Configuração. Após ser instalado, o produto Avira é configurado com configurações padrão, garantindo uma excelente proteção para seu computador. No entanto, seu computador ou seus requisitos específicos para o produto Avira 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.

4.1.6 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 produto Avira.
- no Centro de controle através do item de menu Extras > Configuração.
- no Centro de controle através do botão Configuração.

Observação

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.

4.1.7 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.

Observação

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.

Observação

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.

4.1.8 Perfis de configuração

Você tem a opção de salvar suas configurações como perfis de configuração. No perfil de configuração, todas as opções de configuração são salvas em um grupo. A configuração é exibida na barra de navegação como um nó. Você pode adicionar outras configurações à configuração padrão. Você também pode definir regras para alternar para uma configuração específica:

Ao mudar de configuração usando um procedimento baseado em regra, a configuração pode ser vinculada a uma LAN ou conexão via Internet (identificação através do gateway padrão). Desse modo, os perfis de configuração podem ser criados para diferentes cenários de uso de notebooks:

- Uso em redes corporativas: atualização por meio do servidor de intranet, Proteção da web desativada
- Uso doméstico: atualização através do servidor padrão da web da Avira, Web Protection ativado

Se nenhuma regra de alternância tiver sido definida, você poderá alternar para uma configuração manualmente no menu de contexto do ícone de bandeja. Você pode adicionar, renomear, excluir, copiar ou restaurar configurações e definir regras para mudar configurações usando os botões da barra de navegação ou os comandos do menu de contexto na seção de configuração.

Observação

A alternância automática para outra configuração não tem suporte no Windows 2000. Nenhuma regra para alternar configurações pode ser definida no Windows 2000.

Visão geral das opções de configuração

As seguintes opções de configuração estão disponíveis:



- **System 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
- **Realtime Protection:** 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
- **Mail Protection:** Configuração da Mail Protection
 - Opções de verificação: ativar o monitoramento das contas POP3, das contas IMAP, dos emails de saída (SMTP)
 - Ações para malware
 - Heurísticas da verificação da Mail Protection
 - Exceções de verificação da Mail Protection
 - Configuração do cache, esvaziar cache
 - Configuração de um rodapé nos emails enviados
 - Configuração da função de registro
- **Web Protection:** Configuração da Web Protection
 - Opções de verificação, ativação e desativação da Web Protection
 - Ação para detecção
 - Acesso bloqueado: tipos de arquivo e tipos MIME indesejados, filtro da Web para URLs indesejados conhecidos (malware, phishing etc.)
 - Exceções de verificação da Web Protection URLs, tipos de arquivo, tipos MIME
 - Heurísticas da Web Protection
 - 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)
- **Geral:**
 - Configuração de email usando SMTP
 - 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, download através do servidor da Web ou do servidor de arquivos, configuração das atualizações do produto
 - Alertas: Configuração de alertas de email para componentes:
 - System Scanner
 - Proteção em tempo real
 - Atualizador
 - Configuração de alertas de rede para os componentes System Scanner, Realtime Protection

- Configuração de alertas acústicos emitidos quando malwares são detectados

4.1.9 Ícone de bandeja

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

Ícone	Descrição
	A Realtime Protection da Avira é ativada e o FireWall é ativado
	A Realtime Protection da Avira é desativada e o FireWall é desativado

O ícone na bandeja exibe o status do serviço Realtime Protection e FireWall.

As funções centrais do produto Avira 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.

4.1.10 Entradas do menu de contexto

- **Ativar a Realtime Protection da Avira:** Ativa ou desativa a Realtime Protection da Avira.
- **Ativar a Mail Protection da Avira:** Ativa ou desativa a Mail Protection da Avira.
- **Ativar a Web Protection da Avira:** Ativa ou desativa a Web Protection da Avira.
- **FireWall:**
 - **Ativar FireWall:** Ativa ou desativa o FireWall
 - **Bloquear todo o tráfego:** Ativado: bloqueia todas as transferências de dados, exceto as transferências 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 Avira:** Abre o Centro de controle.
- **Configurar o Avira:** Abre a Configuração
- **Iniciar atualização** Inicia uma atualização.
- **Selecionar configuração:** Abre um submenu com os perfis de configuração disponíveis. Clique em uma configuração para ativá-la. O comando de menu é

desativado se você tiver definido regras para alternar automaticamente para uma configuração.

- **Ajuda:** abre a Ajuda on-line.
- **Sobre Avira Professional Security:** Abre uma caixa de diálogo com informações sobre o produto Avira: 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.

4.2 Como...?

4.2.1 Ativar licença

Para ativar a licença de seu produto Avira:

Ative sua licença de seu produto Avira com o arquivo de licença *hbedv.key*. Você pode obter o arquivo de licença por email com a Avira. O arquivo de licença contém a licença de todos os produtos que você adquiriu em um processo de pedido.

Caso ainda não tenha instalado seu produto Avira:

- ▶ Salve o arquivo de licença em um diretório local do seu computador.
- ▶ Instale o produto Avira.
- ▶ Durante a instalação, insira o local de salvamento do arquivo de licença.

Caso já tenha instalado seu produto Avira:

- ▶ Clique duas vezes no arquivo de licença no Gerenciador de arquivos ou no email de ativação e siga as instruções exibidas na tela quando o Gerenciador da licença for aberto.
- OU -

No Centro de controle de seu produto Avira, selecione o item de menu **Ajuda > Carregar arquivo de licença...**


Observação

No Windows Vista, a caixa de diálogo Controle de Conta de Usuário é exibida. Faça login como administrador, se apropriado. Clique em **Continuar**.

- ▶ Realce o arquivo de licença e clique em **Abrir**.
 - ↪ Uma mensagem é exibida.
- ▶ Clique em **OK** para confirmar.
 - ↪ A licença é ativada.
- ▶ Se necessário, reinicie o sistema.

4.2.2 Executar atualização automática

Para criar um trabalho com o Avira Scheduler para atualizar seu produto Avira automaticamente:

- ▶ No Centro de Controle, selecione a seção **Administração > Programador**.
- ▶ Clique no  ícone **Inserir novo trabalho**.
 - ↳ 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**

Observação

Recomendamos que você faça atualizações regularmente e com frequência. O intervalo de atualização recomendado é: 60 minutos.






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

Os trabalhos antigos são executados agora porque não foram executados no horário programado (por exemplo, o computador foi desligado).
 - **Iniciar trabalho ao conectar-se à Internet (discada)**

Além da frequência definida, o trabalho é executado quando uma conexão com a Internet é configurada.
- ▶ Clique em **Avançar**.
 - ↳ A caixa de diálogo **Selecionar modo de exibição** é exibida.
- ▶ Selecione o modo de exibição da janela do trabalho:

- **Invisível:** sem janela de trabalho
- **Minimizar:** somente barra de andamento
- **Maximizar:** janela de trabalho inteira
- ▶ Clique em **Concluir**.
 - ↳ O trabalho recém criado aparece na página inicial da seção **Administração > 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
-  Editar trabalho
-  Excluir trabalho
-  Iniciar trabalho
-  Interromper trabalho

4.2.3 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 **Fazer download e instalação das atualizações do produto automaticamente** na configuração em [Proteção do PC > Atualizar > Atualização do produto](#).

Para iniciar uma atualização manualmente de seu produto Avira:

- ▶ Com o botão direito do mouse, clique no ícone de bandeja da Avira 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.

Observação

Recomendamos a realização de atualizações automáticas periódicas. O intervalo de atualização recomendado é: 60 minutos.

Observação

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

4.2.4 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 de PC > Scanner do sistema**.
 - ↳ 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 do sistema 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 relevante do nível de diretório apropriado:
 - As seguintes opções estão disponíveis, para selecionar diretórios:
 - Diretório, incluindo os subdiretórios (marca de verificação preta)
 - 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)
- Subdiretórios de apenas um diretório (marca de verificação cinza; os subdiretórios têm marcas de verificação pretas)
- Nenhum diretório (sem marca de verificação)

4.2.5 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 produto Avira 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 do sistema é iniciada.
 - Quando a verificação termina, os resultados são exibidos.

4.2.6 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 Avira** no menu de contexto.
 - A janela **Luke Filewalker** é exibida e uma verificação do sistema é iniciada.
 - Quando a verificação termina, os resultados são exibidos.

4.2.7 Verificar presença de vírus e malwares automaticamente

Observação

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 **Administração > 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 **Seleção do 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 **Seleção do modo de exibição** é exibida.
- ▶ Selecione o modo de exibição da janela do trabalho:
 - **Invisível**: sem janela de trabalho
 - **Minimizado**: somente barra de andamento
 - **Maximizado**: janela de trabalho inteira
- ▶ Selecione a opção **Desligar o computador se o trabalho tiver sido concluído** 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 **Administração > 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



Editar trabalho



Excluir trabalho



Iniciar trabalho





Interromper trabalho

4.2.8 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 de PC > System 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 do sistema é iniciada.
 - ↳ Quando a verificação termina, os resultados são exibidos.

4.2.9 Reação aos vírus e malwares detectados

Para os componentes de proteção individuais de seu produto Avira, 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 da Realtime Protection: A Notificação de uma detecção é sempre dada na janela **Realtime Protection: Comportamento suspeito de aplicativo detectado**.

Opções de ação para o System Scanner:

Interativo

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

No caso de uma **Verificação com o System 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 System Scanner.

Automático

No modo de ação automático, quando um vírus ou programa indesejado é detectado, a ação selecionada nessa área é executada automaticamente. Se você puder ativar a opção **Exibir alertas de detecção**, você receberá um alerta sempre que um vírus for detectado, indicando a ação realizada.

Opções de ação para a Realtime Protection:

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 System Scanner, usando o botão **Detalhes**, para o gerenciamento futuro do vírus. O System 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 **Deteção > System Scanner**):

Automático

No modo de ação automático, quando um vírus ou programa indesejado é detectado, a ação selecionada nessa área é executada automaticamente. Se você puder ativar a opção **Exibir alertas de detecção**, você receberá um alerta sempre que um vírus for detectado, indicando a ação realizada.

Opções de ação para detecções para Realtime Protection, Web Protection:

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. Se você puder ativar a opção **Mostrar barra de andamento**, você receberá um alerta sempre que um vírus for detectado, indicando a ação realizada. O alerta permitirá que você confirme a ação a ser executada.

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:

Observação

As ações disponíveis para seleção dependem do sistema operacional, dos componentes de proteção (Realtime Protection, AviraSystem Scanner, AviraMail Protection, Web Protection da Avira) que reportam a detecção e do tipo de malware detectado.

Ações do System Scannere da Realtime Protection (não detecções do ProActiv):

Reparar

O arquivo é reparado.

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

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.

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 posteriormente ou, se necessário, enviados para a Avira.

Excluir

O arquivo será excluído. Esse processo é muito mais rápido do que **Substituir e excluir**. Se um vírus no setor de inicialização for detectado, será possível excluí-lo por meio da exclusão do setor de inicialização. Um novo setor de inicialização é gravado.

Ignorar

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

Substituir e excluir

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

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 da Realtime Protection: Nenhuma ação adicional é executada pela Realtime Protection. 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 rootkits: a detecção é copiada para a quarentena.

Reparar setor de inicialização | Fazer download da 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 produto Avira não puder executar o reparo, você poderá fazer o download de uma ferramenta especial para detecção e remoção dos vírus do setor de inicialização.

Observação

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

Ações da Realtime Protection 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 > Realtime Protection > 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 > Realtime Protection > 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 da Mail Protection: emails recebidos

Mover para quarentena

O email com todos os anexos é movido para a quarentena. O email afetado é excluído. O corpo do texto e todos os anexos do email são substituídos por um [texto padrão](#).

Excluir email

O email 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 email for afetado, ele será excluído e também substituído por um [texto padrão](#). O email 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 email é entregue. O anexo afetado pode ser entregue posteriormente pelo gerenciador de quarentena.

Ignorar

O email 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 email. Nunca abra nenhum anexo clicando duas vezes nele.

Ações da Mail Protection: emails enviados

Mover email para quarentena (não enviar)

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

Bloquear envio de emails (não enviar)

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

Ignorar

O email afetado é enviado.

Aviso

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

Ações da Web Protection:

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 pela Web Protection 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.

Observação

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

Observação

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.com/pt-br/sample-upload>

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

4.2.10 Manipulação de arquivos em quarentena (*.qua)

Para manipular os arquivos em quarentena:


- ▶ No Centro de Controle, selecione a seção **Administração > 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 produto Avira 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 do sistema.
 - Após a verificação, a caixa de diálogo **Estatísticas da nova 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 .

- ▶ Confirme sua escolha com **Sim**.

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 **Suspeita de falso positivo**.
- ▶ Selecione um Formato da resposta: **HTML, Texto, HTML e Texto**.
- ▶ Clique em **OK**.
 - ↳ O arquivo é carregado em um servidor da Web do Centro de pesquisa de malware da Avira em formato compactado.

Observação

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 produto Avira 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.

Suspeita de falso positivo: você supõe que uma detecção de vírus é um falso-positivo: Seu Produto Avira registra uma detecção em um arquivo que pouco provavelmente foi infectado por malware.

Observação

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

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


- ▶ Realce o objeto em quarentena e clique em .
 - ↳ A caixa de diálogo *Procurar pasta* 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.

Observação

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 *quarentena - Bloco de notas* é aberto contendo dados do objeto de quarentena selecionado.
- ▶ Salve o arquivo de texto.



Você também pode restaurar os arquivos em quarentena (consulte Capítulo: [Quarentena: Restauração de arquivos em quarentena](#)).

4.2.11 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 **Administração > Quarentena**.

Observação


Os emails e os anexos de email podem ser restaurados somente usando a opção  se a extensão de 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 emails.

Observação

Os emails e os anexos de email podem ser restaurados somente usando a opção  se a extensão de 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, *Salvar como*, para selecionar o diretório é exibida.
- ▶ Selecione o diretório onde o arquivo será restaurado e confirme.
 - O arquivo é restaurado no diretório selecionado.

4.2.12 Mover arquivos suspeitos para quarentena

Para mover um arquivo suspeito para a quarentena manualmente:

- ▶ No Centro de Controle, selecione a seção **Administração > Quarentena**.
- ▶ Clique em .
- A janela padrão do Windows para selecionar um arquivo é exibida.
- ▶ Selecione o arquivo e confirme **Abrir**.
- O arquivo é movido para a quarentena.

Você pode verificar os arquivos em quarentena com o Avira System Scanner (consulte Capítulo: [Quarentena: Manipulação de arquivos em quarentena \(*.qua\)](#)).

4.2.13 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 de perfis de verificação personalizados):

- ✓ No Centro de controle, vá até a seção **Proteção de PC > System Scanner**.
- ▶ 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 um tipo de arquivo.
- ▶ Clique em **Inserir** 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 permitidos.

4.2.14 Criar atalho na área de trabalho para o perfil de verificação

Você pode iniciar uma verificação do sistema diretamente na área de trabalho através de um atalho para um perfil de verificação sem acessar o Centro de controle do produto da Avira.

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

- ✓ No Centro de controle, e vá até a seção **Proteção de PC > System Scanner**.
- ▶ Selecione o perfil de verificação para o qual deseja criar um atalho.
- ▶ Clique no ícone .
- O atalho é criado na área de trabalho.

4.2.15 Filtrar eventos

Os eventos que foram gerados pelos componentes do programa de seu produto Avira são exibidos no Centro de controle, em **Administração > Eventos** (análogo à exibição do evento do seu sistema operacional Windows). Os componentes do programa, in em ordem alfabética, são os seguintes:

- FireWall
- Serviço de ajuda
- Proteção de email
- Proteção em tempo real
- Programador
- System Scanner
- Atualizador
- Web Protection

Os seguintes tipos de evento são exibidos:

- *Informações*
- *Aviso*
- *Erro*
- *Detecção*

Para filtrar os eventos exibidos:

- ▶ No Centro de Controle, selecione a seção **Administração > 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.

4.2.16 Excluir endereços de email da verificação


Para definir quais endereços de email (remetentes) devem ser excluídos da verificação da Mail Protection (lista de permissões):

- ▶ Vá até o Centro de controle e selecione a seção **Proteção da Internet > Mail Protection**.

→ A lista mostra os emails recebidos.

- ▶ Realce o email que deseja excluir da verificação da Mail Protection.

- ▶ Clique no ícone para excluir o email da verificação do Mail Protection:

-  O endereço de email selecionado não será mais verificado em busca de vírus e programas indesejados.

→ O endereço de email do remetente é incluído na lista de exclusões e não será mais verificado quanto a vírus, malwares.

Aviso

Exclua endereços de email da verificação da Mail Protection somente se os remetentes forem totalmente confiáveis.

Observação

Na Configuração, em [Mail Protection > Geral > Exceções](#), é possível adicionar outros endereços de email à lista de exclusões ou remover endereços de email dessa lista.

4.2.17 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.

Observação

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

Para definir o nível de segurança para o FireWall:

- ▶ Vá até o Centro de controle e selecione a seção **Proteção na Internet > FireWall**.
- ▶ Mova o controle deslizante até o nível de segurança desejado.
 - ↳ O nível de segurança selecionado é aplicado imediatamente.

5. System Scanner

Com o componente System 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 do sistema através do menu de contexto**
A verificação do sistema através do menu de contexto (botão direito do mouse, entrada **Verificar arquivos selecionados com Avira**) 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 do sistema através do menu de contexto.
- **Verificação do sistema através do método de arrastar e soltar**
Quando um arquivo ou diretório é arrastado na janela do programa do Centro de controle, o System 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 do sistema 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. Consulte Verificação do sistema através de perfis
- **Verificação do sistema através do Programador**
O Programador permite que você realize verificações controladas por tempo. Consulte Verificação do sistema através do Programador

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 **Verificação dos registros de inicialização...** no menu **Extras**

6. 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 produto Avira. O Atualizador garante que o produto Avira 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 produto Avira para verificar a presença de vírus e malwares e reparar objetos infectados.
- Mecanismo de verificação:
O mecanismo de verificação contém os métodos usados pelo produto Avira 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.

Observação

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: 60 minutos. Você pode editar ou desativar a atualização automática na configuração ([Configuração > Atualizar](#)).

No Centro de controle, em **Programador**, é possível criar outros trabalhos de atualização realizados pelo Atualizador em intervalos especificados. Você também tem a opção de 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 proprietário ou de um servidor da Web ou de arquivos em uma intranet, que baixa os arquivos de atualização da Internet e os disponibiliza para outros computadores na rede. Isso é útil se você deseja atualizar os produtos Avira em mais de um computador em uma rede. É possível usar um servidor de download em uma intranet para garantir que os produtos Avira sejam atualizados nos computadores protegidos usando o mínimo de recursos. Para configurar um servidor de download funcional em uma intranet, você precisa de um servidor que seja compatível com a estrutura de atualização do produto Avira.

Observação

Você pode usar o Avira Update Manager (servidor da web ou de arquivos no Windows) como um servidor da Web ou de arquivos na Intranet. O Avira Update Manager espelha os servidores de download de produtos Avira e pode ser obtido no site da Avira na Internet.

<http://www.avira.com/pt-br>

Quando um servidor da Web é usado, o protocolo HTTP é usado para o download. Ao usar um servidor de arquivos, o acesso ao arquivo de atualização é concedido pela rede. Você pode configurar a conexão com o servidor da web ou com o servidor de arquivos na Configuração em **Geral > Atualizar**. A configuração padrão usa a conexão com a Internet existente como a conexão com os servidores da web da Avira.

7. Firewall

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.

8. Perguntas frequentes, dicas

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

- Consulte o Capítulo [Ajuda caso ocorra um problema](#)
- Consulte o Capítulo [Atalhos](#)
- Consulte o Capítulo [Central de segurança do Windows](#)

8.1 Ajuda no caso de 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.
- A mensagem de erro *Falha de conexão ao baixar o arquivo ...* é exibida ao tentar iniciar uma atualização.
- Vírus e malwares não podem ser movidos nem excluídos.
- O status do ícone de bandeja está desativado.
- O computador fica extremamente lento quando faço backup dos dados.
- Meu firewall reporta a Realtime Protection da Avira e a Mail Protection da Avira imediatamente após a ativação.
- A Proteção AviraMail 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 pela Mail Protection.
- 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. Consulte também o Capítulo [Gerenciador de licença](#).

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 email, 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 Avira.
- ▶ Se você usar o sistema operacional Windows XP, desative a restauração do sistema.
- ▶ Inicie o computador no modo de segurança.
- ▶ Inicie o produto Avira e a Configuração (Modo de especialista).
- ▶ Selecione [System Scanner > Verificar > 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: Realtime Protection da Avira está desativada.

- ▶ No Centro de controle, na seção Status, na área Realtime Protection da Avira, clique no botão **Ativar**.

Motivo: A Realtime Protection está sendo bloqueada por um firewall.

- ▶ Defina uma aprovação geral para a Realtime Protection na configuração de seu firewall. A Realtime Protection da Avira funciona apenas com o endereço 127.0.0.1 (localhost). Uma conexão com a Internet não é estabelecida. O mesmo se aplica à Mail Protection da Avira.

Caso contrário:

- ▶ Verifique o tipo de inicialização do serviço Realtime Protection. 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*). Encontre a entrada *Realtime Protection da Avira*. **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, a Realtime Protection verifica todos os arquivos que estão sendo usados pelo procedimento de backup.

- ▶ Na Configuração (modo de especialista), escolha **Realtime Protection > Verificar > Exceções** e insira os nomes dos processos do software de backup.

Meu firewall reporta a Realtime Protection da Avira e a Mail Protection da Avira imediatamente após a ativação.

Motivo: a comunicação com a Realtime Protection e a Mail Protection da Avira ocorre através do protocolo de Internet TCP/IP. Um firewall monitora todas as conexões através desse protocolo.

- ▶ Defina uma aprovação geral para a Realtime Protection e para a Mail Protection da Avira. A Realtime Protection da Avira funciona apenas com o endereço 127.0.0.1 (localhost). Uma conexão com a Internet não é estabelecida. O mesmo se aplica à Mail Protection da Avira.

A Mail Protection da Avira não funciona.

Verifique o funcionamento correto da Realtime Protection da Avira com a ajuda das listas de verificação a seguir, caso ocorram problemas com a Mail Protection da Avira.

Lista de verificação

- ▶ Verifique se seu cliente de email 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). A Mail Protection da Avira não é compatível com SSL e, portanto, encerra qualquer conexão SSL criptografada. Se você quiser usar conexões SSL criptografadas sem que elas sejam protegidas pela

Mail Protection, será necessário usar uma porta que não seja monitorada pela Mail Protection. As portas monitoradas pela Mail Protection podem ser definidas na configuração, em [Mail Protection > Verificar](#).

- ▶ O serviço Mail Protection da Avira 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 *Mail Protection da Avira*. 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 produto Avira em "Iniciar > Configurações > Painel de controle > Adicionar ou remover programas", reinicie o computador e reinstale o produto Avira.

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 emails enviados em busca de vírus e programas indesejados.

Observação

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 Avira 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 botão **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 regra**.
- ▶ 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 pela Mail Protection.

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

- ▶ Use uma porta que não seja a porta 25, que é usada pelo SMTP. Isso não será observado pelo monitoramento da Mail Protection.
- ▶ Desative a conexão TSL criptografada e desative o suporte para TSL em seu cliente de email.
- ▶ Desative (temporariamente) o monitoramento dos emails de saída pela Mail Protection na configuração em [Mail Protection > 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: a Web Protection 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", a Web Protection 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: [Web Protection > Exceções](#)).

8.2 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.

8.2.1 Nas caixas de diálogo

Atalho	Descrição
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.

8.2.2 Na ajuda

Atalho	Descrição
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.
------------------------------------	------------------------

8.2.3 No Centro de controle

Geral

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

Seção Verificar

Atalho	Descrição
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)

8.3 Central de segurança do Windows

- Windows XP Service Pack 2 ou superior -

8.3.1 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.

8.3.2 A Central de segurança do Windows e o produto Avira

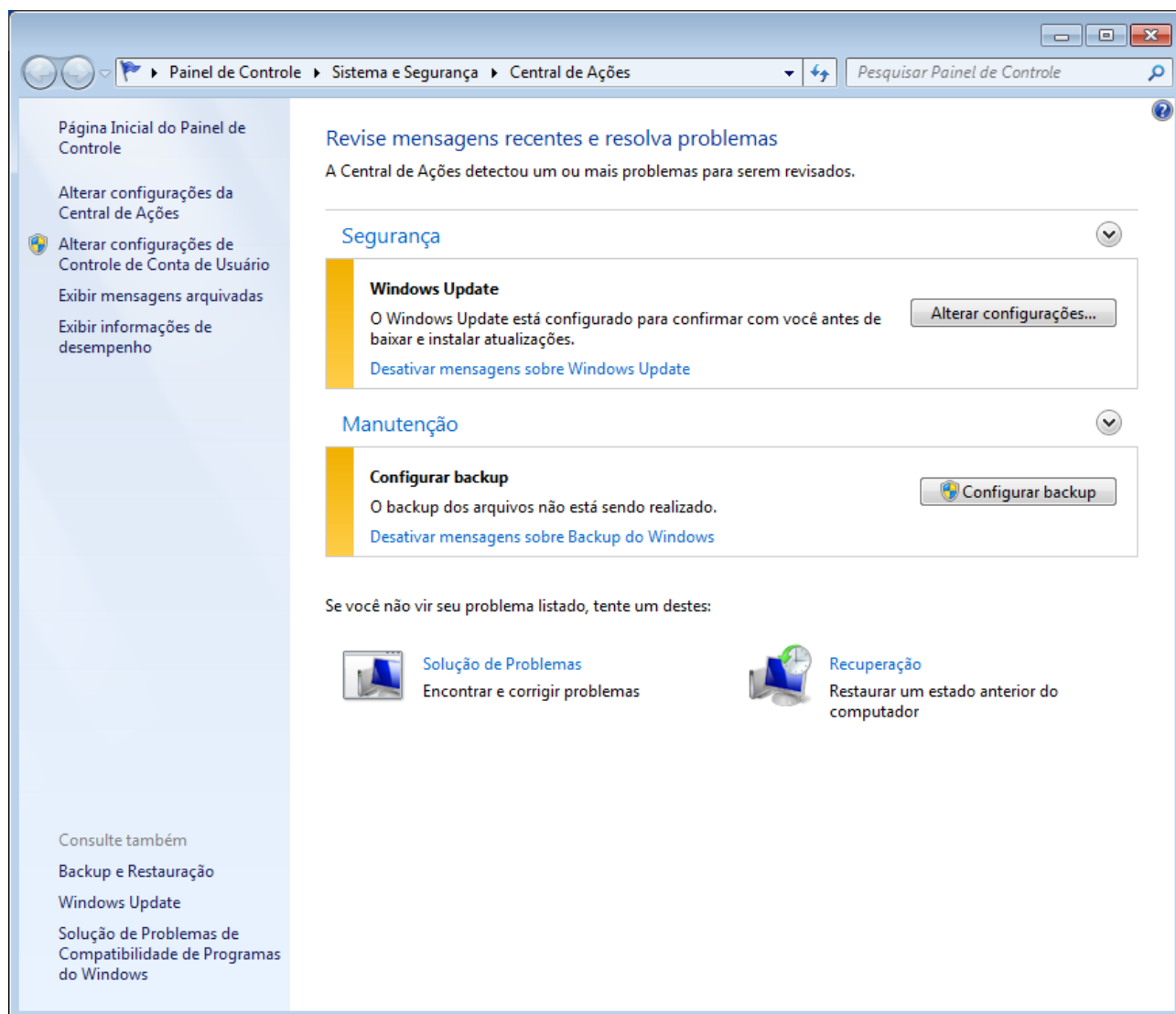
FireWall

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

- [Firewall ATIVO/Firewall ativado](#)
- [Firewall INATIVO/Firewall desativado](#)

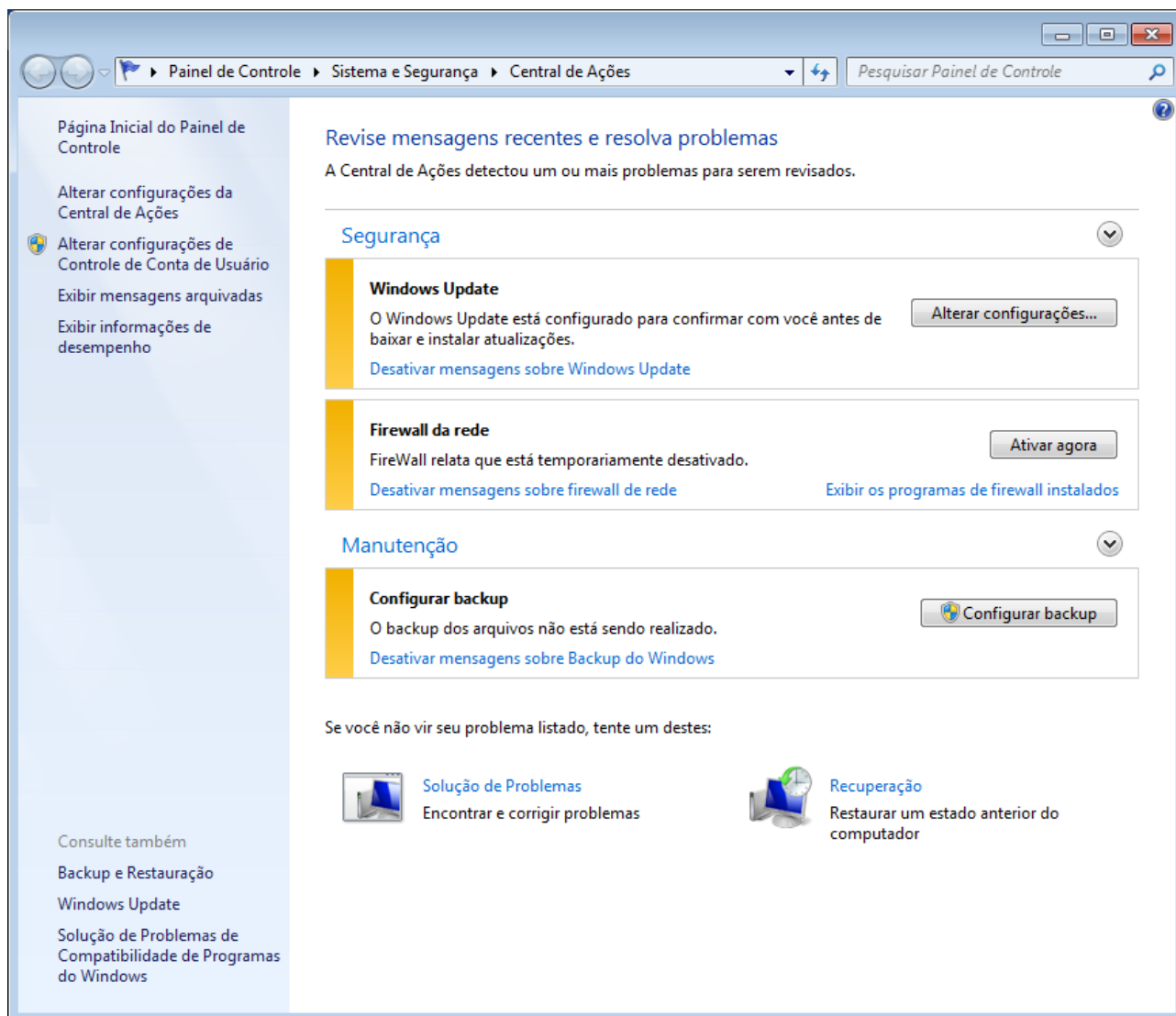
Firewall ATIVO/Firewall ativado

Após a instalação do produto Avira 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:



Observação

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.

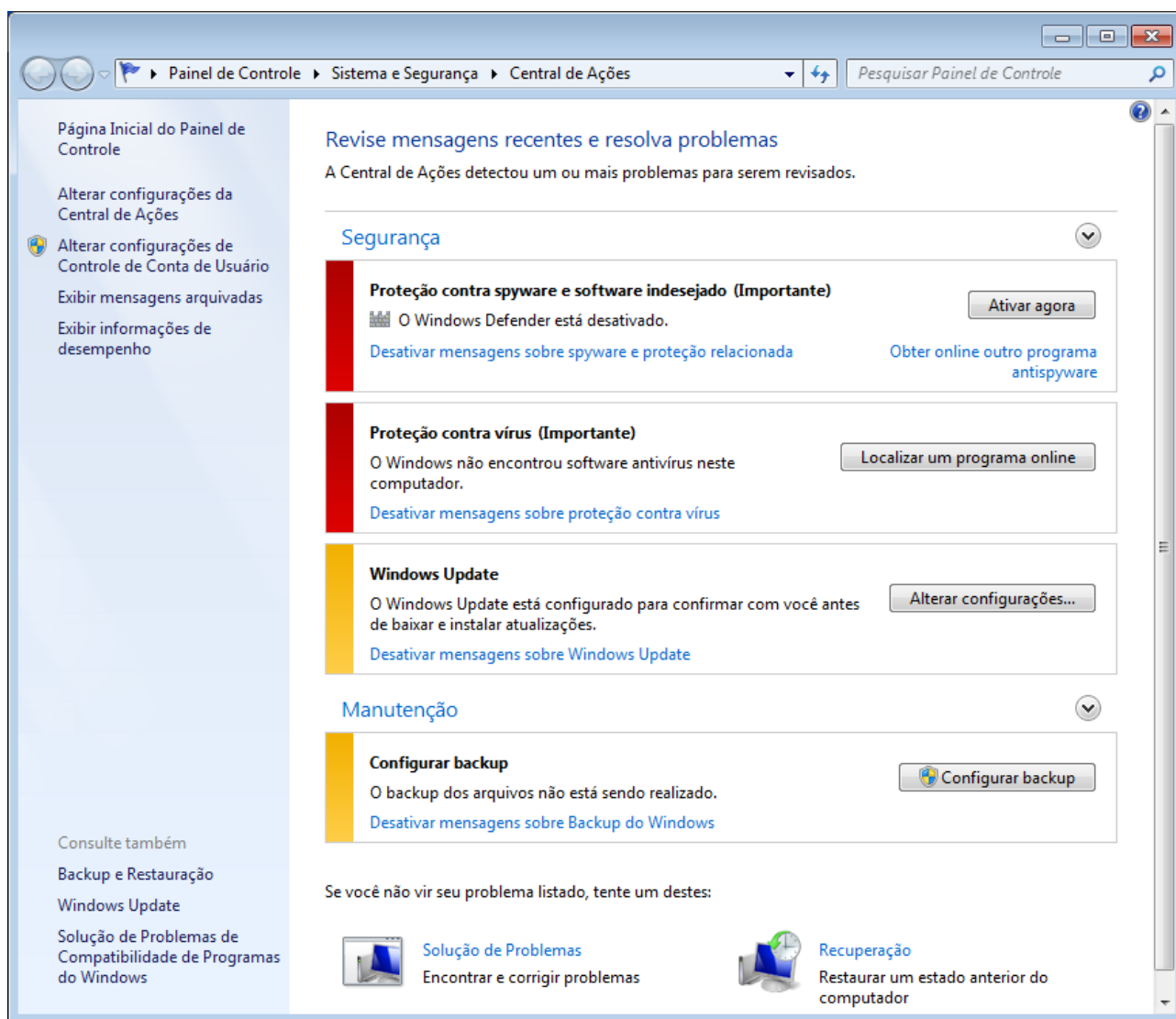
Software de proteção contra vírus/Proteção contra software malicioso

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.

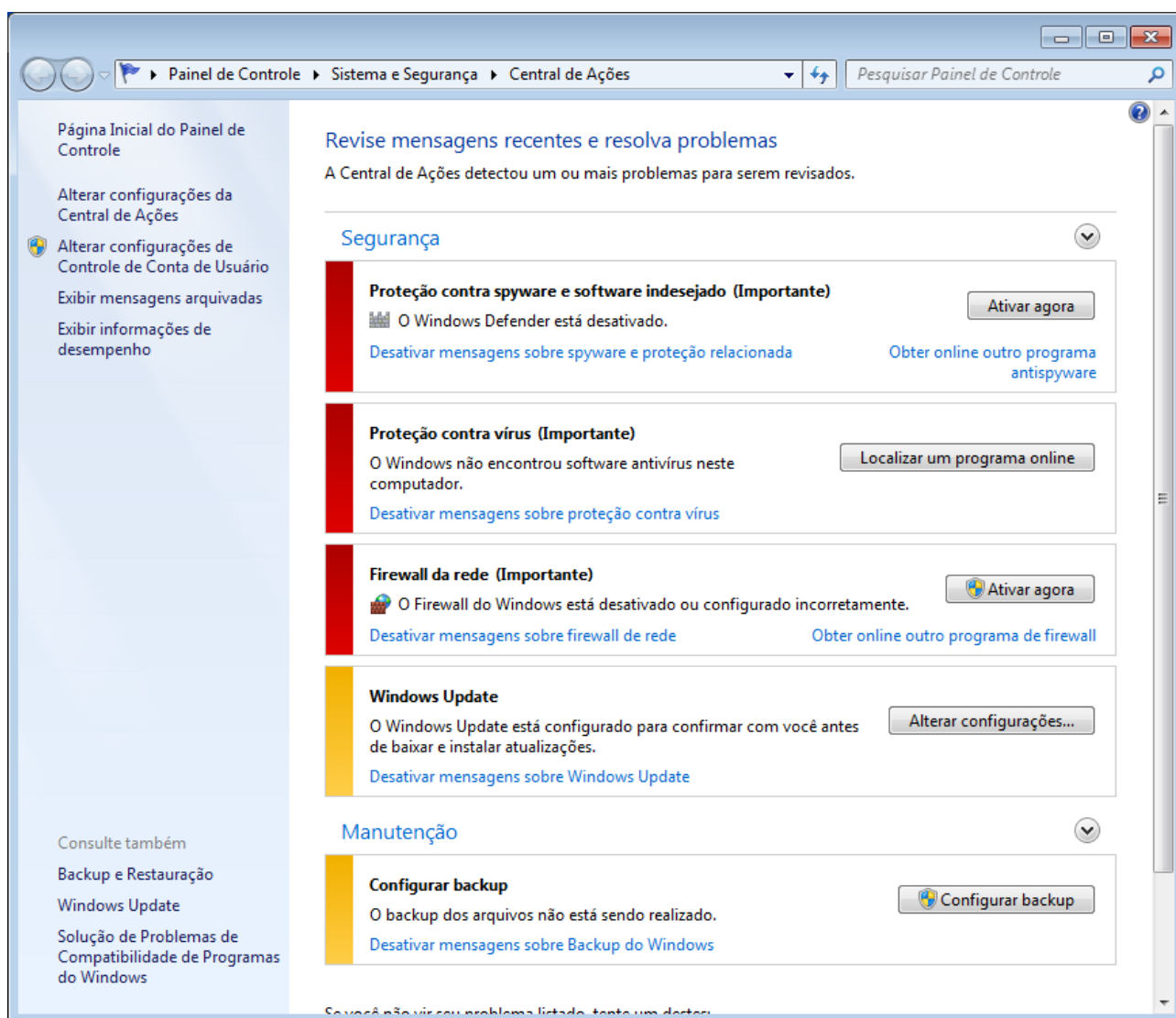


Observação

Instale o produto Avira 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 produto Avira ou se você instalar o Windows XP Service Pack 2 ou o Windows Vista em um sistema no qual o produto Avira já está instalado, a seguinte mensagem será exibida:



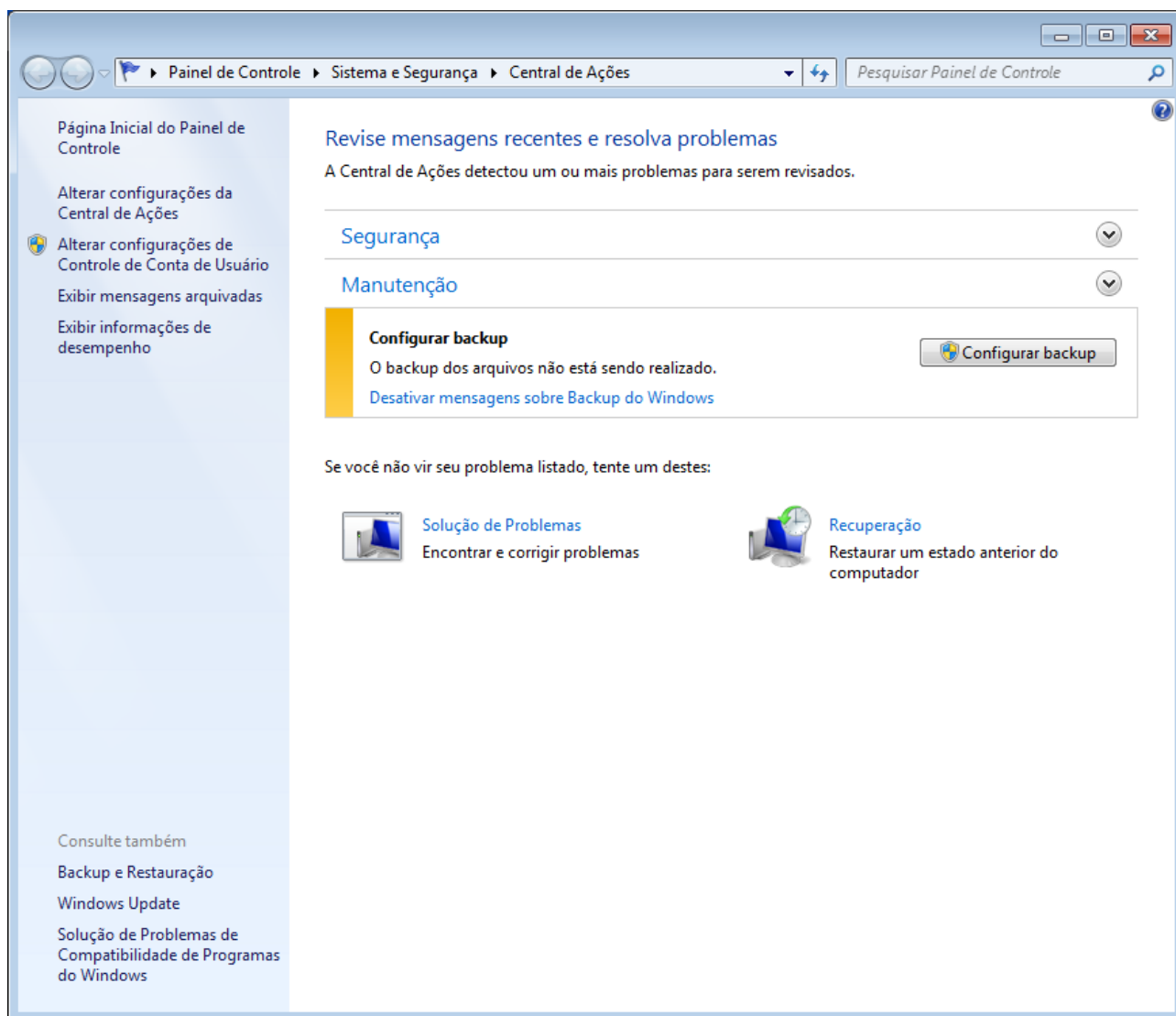
Observação

Para que a Central de segurança do Windows reconheça o produto Avira como

um produto atualizado, é necessário executar uma atualização após a instalação. Atualize o sistema executando uma atualização.

Proteção contra vírus ATIVADA

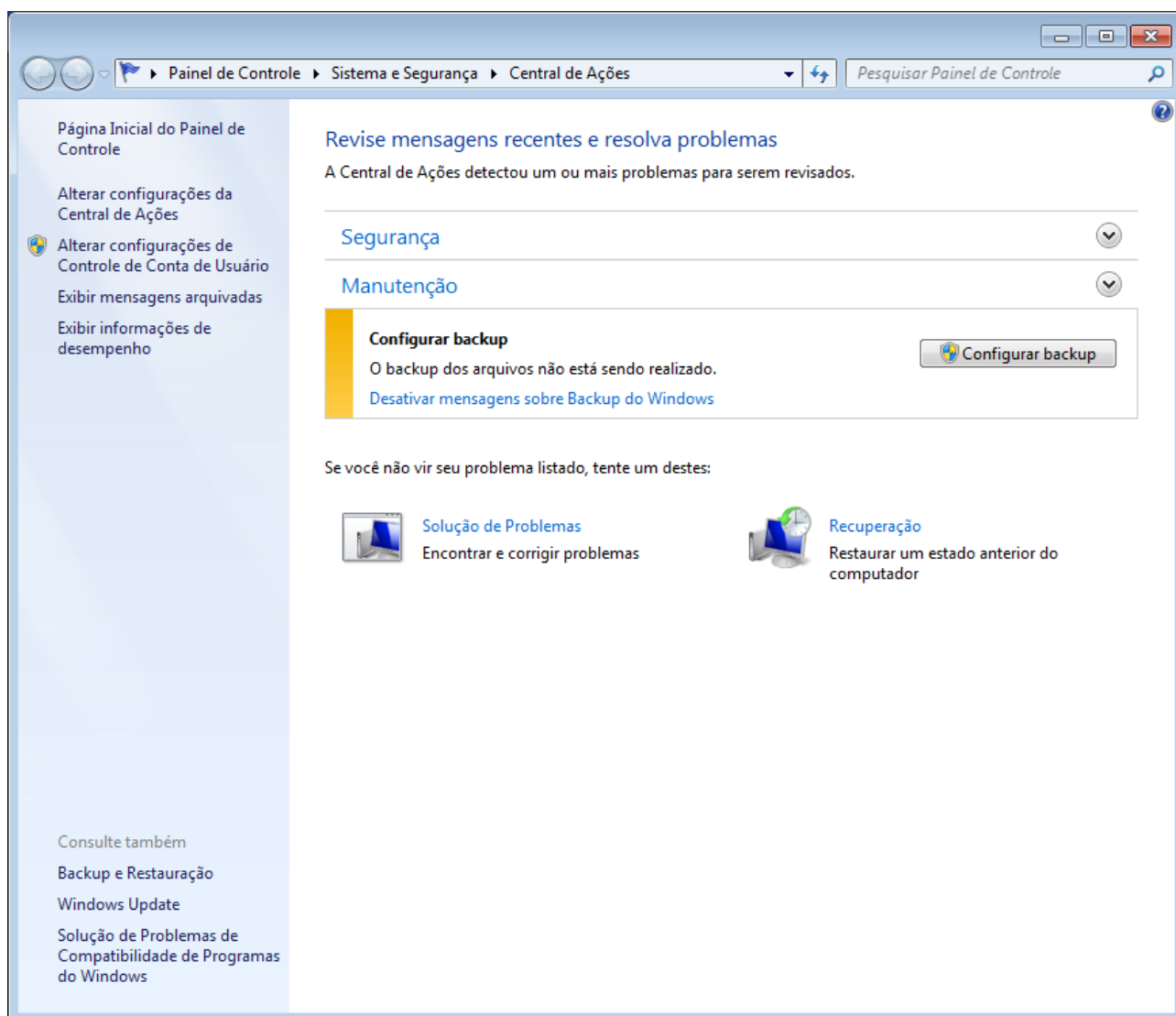
Após a instalação do produto Avira e a execução de uma atualização em seguida, a seguinte mensagem será exibida:



O produto Avira agora está atualizado e a Realtime Protection da Avira está ativada.

Proteção contra vírus DESATIVADA

A seguinte mensagem será exibida se você desativar a Realtime Protection da Avira ou interromper o serviço Realtime Protection.



Observação

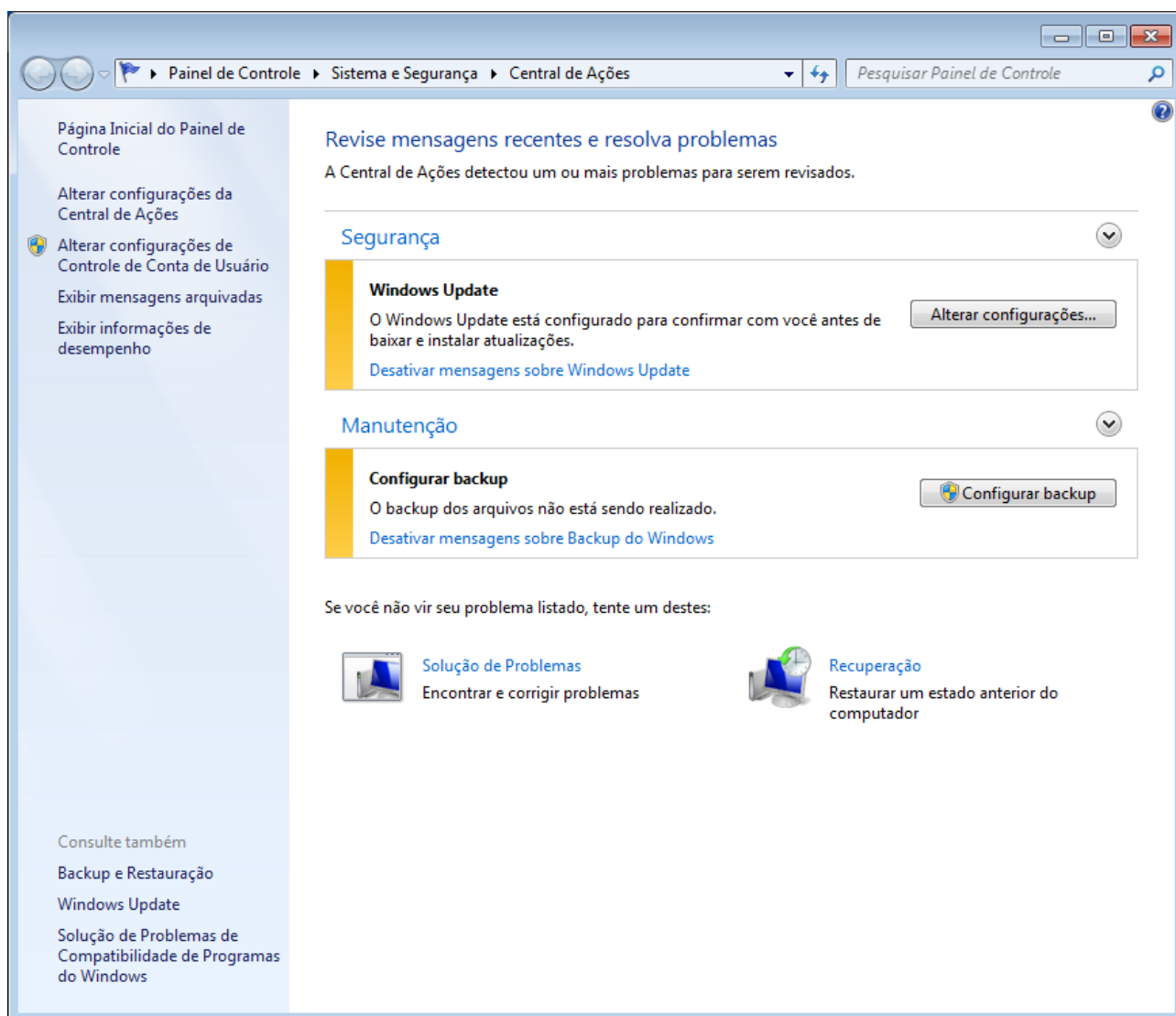
Você pode ativar ou desativar a Realtime Protection na seção Visão geral > Status do Centro de controle. Você também poderá saber se a Realtime Protection da Avira está ativada se o guarda-chuva vermelho em sua barra de tarefas estiver aberto.

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.

Observação

Essa função não é compatível com o Windows Vista.



Observação

A Central de segurança do Windows é compatível com o produto Avira. Você pode ativar essa opção a qualquer momento com o botão **Recomendações**.

Observação

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.

9. Vírus e mais

9.1 Categorias de ameaça

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.

Seu produto Avira detectou Adware. Se a opção **Adware** estiver ativada com uma marca de verificação na configuração, em [Categorias de ameaça](#), você receberá um alerta correspondente se o produto Avira detectar um adware.

Adware/Spyware

Software que exibe 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 produto Avira reconhece "Adware/Spyware". Se a opção **Adware/Spyware** estiver ativada com uma marca de verificação na configuração, em [Categorias de ameaça](#), você receberá um alerta correspondente se o produto Avira detectar um adware ou spyware.

Aplicativo

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

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

Clientes back-door

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 produto Avira 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](#), você receberá um alerta correspondente se o produto Avira detectar esse software.

Discador

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 produto Avira pode detectar os discadores conhecidos por padrão.

Se a opção **Discadores** estiver ativada com uma marca de verificação na configuração, em [Categorias de ameaça](#), 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.

Arquivos com extensão dupla

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

O produto Avira reconhece "Arquivos com extensão dupla". Se a opção **Arquivos com extensão dupla** estiver ativada com uma marca de verificação na configuração, em [Categorias de ameaças](#), você receberá um alerta correspondente se o produto Avira detectar esses arquivos.

Fraudulent software

Conhecido também como "scareware" ou "rogueware", é um software fraudulento que finge que seu computador está infectado por vírus ou malware. Esse software é enganosamente parecido com um software antivírus profissional, mas tem como objetivo levantar incertezas ou amedrontar o usuário. Sua finalidade é fazer as vítimas se sentirem ameaçadas por um perigo iminente (irreal) e fazê-las pagar para eliminar esse perigo. Também há casos em que as vítimas são levadas a acreditar que foram atacadas e recebem instruções para executar uma ação que é, na verdade, o ataque real.

Seu produto Avira detectou uma scareware. Se a opção **Software fraudulento** estiver ativada com uma marca de verificação na configuração, em [Categorias de ameaças](#), você receberá um alerta correspondente se o produto Avira detectar esses arquivos.

Jogos

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 email 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 email, 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 produto Avira 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 produto Avira detectar um jogo. Agora o jogo acabou (literalmente) porque você pode simplesmente excluí-lo.

Piadas

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 produto Avira 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.

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 produto Avira reconhece "Phishing". Se a opção **Phishing** estiver ativada com uma marca de verificação na configuração, em [Categorias de ameaça](#), você receberá um alerta correspondente se o produto Avira detectar esse comportamento.

Programa que viola o domínio privado

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 produto Avira detecta softwares de "Risco de privacidade de segurança". Se a opção **Programas que violam o domínio privado** estiver ativada com uma marca de verificação na configuração, em [Categorias de ameaça](#), você receberá um alerta correspondente se o produto Avira detectar esse software.

Compactadores de tempo de execução incomuns

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

O produto Avira 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](#), você receberá um alerta correspondente se o produto Avira detectar esses compactadores.

9.2 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.

Fraudulent software

Conhecido também como "scareware" ou "rogueware", é um software fraudulento que finge que seu computador está infectado por vírus ou malware. Esse software é enganosamente parecido com um software Antivírus profissional, mas tem como objetivo levantar incertezas ou amedrontar o usuário. Sua finalidade é fazer as vítimas se sentirem

ameaçadas por um perigo iminente (irreal) e fazê-las pagar para eliminar esse perigo. Também há casos em que as vítimas são levadas a acreditar que foram atacadas e recebem instruções para executar uma ação que é, na verdade, o ataque real.

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 email 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 emails, 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 on-line. 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 email, 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.

Rootkits

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 email 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 email 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 emails de phishing.

10. 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](#)

10.1 Endereço de contato

Se você tiver alguma dúvida ou desejar fazer alguma solicitação relacionada aos produtos Avira, teremos prazer em ajudar. Para obter nossos endereços de contato, consulte o Centro de controle em **Ajuda > Sobre Avira Professional Security**.

10.2 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.com/pt-br/professional-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 Avira Professional Security > Informações de licença**. Consulte Informações de licença.
- **Informações da versão.** É possível encontrar a interface do programa no item de menu **Ajuda > Sobre Avira Professional Security > Informações de versão**. Consulte 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.

10.3 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 email para o seguinte endereço:
virus-professional-pt-br@avira.com
Como alguns gateways de email 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.com/pt-br/sample-upload>

10.4 Registrando falso-positivos

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

virus-professional-pt-br@avira.com

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

10.5 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 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 email para o seguinte endereço:

vulnerabilities-professional-pt-br@avira.com

11. Referência: opções de configuração

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

11.1 System Scanner

A seção **System Scanner** da Configuração é responsável pela configuração da verificação sob demanda. (Opções disponíveis somente no modo de especialista.)

11.1.1 Fazer verificação

É possível definir o comportamento da rotina de verificação sob demanda (opções disponíveis somente no modo especialista). Se você selecionar alguns diretórios a serem verificados sob demanda, dependendo da configuração, o System Scanner verificará:

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

Arquivos

O System 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.

Observação

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

Usar 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 Avira 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 arquivos](#), 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.

Observação

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

Usar lista de extensões de arquivos

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**".

Observação

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 arquivos**". As entradas padrão são definidas para as extensões, mas as entradas podem ser adicionadas ou excluídas.

Observação

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 System Scanner verificará somente os setores de inicialização das unidades selecionadas para a verificação do sistema. Essa opção é ativada como configuração padrão.

Fazer a varredura de setores de inicialização principais

Se essa opção for ativada, o System 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.

Observação

Essa opção está disponível somente no Windows Vista e superior. A opção **não** estará disponível se você estiver gerenciando o programa Avira sob AMC.

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 System 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 seu programa Avira for gerenciado com AMC, a opção sempre será exibida e poderá ser ativada: Se o sistema gerenciado não tiver mais de um processador, a opção System Scanner não será usada.

Seguir links simbólicos

Se essa opção for ativada, o System 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.

Observação

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 System 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.

Observação

A verificação de rootkits 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.

Ignorar arquivos e caminhos nas unidades de rede

Se essa opção for ativada, as unidades de rede conectadas ao computador serão excluídas da verificação sob demanda. Essa opção é recomendada quando os servidores ou outras estações de trabalho são protegidos com software antivírus. Essa opção é desativada como configuração padrão.

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 System 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 System 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 System 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 System Scanner continua em execução em segundo plano.

normal

O System Scanner é executado com prioridade normal. Todos os processos recebem do sistema operacional a mesma quantidade de tempo de processador. Essa opção está ativada como a configuração padrão é recomendada. Em algumas circunstâncias, o trabalho com outros aplicativos pode ser afetado.

alto

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

Ação para detecção

Você pode definir as ações a serem realizadas pelo System Scanner quando um vírus ou programa indesejado for detectado. (Opções disponíveis somente no modo especialista.)

Interativo

Se essa opção for ativada, os resultados da verificação do System Scanner serão exibidos em uma caixa de diálogo. Ao realizar uma verificação com o System 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 System Scanner.

Observação

Na caixa de diálogo System Scanner, a ação **Quarentena** é exibida como ação padrão.

Ações permitidas

Nessa caixa de exibição, é possível especificar as ações que podem ser selecionadas na caixa de diálogo caso um vírus seja detectado no modo de notificação individual ou de especialista. Para isso, é necessário ativar as opções correspondentes.

Reparar

O System Scanner repara o arquivo infectado se possível.

Renomear

O System Scanner renomeia o arquivo. Portanto, o acesso direto a esses arquivos (por exemplo, com clique duplo) não é mais possível. O arquivo pode ser reparado posteriormente e renomeado de novo.

Quarentena

O System Scanner move o arquivo para a Quarentena. O arquivo 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. Dependendo do arquivo, outras opções de seleção estão disponíveis no Gerenciador de quarentena.

Excluir

O arquivo será excluído. Esse processo é muito mais rápido do que "substituir e excluir".

Ignorar

O arquivo deve ser ignorado.

Substituir e excluir

O System Scanner substitui o arquivo por um padrão e o exclui. Não é possível restaurá-lo.

Padrão

O botão é usado para definir uma ação padrão a ser realizada pelo System Scanner para manipular os arquivos encontrados. Realce uma ação e clique no botão "**Padrão**". Somente a ação padrão selecionada para os arquivos relevantes pode ser executada no modo de notificação combinado. A ação padrão selecionada para os arquivos relevantes é predefinida no modo de notificação individual e de especialista.

Observação

A ação **reparar** não pode ser selecionada como ação padrão.

Observação

Se você tiver selecionado **Excluir** ou **Substituir e excluir** como ação padrão e desejar definir o modo de notificação como combinado, considere o seguinte: no caso de acessos heurísticos, os arquivos afetados não são excluídos, mas movidos para a quarentena.

Automático

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

Copiar arquivo à quarentena antes da ação

Se essa opção for ativada, o System 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.

Exibir alertas de detecção

Se essa opção for ativada, um alerta será exibida para cada vírus ou programa indesejado detectado, mostrando as ações que estão sendo executadas.

Ação primária

Ação primária é a ação executada quando o System 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.

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 System Scanner reparará os arquivos afetados automaticamente. Se o System Scanner não conseguir reparar um arquivo afetado, realizará a ação selecionada em **Ação secundária**.

Observação

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

Renomear

Se essa opção for ativada, o System 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.

Quarentena

Se essa opção for ativada, o System 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.

Excluir

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

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.

Substituir e excluir

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

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.

Renomear

Se essa opção for ativada, o System 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.

Quarentena

Se essa opção for ativada, o System 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.

Excluir

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

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.

Substituir e excluir

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

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.

Mais ações

Iniciar programa após a detecção

Depois da verificação sob demanda, o System Scanner pode abrir um arquivo de sua preferência (por exemplo, um programa de email) se pelo menos um vírus ou programa indesejado tiver sido detectado para que você possa informar outros usuários ou o administrador. (Opções disponíveis somente no modo de especialista.)

Observação

Por motivos de segurança, só é possível iniciar um programa após uma detecção quando o usuário está conectado no computador. Em seguida, o arquivo é aberto com os direitos aplicáveis ao usuário conectado. Se nenhum usuário estiver conectado, essa opção não será executada.

Nome do programa

Nessa caixa de entrada, é possível inserir o nome e o caminho relevante do programa que deve ser iniciado pelo System Scanner após uma detecção.



Esse botão abre uma janela na qual é possível selecionar o programa desejado com a ajuda da caixa de diálogo de seleção de arquivo.

Argumentos

Nessa caixa de entrada, é possível inserir parâmetros de linha de comando para o programa a ser iniciado, se necessário.

*Registro de eventos***Usar registro de eventos**

Se essa opção for ativada, um relatório de eventos com os resultados da verificação será transferido para o Registro de eventos do Windows após o término de uma verificação do System Scanner. Os eventos podem ser chamados no Visualizador de eventos do Windows. A opção é desativada como configuração padrão. (Opção disponível somente no modo de especialista.)

Arquivos

Ao verificar arquivos compactados, o System 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. (Opções disponíveis somente no modo de especialista.)

Verificar arquivos compactados

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 System 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 System Scanner também descompactará e verificará esse arquivo. Essa opção é ativada como configuração padrão.

Observação

Somente os tipos de arquivo marcados na lista são suportados.

Limitar profundidade da 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.

Observação

Para encontrar um vírus ou programa indesejado em um arquivo, o System 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 profundidade máxima da recursão, a opção [Limitar profundidade da recursão](#) 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 compactados

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

Exceções

Objetos a serem omitidos na verificação (Opções disponíveis somente no modo de especialista)

A lista dessa janela contém arquivos e caminhos que não devem ser incluídos pelo System 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.

Observação

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

Aviso

Esses arquivos não são incluídos em uma verificação.

Observação

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.

Observação

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 System Scanner, D:\folder\file.txt não será excluído da verificação.

Observação

Se o programa Avira estiver sendo gerenciado no AMC, você poderá usar variáveis nos detalhes de caminho para exceções de arquivo. Você pode encontrar uma lista de variáveis que podem ser usadas em [Variáveis: Exceções da Realtime Protection e do System Scanner](#).

Heurística

Essa seção de configuração contém as configurações de heurística do mecanismo de verificação. (Opções disponíveis somente no modo de especialista.)

Os produtos Avira 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 Avira 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 Avira contém uma heurística muito poderosa na forma da tecnologia Avira 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.

11.1.2 Relatório

O System 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. (Opções disponíveis somente no modo de especialista.)

Observação

Para que você possa estabelecer quais ações o System Scanner realizou ao detectar vírus ou programas indesejados, ative o arquivo de relatório na configuração do modo de especialista.

Relatório

Desativado

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

Padrão

Quando essa opção está ativada, o System 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.

Estendido

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

Concluído

Quando essa opção está ativada, o System 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.

Observação

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

11.2 Realtime Protection

A seção **Realtime Protection** da configuração é responsável pela configuração da verificação durante o acesso. (Opções disponíveis somente no modo especialista.)

11.2.1 Fazer verificação

Em geral, você quer monitorar seu sistema constantemente. Para fazer isso, use a Realtime Protection (= System Scanner durante o acesso). Com ele, você pode verificar imediatamente todos os arquivos que são copiados ou abertos no computador em busca de vírus e programas indesejados. (Opções disponíveis somente no modo de especialista.)

Arquivos

A Realtime Protection 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.

Observação

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

Usar 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 de arquivos**, porém é mais seguro visto que não é apenas a extensão do arquivo que é verificada.

Observação

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

Usar lista de extensões de arquivos

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.

Observação

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 arquivos**". As entradas padrão são definidas para as extensões, mas as entradas podem ser adicionadas ou excluídas.

Observação

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

Modo de verificação

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

Fazer verificação ao ler

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

Fazer varredura ao gravar

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

Fazer verificação ao ler e gravar

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

Unidades

Monitorar unidades de rede

Se essa opção for ativada, os arquivos das unidades de rede (unidades mapeadas), como volumes de servidor e unidades pontuais, serão verificados.

Observação

Para não prejudicar muito o desempenho do computador, a opção **Monitorar unidades de rede** deve ser ativada somente em casos excepcionais.

Aviso

Se essa opção for desativada, as unidades de rede **não** serão monitoradas. Não há mais proteção contra vírus ou programas indesejados.

Observação

Quando são executados em unidades de rede, os arquivos são verificados pela Realtime Protection, independentemente da configuração da opção **Monitorar unidades de rede**. Em alguns casos, os arquivos das unidades de rede são verificados quando são abertos, mesmo que a opção **Monitorar unidades de rede** esteja desativada. Motivo: esses arquivos são acessados com os direitos "Executar arquivo". Se desejar excluir esses arquivos ou até mesmo os arquivos executados nas unidades de rede da verificação feita pela Realtime Protection, insira os arquivos na lista de objetos de arquivo a serem excluídos (consulte: [Realtime Protection > Verificar > Exceções](#)).

Ativar armazenamento em cache

Se essa opção for ativada, os arquivos monitorados nas unidades de rede serão disponibilizados no cache da Realtime Protection. O monitoramento das unidades de rede sem a função de armazenamento em cache é mais segura, mas não executa tão bem o monitoramento das unidades de rede com armazenamento em cache.

Arquivos

Verificar arquivos compactados

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.

Observação

Essa opção é desativada por padrão, pois o processo consome muita memória do computador. Geralmente, é recomendado verificar arquivos compactados com uma verificação sob demanda.

Profundidade máxima de recursão

Ao verificar arquivos compactados, a Realtime Protection 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.

Ação para detecção

Você pode definir as ações a serem realizadas pela Realtime Protection quando um vírus ou programa indesejado for detectado. (Opções disponíveis somente no modo especialista.)

Interativo

Se essa opção for ativada, uma notificação de área de trabalho aparecerá quando a Realtime Protection um 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. Essa opção é ativada como configuração padrão.

Ações permitidas

Nesta caixa de exibição, é possível especificar as ações de gerenciamento de vírus que devem ser disponibilizadas como ações adicionais na caixa de diálogo. Para isso, é necessário ativar as opções correspondentes.

Reparar

A Realtime Protection repara o arquivo infectado, se for possível.

Renomear

A Realtime Protection renomeia o arquivo. Portanto, o acesso direto a esses arquivos (por exemplo, com clique duplo) não é mais possível. O arquivo pode ser reparado posteriormente e renomeado de novo.

Quarentena

A Realtime Protection move o arquivo para a pasta Quarentena. O arquivo 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. Dependendo do arquivo, há outras opções de seleção disponíveis no Gerenciador de quarentena.

Excluir

O arquivo será excluído. Esse processo é muito mais rápido do que **Substituir e excluir** (veja abaixo).

Ignorar

O acesso ao arquivo é permitido e o arquivo é ignorado.

Substituir e excluir

A Realtime Protection substitui o arquivo por um padrão antes de excluí-lo. Não é possível restaurá-lo.

Aviso

Se a Realtime Protection estiver definida como **Fazer verificação ao gravar**, o arquivo afetado não será gravado.

Padrão

Esse botão permite selecionar uma ação que é ativada na caixa de diálogo por padrão quando um vírus é detectado. Selecione a ação que deve ser ativada por padrão e clique no botão "**Padrão**".

Observação

A ação **Reparar** não pode ser selecionada como ação padrão.

[Clique aqui para obter mais informações.](#)

Automático

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

Copiar arquivo à quarentena antes da ação

Se essa opção for ativada, a Realtime Protection criará uma cópia de backup antes de executar 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.

Exibir alertas de detecção

Se essa opção for ativada, para cada detecção de um vírus ou programa indesejado, será exibido um alerta.

Ação primária

Ação primária é a ação executada quando a Realtime Protection encontra um vírus ou um 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, a Realtime Protection reparará os arquivos afetados automaticamente. Se a Realtime Protection não conseguir reparar um arquivo afetado, realizará a ação selecionada em **Ação secundária**.

Observação

Um reparo automático é recomendado, mas a Realtime Protection modificará os arquivos na estação de trabalho.

Renomear

Se essa opção for ativada, a Realtime Protection 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.

Quarentena

Se essa opção for ativada, a Realtime Protection 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.

Excluir

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

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.

Substituir e excluir

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

Negar acesso

Se essa opção for ativada, a Realtime Protection inserirá a detecção no [arquivo de relatório](#) somente se a função de relatório estiver ativada. Além disso, a Realtime Protection grava uma entrada no [Registro de eventos](#), se essa opção for ativada.

Aviso

Se a Realtime Protection estiver definida como **Fazer verificação ao gravar**, o arquivo afetado não será gravado.

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.

Renomear

Se essa opção for ativada, a Realtime Protection 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.

Quarentena

Se essa opção for ativada, a Realtime Protection 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.

Excluir

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

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.

Substituir e excluir

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

Negar acesso

Se essa opção for ativada, o arquivo afetado não será gravado; a Realtime Protection inserirá a detecção no [arquivo de relatório](#) somente se a função de relatório estiver ativada. Além disso, a Realtime Protection grava uma entrada no [Registro de eventos](#), se essa opção for ativada.

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.

Mais ações

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 está ativada como a configuração padrão. (Opção disponível somente no modo de especialista.)

Exceções

Com essas opções, é possível configurar objetos de exceção para a Realtime Protection (verificação durante o acesso). Os objetos relevantes não são incluídos na verificação durante o acesso. A Realtime Protection pode ignorar os acessos do arquivo a esses objetos durante a verificação no acesso através da lista de processos a serem omitidos. Isso é útil, por exemplo, com soluções de backup ou de bancos de dados. (Opções disponíveis somente no modo especialista)

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 pela Realtime Protection

Todos os acessos de arquivo dos processos dessa lista são excluídos do monitoramento pela Realtime Protection.

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.

O caminho e o nome de arquivo especificados do processo devem ter no máximo 255 caracteres. Você pode inserir até 128 processos. As entradas da lista devem ter no máximo 6000 caracteres no total.

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

As informações da unidade devem ser inseridas da seguinte forma: [Letra da unidade]:\

O símbolo de dois-pontos (:) é somente usado para especificar unidades.

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

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

É possível excluir processos do monitoramento da Realtime Protection sem detalhes de caminho completos. Por exemplo: `application.exe`

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

Os detalhes de caminho completos são necessários para os processos em que os arquivos executáveis estão localizados nas unidades conectadas, por exemplo, unidades de rede. Observe as informações gerais sobre a notação de [Exceções em unidades de rede conectadas](#).

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.

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 pela Realtime Protection

Todos os acessos de arquivo aos objetos dessa lista são excluídos do monitoramento pela Realtime Protection.

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.

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

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
```

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

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

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
```

O número máximo de exceções sem um caminho completo é 64. Por exemplo:

```
*.log
\computer1\C\directory1
```

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 da Realtime Protection.



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:

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.

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

`C:\Arquivos de programas\Application\application*.exe\`
 Essa entrada não é válida e não é tratada como uma exceção.

Com relação às **exceções nas unidades de rede conectadas** leve em consideração o seguinte: Se você usar a letra de unidade de rede conectada, os arquivos e pastas especificados NÃO serão excluídos da verificação da Realtime Protection. Se o caminho UNC na lista de exceções for diferente do caminho UNC usado para estabelecer conexão com a unidade de rede (especificação do endereço IP na lista de exceções – especificação do nome do computador para conexão com a unidade de rede), os arquivos e pastas especificados NÃO serão excluídos pela verificação da Realtime Protection. Localize o caminho UNC relevante no arquivo de relatório da Realtime Protection:

`\\<Nome do computador>\<Ativar>\ - OU - \\<Endereço IP>\<Ativar>\`

Você pode localizar o caminho usado pela Realtime Protection para verificar os arquivos infectados no arquivo de relatório da Realtime Protection. Indique exatamente o mesmo caminho na lista de exceções. Proceda do seguinte modo: Defina a função de protocolo da Realtime Protection como **Concluído** na configuração em [Realtime Protection > Relatório](#). Em seguida, acesse os arquivos, as pastas, as unidades montadas ou as unidades de rede conectadas com a Realtime Protection ativada. Agora você pode ler o caminho a ser usado no arquivo de relatório da Realtime Protection. O arquivo de relatório pode ser acessado no Centro de controle em [Proteção local > Realtime Protection](#).

Se o produto Avira estiver sendo gerenciado no AMC, você poderá usar variáveis nos detalhes de caminho do processo e exceções de arquivo. Você pode encontrar uma lista de variáveis que podem ser usadas em [Variáveis: Exceções da Realtime Protection e do Scanner](#).

Exemplos de processos a serem excluídos:

- `application.exe`
O processo *application.exe* é excluído da verificação da Realtime Protection, 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 programa1*, é excluído da verificação da Realtime Protection.
- `C:\Arquivos de programas1*.exe`
Todos os processos dos arquivos executáveis localizados no caminho *C:\Arquivos de programa1* são excluídos da verificação da Realtime Protection.

Exemplos de arquivos a serem excluídos:

- `*.mdb`
Todos os arquivos com a extensão “*mdb*” são excluídos da verificação da Realtime Protection.
- `*.xls*`
Todos os arquivos com uma extensão de arquivo começando com '*xls*' são excluídos da verificação da Realtime Protection, 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 da Realtime Protection.
- `\\Nome do computador\Compartilhado1\`
Todos os arquivos são excluídos da verificação da Realtime Protection acessados através de uma conexão com “*\\Nome do computador1\Compartilhado1*”. Geralmente, trata-se de uma unidade de rede conectada que acessa outro computador com uma pasta compartilhada através do nome do computador “*Nome do computador1*” e o nome compartilhado “*Compartilhado1*”.
- `\\1.0.0.0\Compartilhado1*.mdb`
Todos os arquivos com a extensão '*mdb*' são excluídos da verificação da Realtime Protection por meio de uma conexão '*\\1.0.0.0\Compartilhado1*'. Geralmente, trata-se de uma unidade de rede conectada que acessa outro computador com uma pasta compartilhada através do endereço IP “1.0.0.0” e o nome compartilhado '*Compartilhado1*'.

Heurística

Essa seção de configuração contém as configurações de heurística do mecanismo de verificação. (Opções disponíveis somente no modo de especialista.)

Os produtos Avira 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 Avira 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 a AHeAD”

O programa Avira contém uma heurística muito poderosa na forma da tecnologia Avira 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.

11.2.2 ProActiv

O Avira 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 Realtime Protection 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 regra são fornecidos pelos bancos de dados da Avira. O Avira 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.

Observação

A tecnologia ProActiv ainda não está disponível para os sistemas de 64 bits.

Geral (Opções disponíveis somente no modo de especialista.)

Ativar o Avira 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.

Melhore a segurança do seu computador com o Avira ProActiv.

Se essa opção for ativada, o Avira 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 saber mais

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.

Aplicativos bloqueados

Em *Aplicativos a serem bloqueados* é possível inserir os aplicativos classificados como prejudiciais que devem ser bloqueados pelo Avira 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 da Realtime Protection sobre programas com comportamento suspeito selecionando a opção **Sempre bloquear este programa**.

Aplicativos a serem bloqueados

Aplicativo

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 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 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.

Observação

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.

Aplicativos permitidos

A seção *Aplicativos a serem ignorados* 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 da Realtime Protection usando a opção **Programa confiável** na notificação da Realtime Protection.

Aplicativos a serem ignorados

Aplicativo

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 da Realtime Protection. O componente ProActiv identifica aplicativos usando o caminho, o nome do arquivo e o conteúdo. Recomendamos verificar o conteúdo, pois malwares 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 realizada antes de o aplicativo ser excluído do monitoramento pela Realtime Protection. 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.

Observação

Alguns aplicativos confiáveis, incluindo, por exemplo, todos os componentes de aplicativo do produto Avira, 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.

11.2.3 Relatório

A Realtime Protection inclui uma função de registro abrangente para fornecer ao usuário ou administrador observações exatas sobre o tipo e a maneira de uma detecção. (Opções disponíveis somente no modo de especialista.)

Relatório

Este grupo permite determinar o conteúdo do arquivo do relatório.

Desativado

Se essa opção for ativada, a Realtime Protection 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, a Realtime Protection 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.

Estendido

Se essa opção for ativada, a Realtime Protection registrará informações menos importantes no arquivo de relatório também.

Concluído

Se essa opção for ativada, a Realtime Protection 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. 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. Para saber qual é o local de salvamento, consulte [Diretório do relatório](#).

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.

11.3 Variáveis: Exceções da Realtime Protection e do System Scanner

Se seu produto Avira estiver sendo gerenciado com AMC, você poderá usar variáveis para configurar exceções para a Realtime Protection e o System Scanner. Ao salvar a configuração no sistema gerenciado, as variáveis são substituídas automaticamente por valores verdadeiros que correspondem ao sistema operacional e ao idioma.

As seguintes variáveis podem ser usadas:

Variável	Windows XP 32 bits (**inglês)	Windows 7 32 bits (**inglês)	Windows 7 64 bits (**inglês)
%WINDIR%	<i>C:\Windows</i>	<i>C:\Windows</i>	<i>C:\Windows</i>
%SYSDIR%	<i>C:\Windows\System32</i>	<i>C:\Windows\System32</i>	<i>C:\Windows\System32</i>
%ALLUSERSPROFILE%	<i>C:\Documents and Settings\All Users**</i>	<i>C:\ProgramData</i>	<i>C:\ProgramData</i>
%PROGRAMFILES%	<i>C:\Arquivos de programas**</i>	<i>C:\Arquivos de programas**</i>	<i>C:\Arquivos de programas (x86)**</i>
%PROGRAMFILES (x86) %	%PROGRAMFILES (x86) %	%PROGRAMFILES (x86) %	<i>C:\Arquivos de programas (x86)**</i>
%SYSTEMROOT%	<i>C:\Windows</i>	<i>C:\Windows</i>	<i>C:\Windows</i>
%INSTALLDIR%	<i>C:\Arquivos de programas\Avira\Antivir Desktop**</i>	<i>C:\Arquivos de programas\Avira\Antivir Desktop**</i>	<i>C:\Arquivos de programas (x86)\Avira\Antivir Desktop**</i>
%AVAPPDATA%	<i>C:\Documents and Settings\All Users\Avira\AntiVir Desktop**</i>	<i>C:\ProgramData\Avira\AntiVir Desktop</i>	<i>C:\ProgramData\Avira\AntiVir Desktop</i>

Os caminhos marcados com ** dependem do idioma. Os exemplos mencionados acima nomeiam os caminhos relevantes em um sistema operacional em inglês.

11.4 Atualizar

Na seção **Atualizar**, é possível configurar o recebimento automático de atualizações e a conexão aos servidores de download. Você pode especificar vários intervalos de atualização e ativar ou desativar a atualização automática.

Observação

Se você configurar seu produto Avira no Avira Management Console, as atualizações automáticas não estarão disponíveis.

*Atualização automática***Ativar**

Se essa opção for ativada, as atualizações automáticas serão executadas para os eventos ativados no intervalo especificado.

Todo(s) o(s) dia(s) n / hora(s) / minuto(s)

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. (Opção disponível somente no modo de especialista.)

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. (Opção disponível somente no modo de especialista.)

*Fazer download***através do servidor da web**

A atualização é executada através de um servidor da Web usando uma conexão HTTP. Você pode usar um servidor da Web patenteado na Internet ou um servidor da Web em uma intranet, que obtém os arquivos de atualização de um servidor de download patenteado na Internet.

Observação

Você pode acessar outras configurações de atualização através de um servidor da Web em: [Configuração > Proteção local > Atualização > Servidor da web](#). Se essa opção for ativada, você poderá configurar o servidor da Web e, quando necessário, o servidor proxy.

através de servidor de arquivo/pastas compartilhadas

A atualização é realizada através de um servidor de arquivos em uma intranet, que obtém os arquivos de atualização de um servidor de download patenteado na Internet.

Observação

Você pode acessar outras configurações de atualização através de um servidor de arquivos em: [Configuração > Proteção local > Atualização > Servidor de arquivos](#).

Se essa opção for ativada, você poderá configurar o servidor de arquivos que está sendo usado.

11.4.1 Atualização do produto

Em **Atualização do produto**, configure como as atualizações do produto ou a notificação das atualizações devem ser tratadas. (Opções disponíveis somente no modo especialista.)

Atualizações de produto

Fazer o download 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.

Notificar usuário se as atualizações de produto estiverem disponíveis

Se essa opção for ativada, você receberá uma notificação por email 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 por meio de uma janela pop-up e por 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.

Aviso

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 oCapítulo [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](#). (Opções disponíveis somente no modo especialista.)

11.4.2 Reiniciar configurações

Quando uma atualização do produto Avira é realizada, talvez seja necessário reiniciar o sistema do computador. Se tiver selecionado atualizações automáticas do produto em [Proteção local > Atualizar > Atualização do produto](#), você poderá escolher entre as diferentes opções de cancelamento e notificação de reinicialização em **Configurações de reinicialização**. (Opções disponíveis somente no modo de especialista.)

Observação

As configurações de reinicialização permitem escolher entre duas opções para executar uma atualização do produto que requer a reinicialização do computador na configuração em [Proteção local > Atualizar > Atualização do produto](#).

Fazer o download e instalar as atualizações do produto automaticamente:

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.

Baixar atualizações do produto. Se for necessário reiniciar, instalar a atualização após o reinício do sistema; caso contrário, instalar imediatamente:

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 o computador após n segundos (com mensagens de contagem regressiva, sem possibilidade de cancelamento)

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.

Lembrete periódico para reiniciar

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.

11.4.3 Servidor de arquivos

Caso haja mais de uma estação de trabalho em uma rede, o produto Avira poderá baixar uma atualização de um servidor de arquivos na intranet que, por sua vez, obterá os arquivos de atualização de um servidor de download patentado na Internet. Isso garante que o produto Avira esteja atualizado em todas as estações de trabalho.

Observação

O título Configuração só poderá ser ativado se em [Configuração > Geral > Atualização do produto](#) a opção **através de servidor de arquivo/pastas compartilhadas** tiver sido selecionada.

Fazer download

Insira o nome do servidor de arquivos no qual estão localizados os arquivos de atualização do produto Avira e os diretórios "/release/update/" desejados. O seguinte

deve ser especificado: file:///release/update/. O diretório “release” deve ser um diretório que possa ser acessado por todos os usuários.



O botão abre uma janela na qual é possível selecionar o diretório de download desejado.

Login do servidor

Nome de login

Insira seu nome de usuário para fazer login no servidor. Use uma conta de usuário com direitos de acesso para as pastas compartilhadas usadas no servidor.

Senha de login

Insira a senha da conta de usuário. Os caracteres inseridos são mascarados com *.

Observação

Se nenhum dado for especificado na seção Login do servidor, nenhuma autenticação será realizada no servidor de arquivos durante o acesso. Nesse caso, o usuário deve ter direitos suficientes para o servidor de arquivos.

11.4.4 Servidor da Web

A atualização pode ser realizada diretamente através de um servidor da Web na Internet ou na intranet. (Opções disponíveis somente no modo de especialista.)

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.

Password

Insira a senha dessa conta. Por motivos de segurança, os caracteres reais digitados neste espaço são substituídos por asteriscos (*).

Observação

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.

Observação

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 discada estabelecida para a atualização será interrompida automaticamente mais uma vez assim que o download tiver sido concluído.

Observação

Essa opção não está disponível no Windows Vista e no Windows 7. Nesses sistemas operacionais, a conexão discada aberta para a atualização sempre é encerrada assim que o download é executado.

*Fazer download***Servidor de prioridade**

Neste campo, insira o diretório de atualização e o URL do servidor da Web que será solicitado primeiro para fornecer a atualização. Se esse servidor não puder ser contatado, os servidores padrão indicados serão usados. O formato do endereço do servidor da Web é o seguinte: `http://<endereço do servidor da Web>[:Porta]/update`. Se você não especificar uma porta, será usada a porta 80.

Valores padrão

Insira os endereços (URL) dos servidores da Web a partir dos quais as atualizações e o diretório "update" desejado devem ser carregados. O formato do endereço do servidor da Web é o seguinte: `http://<endereço do servidor da Web>[:Porta]/update`. Se você não especificar uma porta, será usada a porta 80. Por padrão, os servidores da Web acessíveis são especificados para a atualização da Avira. No entanto, você pode usar seus próprios servidores da Web na intranet corporativa. Se vários servidores da Web forem especificados, separe cada um por vírgula.

Padrão

O botão restaura os endereços predefinidos.

Configurações de 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 proxy

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 proxy** 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

11.5 Firewall

A seção **FireWall** em **Proteção on-line > Configuração** é responsável pela configuração do componente Avira FireWall.

11.5.1 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. (Opções disponíveis somente no modo de especialista.)

- [Protocolo ICMP](#)
- [Verificação da porta TCP](#)
- [Verificação da porta UDP](#)
- [Regras de entrada](#)
- [Regra de protocolo IP de entrada](#)
- [Regras de saída](#)
- [Botões para gerenciar as regras](#)

Uma regra de adaptador predefinida depende do nível de segurança. Você pode alterar o *Nível de segurança* em **Proteção on-line > FireWall** no Centro de controle ou definir suas próprias regras do adaptador. Se você tiver definido suas próprias regras do adaptador, o *Nível de segurança* na seção **FireWall** do Centro de controle será definido como **Personalizado**.

Observação

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	Regras
Baixo	<p>Tipos de entrada bloqueados: nenhum tipo.</p> <p>Tipos de saída bloqueados: nenhum tipo.</p> <p>Assumir inundaçãõ se o atraso entre pacotes for menor do que 50 ms.</p> <p>Rejeitar pacotes ICMP fragmentados.</p>
Médio	Mesma regra do nível Inferior.
Alto	<p>Tipos de entrada bloqueados: vários tipos</p> <p>Tipos de saída bloqueados: vários tipos</p> <p>Assumir inundaçãõ se o atraso entre pacotes for menor do que 50 ms.</p> <p>Rejeitar pacotes ICMP fragmentados.</p>

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.

Assumir inundaçãõ

Com o mouse, clique no link para exibir uma caixa de diálogo na qual é possível inserir o atraso máximo permitido de ICMP. Exemplo: 50 milissegundos.

Pacotes ICMP fragmentados

Com o mouse, clique no link e escolha "**Rejeitar**" ou "**Não rejeitar**" 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	Regras
Baixo	Assumirá a Verificação da porta TCP se 50 ou mais portas tiverem sido verificadas em 5.000 milissegundos. Quando detectado, registra o IP do invasor e não adiciona a regra para bloquear o ataque.
Médio	Assumirá a Verificação da porta TCP se 50 ou mais portas tiverem sido verificadas em 5.000 milissegundos. Quando detectado, registra o IP do invasor e adiciona a regra para bloquear o ataque.
Alto	Mesma regra do nível Médio.

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.

Banco de dados de evento

Com o mouse, clique no link para escolher "**registrar**" ou "**não registrar**" o endereço IP do invasor.

Regra

Com o mouse, clique no link para escolher "**adicionar**" ou "**não adicionar**" 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

Configuração	Regras
Baixo	Assumirá a verificação da porta UDP se 50 ou mais portas tiverem sido verificadas em 5.000 milissegundos. Quando detectado, registra o IP do invasor e não adiciona a regra para bloquear o ataque.
Médio	Assumirá a Verificação da porta UDP se 50 ou mais portas tiverem sido verificadas em 5.000 milissegundos. Quando detectado, registra o IP do invasor e adiciona a regra para bloquear o ataque.
Alto	Mesma regra do nível Médio.

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.

Banco de dados de evento

Com o mouse, clique no link para escolher "**registrar**" ou "**não registrar**" o endereço IP do invasor.

Regra

Com o mouse, clique no link para escolher "**adicionar**" ou "**não adicionar**" a regra para bloquear o ataque de verificação da porta UDP.

Regras de entrada

As regras de entrada são definidas para controlar o tráfego de entrada do Avira FireWall.

Aviso

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 de TCP

Configuração	Regras
Baixo	Nenhum tráfego de dados de entrada é bloqueado pelo Avira FireWall.
Médio	<p>Permitir conexões TCP estabelecidas em 135 Permitir pacotes TCP do endereço 0.0.0.0 com a máscara 0.0.0.0 se as portas locais estiverem em {135} e a porta remota estiver em {0-65535}. Aplicar aos pacotes de conexões existentes. Não registrar quando o pacote corresponder à regra. Avançado: Descartar pacotes que possuem os seguintes bytes com a máscara no deslocamento 0.</p> <p>Negar pacotes TCP em 135 Negar pacotes TCP do endereço 0.0.0.0 com a máscara 0.0.0.0 se a porta local estiver em {135} e a porta remota estiver em {0-65535}. Aplicar a todos os pacotes. Não registrar quando o pacote corresponder à regra. Avançado: Descartar pacotes que possuem os seguintes bytes com a máscara no deslocamento 0.</p> <p>Monitor de tráfego de integridade TCP Permitir pacotes TCP do endereço 0.0.0.0 com a máscara 0.0.0.0 se a porta local estiver em {0-65535} e a porta remota estiver em {0-65535}. Aplicar ao início da conexão e aos pacotes de conexão existentes. Não registrar quando o pacote corresponder à regra. Avançado: Selecionar os pacotes que possuem os seguintes bytes com a máscara no deslocamento 0.</p> <p>Descartar tráfego TCP Negar pacotes TCP do endereço 0.0.0.0 com a máscara 0.0.0.0 se a porta local estiver em {0-65535} e a porta remota estiver em {0-65535}. Aplicar a todos os pacotes. Não registrar quando o pacote corresponder à regra. Avançado: Selecionar os pacotes que possuem os seguintes bytes com a máscara no deslocamento 0.</p>

Alto	<p>Tráfego TCP estabelecido pelo monitor Permitir pacotes TCP do endereço 0.0.0.0 com a máscara 0.0.0.0 se a porta local estiver em {0-65535} e a porta remota estiver em {0-65535}. Aplicar aos pacotes de conexões existentes. Não registrar quando o pacote corresponder à regra. Avançado: Selecionar os pacotes que possuem os seguintes bytes com a máscara no deslocamento 0.</p>
-------------	---

Permitir/Negar 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 IPv4 ou IPv6 obrigatório.

Máscara IP

Ao clicar neste link com o mouse, uma caixa de diálogo será exibida na qual é possível inserir a máscara IPv4 ou IPv6 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 nesse link para escolher aplicar a regra para "**início da conexão e pacotes de conexão existentes**" ou somente para "**pacotes de conexões existentes**" ou para "**todos os pacotes**".

Banco de dados de evento

Ao clicar no link com o mouse, você poderá escolher "**Registrar**" ou "**Não registrar**" no banco de dados de eventos, caso o pacote esteja em conformidade com a regra.

Avançado

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: bytes

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	Regras
Baixo	-
Médio	<p>Monitor de tráfego aceito UDP Permitir pacotes UDP do endereço 0.0.0.0 com a máscara 0.0.0.0 se a porta local estiver em {0- 66535} e a porta remota estiver em {0-66535}. Aplicar regra às portas abertas para todos os fluxos. Não registrar quando o pacote corresponder à regra. Avançado: Descartar pacotes que possuem os seguintes bytes com a máscara no deslocamento 0.</p> <p>Descartar tráfego UDP Negar pacotes UDP do endereço 0.0.0.0 com a máscara 0.0.0.0 se a porta local estiver em {0-65535} e a porta remota estiver em {0-65535}. Aplicar regra a todas as portas para todos os fluxos. Não registrar quando o pacote corresponder à regra. Avançado: Selecionar os pacotes que possuem os seguintes bytes com a máscara no deslocamento 0.</p>

Alto	<p>Tráfego UDP estabelecido pelo monitor</p> <p>Permitir pacotes UDP do endereço 0.0.0.0 com a máscara 0.0.0.0 se a porta local estiver em {0-65535} e a porta remota estiver em {53, 67, 68, 123}. Aplicar regra às portas abertas para todos os fluxos.</p> <p>Não registrar quando o pacote corresponder à regra.</p> <p>Avançado: Descartar pacotes que possuem os seguintes bytes com a máscara no deslocamento 0.</p>
-------------	---

Permitir/Negar 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 IPv4 ou IPv6 obrigatório.

Máscara IP

Ao clicar neste link com o mouse, uma caixa de diálogo será exibida na qual é possível inserir a máscara IPv4 ou IPv6 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

Portas

Com o mouse, clique neste link para aplicar esta regra a todas as portas ou somente a todas as portas abertas.

Fluxos

Ao clicar nesse link com o mouse, você terá a opção de aplicar essa regra a todos os fluxos ou somente aos fluxos de saída.

Banco de dados de evento

Ao clicar no link com o mouse, você poderá escolher "**Registrar**" ou "**Não registrar**" no banco de dados de eventos, caso o pacote esteja em conformidade com a regra.

Avançado

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: bytes

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 de ICMP

Configuração	Regras
Baixo	-
Médio	<p>Não descartar ICMP com base em endereço IP Permitir pacotes ICMP do endereço 0.0.0.0 com a máscara 0.0.0.0. Não registrar quando o pacote corresponder à regra. Avançado: Descartar pacotes que possuem os seguintes bytes com a máscara no deslocamento 0.</p>
Alto	Mesma regra do nível intermediário.

Permitir/Negar 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 IPv4 obrigatório.

Máscara IP

Ao clicar neste link com o mouse, uma caixa de diálogo será exibida na qual é possível inserir a máscara IPv4 obrigatória.

Banco de dados de evento

Ao clicar no link com o mouse, você poderá escolher "**Registrar**" ou "**Não registrar**" no banco de dados de eventos, caso o pacote esteja em conformidade com a regra.

Avançado

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: bytes

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	Regras
Baixo	-
Médio	-
Alto	Negar todos os pacotes IP Negar pacotes IPv4 do endereço 0.0.0.0 com a máscara 0.0.0.0 . Não registrar quando o pacote corresponder à regra.

Permitir/Negar

Ao clicar no link com o mouse, você pode decidir se aceitará ou rejeitará pacotes IP com definição especial.

IPv4/IPv6

Ao clicar no link com o mouse, você pode escolher IPv4 ou IPv6.

Endereço IP

Ao clicar neste link com o mouse, uma caixa de diálogo será exibida na qual é possível inserir o endereço IPv4 ou IPv6 obrigatório.

Máscara IP

Ao clicar neste link com o mouse, uma caixa de diálogo será exibida na qual é possível inserir a máscara IPv4 ou IPv6 obrigatória.

Banco de dados de evento

Ao clicar no link com o mouse, você poderá decidir se gravará ou não no banco de dados de eventos caso o pacote esteja em conformidade com a regra.

Regra de protocolo IP de entrada

É possível definir uma regra para o Protocolo IP de entrada ou saída. Consulte Adicionar nova regra.

Permitir/Negar

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 IPv4 ou IPv6 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 IP

Ao clicar neste link com o mouse, uma caixa de diálogo será exibida na qual é possível inserir o protocolo IP obrigatório.

Banco de dados de evento

Ao clicar no link com o mouse, você poderá escolher "**Registrar**" ou "**Não registrar**" no banco de dados de eventos, caso o pacote esteja em conformidade com a regra.

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, TCP. Consulte Adicionar nova regra.

Aviso

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 para gerenciar as regras

Botão	Descrição
Adicionar regra	Permite criar uma nova regra. Se pressionar esse botão, a caixa de diálogo Adicionar nova regra será aberta. Nessa caixa de diálogo, é possível selecionar novas regras.
Remover regra	Remove a regra selecionada.
Regra acima	Move a regra selecionada uma linha para cima, isto é, aumenta a prioridade da regra.
Regra abaixo	Move a regra selecionada uma linha para baixo, isto é, diminui a prioridade da regra.
Renomear regra	Permite dar outro nome à regra selecionada.

Observação

Você pode adicionar novas regras para adaptadores individuais ou para todos os adaptadores presentes no computador. Para adicionar uma regra de adaptador a todos os adaptadores, selecione **Meu computador**, na hierarquia de adaptador exibida, e clique no botão **Adicionar regra**. Consulte Adicionar nova regra.

Observação

Para alterar a posição de uma regra, você também pode usar o mouse para arrastar a regra até a posição desejada.

11.5.2 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.

Aplicativo

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

Coluna	Descrição
Aplicativo	Nome do aplicativo.
Conexões ativas	Número de conexões ativas abertas pelo aplicativo.
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 Perguntar , Permitir ou Negar . Perguntar é a ação padrão.

Configuração avançada

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 avançada das regras do aplicativo, primeiro ative a opção **Modo de especialista** na janela **Configuração**.
- ▶ Em seguida, acesse **Configuração > Proteção on-line > FireWall > Configurações** e ative a opção **Configurações avançadas** em *Regras de aplicativo*.
- ▶ Salve a configuração clicando em **Aplicar** ou **OK**.
 - ↪ Na seção **Configuração > Proteção on-line > FireWall > Regras de aplicativo**, uma coluna adicional com o cabeçalho **Filtragem** será exibida na lista de regras de aplicativo, com a entrada **Básica** para cada aplicativo.

Coluna	Descrição
Aplicativo	Nome do aplicativo.
Conexões ativas	Número de conexões ativas abertas pelo aplicativo.
Ação	<p>Mostra a ação que o Avira FireWall executará automaticamente quando o aplicativo estiver usando a rede, independentemente do tipo de uso de rede.</p> <p>Se você escolher Básica na coluna Filtragem, poderá clicar no link para selecionar outro tipo de ação. Os valores são Perguntar, Permitir ou Negar.</p> <p>Se você escolher Avançado na coluna Filtragem, o tipo de ação Regras será exibido. O link Regras abre a janela Regras de aplicativo avançadas, na qual é possível inserir regras específicas para o aplicativo.</p>
Filtragem	<p>Mostra o tipo de filtragem. Você pode selecionar outro tipo de filtragem clicando no link.</p> <p>Básica na filtragem simples, a ação especificada é realizada em todas as atividades de rede executadas pelo software.</p> <p>Avançado: com esse tipo de filtragem, as regras que foram adicionadas à configuração estendida são aplicadas.</p>

- ▶ Se você quiser 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 avançada

Com as regras de aplicativo especificadas, você pode permitir ou negar o tráfego de dados especificado para o aplicativo ou pode permitir ou negar a escuta passiva de portas individuais. As seguintes opções estão disponíveis:

Permitir/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/Negar a escuta passiva do aplicativo nas portas

Permitir/Negar tráfego

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 em Regras de aplicativo avançadas).

Observação

Se você alternar a filtragem de **Avançado** para **Básico** de uma regra de aplicativo, as regras de aplicativo já existentes na configuração avançada serão simplesmente desativadas, e não excluídas de modo permanente. Ao selecionar a filtragem **Avançada** novamente, as regras de aplicativo avançadas existentes serão reativadas e exibidas na configuração estendida da janela de configuração das **Regras de aplicativo**.

Detalhes do aplicativo

Nesta caixa, é possível ver os detalhes do aplicativo selecionado na caixa de listagem de aplicativos.

- *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.

Mostrar detalhes	A janela " Propriedades " exibe os detalhes do aplicativo selecionado na caixa de listagem do aplicativo. (Opção disponível somente no modo de especialista)
Recarregar	Recarrega a lista de aplicativos e, ao mesmo tempo, descarta as alterações que acabaram de ser feitas.

11.5.3 Fornecedores confiáveis

Uma lista de fabricantes de software confiáveis é exibida em **Fornecedores confiáveis**. (Opções disponíveis somente no modo de especialista.)

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 criados por 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 Aplicar ou OK na janela de configuração.
Recarregar	As alterações feitas são desfeitas. A última lista salva é carregada.

Observação

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.

Observação

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.

11.5.4 Configurações

Opções disponíveis somente no modo de especialista.

Opções avançadas

Ativar o 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.

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. Na caixa, é possível especificar o número de segundos antes de a regra ser removida.

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](#).

Configurações 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.

11.5.5 Configurações de pop-up

Opções disponíveis somente no modo de especialista.

Inspecionar pilha de inicialização de processo

Se essa opção estiver ativada, a inspeção da pilha do 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.

Lembrar ação para este aplicativo

Sempre ativado

Quando essa opção estiver ativada, a opção "**Lembrar ação para este aplicativo**" da caixa de diálogo "**Evento de rede**" será ativada como configuração padrão.

Sempre desativado

Quando essa opção estiver ativada, a opção "**Lembrar ação para este aplicativo**" da caixa de diálogo "**Evento de rede**" será desativada como configuração padrão.

Ativado para aplicativos assinados

Quando essa opção estiver ativada, a opção "**Lembrar ação para este aplicativo**" da caixa de diálogo "**Evento de rede**" será ativada automaticamente durante o acesso à rede por parte dos aplicativos assinados. Aplicativos assinados são distribuídos por supostos "fornecedores confiáveis" (consulte [Fornecedores confiáveis](#)).

Lembrar último estado usado

Quando essa opção estiver ativada, a opção "**Lembrar ação para este aplicativo**" da caixa de diálogo "**Evento de rede**" será 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.

11.6 Firewall no SMC

O FireWall é configurado para atender aos requisitos específicos de uma administração por meio do Avira Management Console. Existem opções e restrições estendidas para opções de configuração individuais:

- As configurações do FireWall se aplicam a todos os usuários do computador cliente
- Regras do adaptador: os níveis de segurança para adaptadores individuais podem ser definidos com menus de contexto
- Regras de aplicativo: o acesso à rede por parte dos aplicativos pode ser permitido ou negado. Não é possível criar regras específicas do aplicativo.

Se o produto Avira for gerenciado pelo Avira Management Console, as seguintes opções de configuração do FireWall do Centro de controle nos computadores cliente serão desativadas:

- Configuração dos níveis de segurança do FireWall
- Configuração de regras de adaptador e de aplicativo

11.6.1 Configurações gerais

Opções disponíveis somente no modo de especialista.

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.

Modo de aprendizado

Se a opção estiver ativada, o modo de aprendizado do Avira FireWall será ativado.

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.

Regras genéricas do adaptador

Optionen nur bei aktiviertem Expertenmodus verfügbar.

As conexões de rede que foram configuradas são adaptadores designados. As regras do adaptador podem ser elaboradas para as seguintes conexões de rede de cliente:

- Adaptador **padrão**: LAN ou Internet de alta velocidade
- **Sem fio**
- Conexão **discada**

No menu de contexto do adaptador (na janela **Regras genéricas de adaptador**, clique com o botão direito do mouse em **Meu computador** ou **Padrão, Sem fio, Discada** etc.) é possível especificar regras do adaptador predefinidas para cada adaptador disponível:

- **Definir o nível de segurança como Baixo**
- **Definir o nível de segurança como Médio**
- **Definir o nível de segurança como Alto**

Você também pode modificar regras de adaptador individuais de acordo com suas necessidades.

Observação

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

- [Protocolo ICMP](#)
- [Verificação da porta TCP](#)
- [Verificação da porta UDP](#)
- [Regras de entrada](#)
- [Regra de protocolo IP de entrada](#)
- [Regras de saída](#)
- [Botões para gerenciar as regras](#)

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	Regras
Baixo	Tipos de entrada bloqueados: nenhum tipo . Tipos de saída bloqueados: nenhum tipo . Assumir inundação se o atraso entre pacotes for menor do que 50 ms . Rejeitar pacotes ICMP fragmentados.
Médio	Mesma regra do nível inferior.
Alto	Tipos de entrada bloqueados: vários tipos Tipos de saída bloqueados: vários tipos Assumir inundação se o atraso entre pacotes for menor do que 50 ms . Rejeitar 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	Regras
Baixo	Assumirá a verificação da porta TCP se 50 ou mais portas tiverem sido verificadas em 5.000 milissegundos. Quando detectado, registra o IP do invasor e não adiciona a regra para bloquear o ataque.
Médio	Assumirá a verificação da porta TCP se 50 ou mais portas tiverem sido verificadas em 5.000 milissegundos. Quando detectado, registra o IP do invasor e adiciona a regra para bloquear o ataque.
Alto	Mesma regra do nível intermediário.

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

Configuração	Regras
Baixo	Assumirá a verificação da porta UDP se 50 ou mais portas tiverem sido verificadas em 5.000 milissegundos. Quando detectado, registra o IP do invasor e não adiciona a regra para bloquear o ataque.
Médio	Assumirá a verificação da porta UDP se 50 ou mais portas tiverem sido verificadas em 5.000 milissegundos. Quando detectado, registra o IP do invasor e adiciona a regra para bloquear o ataque.
Alto	Mesma regra do nível intermediário.

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.

11.6.2 Regras de entrada

As regras de entrada são definidas para controlar o tráfego de entrada do Avira FireWall.

Aviso

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 de TCP

Configuração	Regras
Baixo	Nenhum tráfego de dados de entrada é bloqueado pelo Avira FireWall.

<p>Médio</p>	<ul style="list-style-type: none"> <p>• Permitir conexões TCP estabelecidas em 135 Permitir pacotes TCP do endereço 0.0.0.0 com a máscara 0.0.0.0 se as porta local estiverem em {135} e as portas remotas em {0-65535}. Aplicar aos pacotes de conexões existentes. Não registrar quando o pacote corresponder à regra. Avançado: descartar pacotes que possuem os seguintes bytes com a máscara no deslocamento 0.</p> <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 com a máscara no deslocamento 0.</p> <p>• Monitorar tráfego de dados de integridade TCP Permitir pacotes TCP do endereço 0.0.0.0 com a máscara 0.0.0.0 se as porta local estiverem em {0-65535} e as portas remotas em {0-65535}. Aplicar ao início da conexão e aos pacotes de conexão existentes. Não registrar quando o pacote corresponder à regra. Avançado: Descartar pacotes que possuem os seguintes bytes com a máscara no deslocamento 0.</p> <p>• Negar todos os pacotes TCP Negará pacotes TCP do endereço 0.0.0.0 com a máscara 0.0.0.0 se as portas locais estiverem no intervalo {0-65535} e a porta remota estiver no intervalo {0-65535}. Aplicar a todos os pacotes. Não registrar quando o pacote corresponder à regra. Avançado: Descartar pacotes que possuem os seguintes bytes com a máscara no deslocamento 0.</p>
---------------------	--

Alto	Tráfego dos dados TCP estabelecido pelo monitor Permitir pacotes TCP do endereço 0.0.0.0 com a máscara 0.0.0.0 se as porta local estiverem em {0-65535} e as portas remotas em {0-65535} . Aplicar aos pacotes de conexões existentes . Não registrar quando o pacote corresponder à regra. Avançado: Descartar pacotes que possuem os seguintes bytes com a máscara no deslocamento 0 .
-------------	---

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 IPv4 ou IPv6 obrigatório.

Máscara IP

Ao clicar neste link com o mouse, uma caixa de diálogo será exibida na qual é possível inserir a máscara IPv4 ou IPv6 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	Regras
Baixo	-
Médio	<ul style="list-style-type: none"> Monitorar tráfego de dados aceito de UDP Permitir pacotes UDP do endereço 0.0.0.0 com a máscara 0.0.0.0 se as porta local estiverem em {0- 66535} e as portas remotas estiverem em {0-66535}. Aplicar regra às portas abertas. Não registrar quando o pacote corresponder à regra. Avançado: Descartar pacotes que possuem os seguintes bytes com a máscara no deslocamento 0. Negar todos os pacotes UDP Negará pacotes UDP do endereço 0.0.0.0 com a máscara 0.0.0.0 se as porta local estiverem no intervalo {0-65535} e a porta remota estiver no intervalo {0-65535}. Aplicar a todas as portas. Não registrar quando o pacote corresponder à regra. Avançado: Descartar pacotes que possuem os seguintes bytes com a máscara no deslocamento 0.

Alto	<p>UDP estabelecido pelo monitor tráfego</p> <p>Permitir pacotes UDP do endereço 0.0.0.0 com a máscara 0.0.0.0 se as porta local estiverem no intervalo {0-65535} e as portas remotas estiverem no intervalo {53, 67, 68, 123}.</p> <p>Aplicar regra às portas abertas.</p> <p>Não registrar quando o pacote corresponder à regra.</p> <p>Avançado: Descartar pacotes que possuem os seguintes bytes com a máscara no deslocamento 0.</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 IPv4 ou IPv6 obrigatório.

Máscara IP

Ao clicar neste link com o mouse, uma caixa de diálogo será exibida na qual é possível inserir a máscara IPv4 ou IPv6 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

Configuração	Regras
Baixo	-
Médio	<p>Não descartar ICMP com base em endereço IP</p> <p>Permitir pacotes ICMP do endereço 0.0.0.0 com a máscara 0.0.0.0.</p> <p>Não registrar quando o pacote corresponder à regra.</p> <p>Avançado: Descartar pacotes que possuem os seguintes bytes com a máscara no deslocamento 0.</p>
Alto	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 IPv4 ou IPv6 obrigatório.

Máscara IP

Ao clicar neste link com o mouse, uma caixa de diálogo será exibida na qual é possível inserir a máscara IPv4 ou IPv6 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	Regras
Baixo	-
Médio	-
Alto	Negar todos os pacotes IP Negar pacotes IP do endereço 0.0.0.0 com a máscara 0.0.0.0 . Não registrar quando o pacote corresponder 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 IPv4 ou IPv6 obrigatório.

Máscara IP

Ao clicar neste link com o mouse, uma caixa de diálogo será exibida na qual é possível inserir a máscara IPv4 ou IPv6 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.

Regra de protocolo IP de entrada

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 IPv4 ou IPv6 obrigatório.

Máscara IP

Ao clicar neste link com o mouse, uma caixa de diálogo será exibida na qual é possível inserir a máscara IPv4 ou IPv6 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.

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. Consulte Adicione nova regra.

Aviso

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 para gerenciar as regras

Botão	Descrição
Adicionar regra	Permite criar uma nova regra. Se você pressionar esse botão, a caixa de diálogo " Adicionar nova regra " será aberta. Nessa caixa de diálogo, é possível selecionar novas regras.
Remover regra	Remove a regra selecionada.
Regra acima	Move a regra selecionada uma linha para cima, isto é, aumenta a prioridade da regra.
Regra abaixo	Move a regra selecionada uma linha para baixo, isto é, diminui a prioridade da regra.
Renomear regra	Permite dar outro nome à regra selecionada.

Observação

Você pode adicionar novas regras para adaptadores individuais ou para todos os adaptadores presentes no computador. Para adicionar uma regra de adaptador a todos os adaptadores, selecione **Meu computador**, na hierarquia de adaptador exibida, e clique no botão **Adicionar regra**. Consulte Adicionar nova regra.

Observação

Para alterar a posição de uma regra, você também pode usar o mouse para arrastar a regra até a posição desejada.

11.6.3 Lista de aplicativos

Você pode usar a lista de aplicativos para criar regras que especificam como os aplicativos acessam as redes. É possível adicionar aplicativos às listas e definir as regras **Permitir** e **Negar** para o aplicativo selecionado usando um menu de contexto:

- O acesso às redes por parte dos aplicativos com a regra **Permitir** é permitido.
- O acesso às redes por parte dos aplicativos com a regra **Negar** é negado.

Quando os aplicativos são adicionados, a regra **Permitir** é definida.

Lista de aplicativos

Esta tabela mostra a lista dos aplicativos para os quais as regras são definidas. Os símbolos indicam se o acesso à rede é permitido ou negado para os aplicativos. As regras dos aplicativos podem ser alteradas com um menu de contexto.

Botões

Botão	Descrição
Adicionar por caminho	Esse botão abre uma caixa de diálogo na qual é possível selecionar aplicativos. O aplicativo é adicionado à lista de aplicativos com a regra "Permitir" . Se você usar a opção "Adicionar por caminho" , o aplicativo de FireWall adicionado será identificado pelo caminho e nome do arquivo. As regras para um aplicativo permanecem válidas e serão usadas pelo FireWall, mesmo que o conteúdo de um arquivo executável adicionado tenha sido alterado, por exemplo por uma atualização.
Adicionar por md5	Esse botão abre uma caixa de diálogo na qual é possível selecionar aplicativos. O aplicativo é adicionado à lista de aplicativos com a regra "Permitir" . Se você usar a opção "Adicionar por md5" , todos os aplicativos adicionados serão identificados exclusivamente com a soma de verificação MD5. Isso permite que o FireWall identifique as alterações no conteúdo do arquivo. Se um aplicativo mudar após uma atualização, por exemplo, o aplicativo com a regra em questão será removido automaticamente da lista de aplicativos. Depois de uma alteração, o aplicativo deve ser adicionado à lista novamente e a regra desejada deve ser reaplicada.
Adicionar grupo	Esse botão abre uma caixa de diálogo na qual é possível selecionar um diretório. Todos os aplicativos no caminho selecionado são adicionados à lista de aplicativos com a regra "Permitir" .
Remover	A regra de aplicativo selecionada é removida.
Remover tudo	Todas as regras de aplicativo são removidas.

11.6.4 Fornecedores confiáveis

Uma lista de fabricantes de software confiáveis é exibida em **Fornecedores confiáveis**. Os aplicativos dos fabricantes de software listados poderão acessar a rede. Você pode adicionar e remover fabricantes da lista.

Fornecedores

A lista mostra todos os fornecedores classificados como confiáveis.

Botões

Botão	Descrição
Adicionar	Esse botão abre uma caixa de diálogo na qual é possível selecionar aplicativos. O fabricante do aplicativo é estabelecido e adicionado à lista de fornecedores confiáveis.
Adicionar grupo	Esse botão abre uma caixa de diálogo na qual é possível selecionar um diretório. Os fabricantes de todos os aplicativos no caminho selecionado são estabelecidos e adicionados à lista de fornecedores confiáveis.
Remover	A entrada destacada é removida da lista de fornecedores confiáveis. Para remover o fornecedor selecionado permanentemente da lista, clique em " Aplicar " ou " OK " na janela de configuração.
Remover tudo	Todas as entradas são removidas da lista de fornecedores confiáveis.
Recarregar	As alterações feitas são desfeitas. A última lista salva é carregada.

Observação

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**.

Observação

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.

11.6.5 Outras configurações

Opções disponíveis somente no modo de especialista.

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.

Configurações de pop-up

Inspeccionar 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.

11.6.6 Configurações de exibição

Opções disponíveis somente no modo de especialista.

Lembrar ação para este aplicativo

Sempre ativado

Quando essa opção estiver ativada, a opção "**Lembrar ação para este aplicativo**" da caixa de diálogo "**Evento de rede**" será ativada como configuração padrão. Essa opção é ativada como configuração padrão.

Sempre desativado

Quando essa opção estiver ativada, a opção "**Lembrar ação para este aplicativo**" da caixa de diálogo "**Evento de rede**" será desativada como configuração padrão.

Ativado para aplicativos assinados

Quando essa opção estiver ativada, a opção "**Lembrar ação para este aplicativo**" da caixa de diálogo "**Evento de rede**" será ativada automaticamente durante o acesso à rede por parte dos aplicativos assinados. Os fabricantes são: Microsoft, Mozilla, Opera, Yahoo, Google, Hewlet Packard, Sun, Skype, Adobe, Lexmark, Creative Labs, ATI e nVidia.

Lembrar último estado usado

Quando essa opção estiver ativada, a opção "**Lembrar ação para este aplicativo**" da caixa de diálogo "**Evento de rede**" será 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.

11.7 Proteção para a web

A seção **Web Protection** em **Configuração > Proteção on-line** é responsável pela configuração da Web Protection. (Opções disponíveis somente no modo especialista.)

11.7.1 Fazer verificação

A Web Protection o protege contra vírus ou malwares que atingem seu computador a partir de páginas da Web carregadas em seu navegador a partir da Internet. A opção **Verificar** pode ser usada para definir o comportamento do componente Web Protection. (Opções disponíveis somente no modo de especialista.)

Verificar

Ativar a Web Protection

Se essa opção for ativada, o recurso Web Protection será ativado.

Ativar suporte para IPv6

Se essa opção for ativada, o Protocolo da Internet versão 6 será suportada pela Web Protection.

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.

Ação para detecção

Você pode definir as ações a serem realizadas pela Web Protection quando um vírus ou programa indesejado for detectado. (Opções disponíveis somente no modo especialista.)

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.

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 a Web Protection, 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.

Ações permitidas

Nessa caixa, as ações podem ser selecionadas para serem exibidas no caso de uma detecção de vírus. Para isso, é necessário ativar as opções correspondentes.

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. A Web Protection registra a detecção do arquivo de relatório se a função de [relatório](#) estiver ativada.

Quarentena

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 pela Web Protection para seu navegador.

Padrão

Esse botão permite selecionar uma ação que é ativada na caixa de diálogo por padrão quando um vírus é detectado. Selecione a ação que deve ser ativada por padrão e clique no botão "Padrão".

Clique aqui para obter mais informações.

Automático

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

Exibir alertas de detecção

Se essa opção for ativada, um alerta será exibida para cada vírus ou programa indesejado detectado, mostrando as ações que estão sendo executadas.

Ação primária

Ação primária é a ação executada quando a Web Protection encontra um vírus ou um 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. A Web Protection registra a detecção do arquivo de relatório se a função de [relatório](#) estiver ativada.

Quarentena

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 pela Web Protection 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.

Solicitações bloqueadas

In **Solicitações bloqueadas** é possível especificar os tipos de arquivo e os tipos MIME (tipos de conteúdo para os dados transferidos) a serem bloqueados pela Web Protection. O filtro da web permite que você bloqueie URLs conhecidos de phishing e de malware. A Web Protection impede a transferência de dados da Internet para seu computador. (Opções disponíveis somente no modo de especialista.)

A Web Protection bloqueia os seguintes tipos de arquivo/tipos MIME

Todos os tipos de arquivo e tipos MIME (tipos de conteúdo para os dados transferidos) na lista são bloqueados pela Web Protection

Caixa de entrada

Nessa caixa, insira os nomes dos tipos MIME e dos tipos de arquivo que devem ser bloqueados pela Web Protection. 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.

Observação

No entanto, os arquivos que já estão armazenados em seu sistema como arquivos de Internet temporários e bloqueados pela Web Protection 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.

Observação

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 [Web Protection > Verificar > Exceções](#).

Observação

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 de arquivo e tipos MIME excluídos

- `application/octet-stream` = os arquivos de tipo MIME `application/octet-stream` (arquivos executáveis `*.bin`, `*.exe`, `*.com`, `*.dll`, `*.class`) são bloqueados pelo Web Protection.
- `application/olescript` = os arquivos de tipo MIME `application/olescript` (arquivos de script ActiveX `*.axs`) são bloqueados pela Web Protection.
- `.exe` = todos os arquivos com a extensão `.exe` (arquivos executáveis) são bloqueados pela Web Protection.
- `.msi` = todos os arquivos com a extensão `.msi` (arquivos do Windows Installer) são bloqueados pela Web Protection.

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 pela Web Protection.

Observação

O filtro da Web é ignorado para as entradas na lista de URLs excluídos em [Web Protection > Verificar > Exceções](#).

Observação

URLs de spam são URLs enviados com emails de spam. A categoria **Fraude/Enganação** abrange as páginas da Web com “Validade de assinatura” e outras ofertas de serviços cujos custos são ocultados pelo fornecedor.

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 pela Web Protection. Os tipos MIME e os URLs especificados são ignorados pela Web Protection, isto é, os dados não são verificados em busca de vírus e malwares quando são transferidos para seu computador. (Opções disponíveis somente para o modo especialista)

Tipos MIME ignorados pela Web Protection

Nesse campo, é possível selecionar os tipos MIME (tipos de conteúdo para os dados transferidos) a serem ignorados pela Web Protection durante a verificação.

Tipos de arquivo/tipos MIME ignorados pela Web Protection (definido pelo usuário)

Todos os tipos MIME (tipos de conteúdo para os dados transferidos) na lista são ignorados pela Web Protection durante a verificação.

Caixa de entrada

Nessa caixa, é possível inserir o nome dos tipos MIME e dos tipos de arquivo a serem ignorados pela Web Protection durante a verificação. Para tipos de arquivo, insira a extensão, 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**.

Observação

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 no navegador da Internet sem outras verificações nas solicitações bloqueadas (Lista de arquivos e tipos de MIME a serem bloqueados em [Web Protection > Verificar > Solicitações bloqueadas](#)) ou pela Web Protection: para todas as entradas na lista de exclusão, as entradas na lista de arquivos e os tipos MIME a serem bloqueados são ignorados. Nenhuma verificação de vírus e malware é realizada.

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 de arquivo e tipos MIME excluídos:

- `audio/` = Todos os arquivos de tipo de mídia de áudio são excluídos das verificações da Web Protection
- `video/quicktime` = Todos os arquivos de vídeo do subtipo Quicktime (*.qt, *.mov) são excluídos das verificações da Web Protection
- `.pdf` = Todos os arquivos Adobe PDF são excluídos das verificações da Web Protection.

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 pela Web Protection

Todos os URLs dessa lista são excluídos das verificações da Web Protection

Caixa de entrada

Nessa caixa, é possível inserir os URLs (endereços da Internet) a serem excluídos das verificações da Web Protection, 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. Indica sites com qualquer domínio de nível superior (`.com` ou `.net`) com um ponto logo em seguida: `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`).

Observação

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`

`.*name*.com` (válido, mas não recomendado)

As especificações sem pontos, como `*name*`, 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 outras verificações do filtro da web ou da Web Protection: Para todas as entradas na lista de URLs excluídos, as entradas no filtro da web (consulte [Web Protection > Verificar > Solicitações bloqueadas](#)) são ignoradas. Nenhuma verificação de vírus e malware é realizada. Desse modo, somente os URLs confiáveis devem ser excluídos das verificações da Web Protection.

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 da Web Protection: `www.avira.com/pt-br/pages/index.php`, `www.avira.com/pt-br/support/index.html`, `www.avira.com/pt-br/download/index.html` etc.
URLs com o domínio `www.avira.de` não são excluídos das verificações da Web Protection.
- `avira.com -OU- *.avira.com`
= Todos os URLs com o domínio de nível superior e de segundo nível `avira.com` são excluídos das verificações da Web Protection: a especificação implica todos os subdomínios existentes para `.avira.com`: `www.avira.com`, `forum.avira.com` etc.
- `avira. -OU- *.avira.*`
= Todos os URLs com o domínio de segundo nível `avira` são excluídos das verificações da Web Protection: A especificação implica todos os domínios de nível superior ou subdomínios existentes para `.avira`: `www.avira.com`, `www.avira.de`, `forum.avira.com` etc.
- `.*domain*.*`
Todos os URLs que contêm um domínio de segundo nível com a string `domain` são excluídos das verificações da Web Protection: `www.domain.com`, `www.new-domain.de`, `www.sample-domain1.de`, ...
- `net -OU- *.net`
= Todos os URLs com o domínio de nível superior `net` são excluídos das verificações da Web Protection: `www.name1.net`, `www.name2.net` etc.

Aviso

Insira os URLs que deseja excluir da verificação da Web Protection 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 da Web Protection 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`

Heurística

Essa seção de configuração contém as configurações de heurística do mecanismo de verificação. (Opções disponíveis somente no modo de especialista.)

Os produtos Avira 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

O produto Avira 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 Avira contém uma heurística muito poderosa na forma da tecnologia Avira 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.

11.7.2 Relatório

A Web Protection 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.

Desativado

Se essa opção for ativada, a Web Protection 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, a Web Protection 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, a Web Protection registrará informações menos importantes no arquivo de relatório também.

Concluído

Se essa opção for ativada, a Web Protection 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%.

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.

11.8 Proteção de e-mail

A seção **Mail Protection** da Configuração é responsável pela configuração da Mail Protection.

11.8.1 Fazer verificação

Use a Mail Protection para verificar emails de entrada em busca de vírus e malware. Os emails de saída podem ser verificados em busca de vírus e malware pela Mail Protection.

Habilitar Mail Protection

Se essa opção for ativada, o tráfego de emails será monitorado pela Mail Protection. A Mail Protection 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 emails de entrada podem ser verificados quanto a malware por padrão. Se essa opção for desativada, o serviço da Mail Protection ainda será iniciado, mas o monitoramento da Mail Protection será desativado.

Fazer verificação nos emails de entrada

Se essa opção for ativada, os emails de entrada serão verificados em busca de vírus, malware. A Mail Protection é compatível com os protocolos POP3 e IMAP. Ative o monitoramento da Mail Protection 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. Múltiplas portas são separadas por vírgulas. (Opções disponíveis somente no modo de especialista.)

Padrão

Esse botão redefine a porta especificada como a porta POP3 padrão. (Opção disponível somente no modo de especialista.)

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. Múltiplas portas são separadas por vírgulas. (Opções disponíveis somente no modo de especialista.)

Padrão

Esse botão redefine a porta especificada como a porta IMAP3 padrão. (Opção disponível somente no modo de especialista.)

Fazer verificação nos emails de saída (SMTP)

Se essa opção for ativada, os emails de saída serão verificados em busca de vírus e malware.

Portas monitoradas

Nesse campo, você deve inserir a porta a ser usada como caixa de saída pelo protocolo SMTP. Múltiplas portas são separadas por vírgulas. (Opções disponíveis somente no modo de especialista.)

Padrão

Esse botão redefine a porta especificada como a porta SMTP padrão. (Opção disponível somente no modo de especialista.)

Observação

Para verificar os protocolos e portas usados, chame as propriedades de suas contas de email em seu programa cliente de email. Na maioria das vezes, as portas padrão são usadas.

Ativar suporte para IPv6

Se essa opção estiver ativada, o Protocolo da Internet versão 6 será compatível com a Mail Protection no momento. (Opção disponível somente no modo de especialista.)

Ação para detecção

Essa seção de configuração contém outras configurações para as ações realizadas quando a Mail Protection encontra um vírus ou programa indesejado em um email ou anexo. (Opções disponíveis somente no modo de especialista)

Observação

Essas ações são realizadas quando um vírus é detectado tanto em emails de entrada quanto em emails de saída.

Interativo

Se essa opção for ativada, uma caixa de diálogo aparecerá quando um vírus ou programa indesejado for detectado em um email ou anexo, na qual você poderá especificar o que deve ser feito com o email ou anexo em questão. Essa opção é ativada como configuração padrão.

Mostrar barra de andamento

Se essa opção for ativada, a Mail Protection mostrará uma barra de andamento durante o download de emails. Essa opção só poderá ser ativada se a opção "**Interativo**" tiver sido selecionada.

Ações permitidas

Nessa caixa, as ações podem ser selecionadas para serem exibidas no caso de uma detecção de vírus. Para isso, é necessário ativar as opções correspondentes.

Mover para quarentena

Quando essa opção é ativada, o email que inclui todos os anexos é movido para a quarentena. Ele pode ser enviado por email posteriormente pelo Gerenciador de quarentena. O email afetado é excluído. O corpo do texto e todos os anexos do email são substituídos por um texto padrão.

Excluir email

Se essa opção for ativada, o email afetado será excluído quando um vírus ou programa indesejado for detectado. O corpo do texto e todos os anexos do email são substituídos por um texto padrão.

Excluir anexo

Se essa opção for ativada, o anexo afetado será substituído por um texto padrão. Se o corpo do texto do email for afetado, será apagado e também será substituído por um texto padrão. O email propriamente dito é entregue.

Mover anexo para quarentena

Se essa opção tiver sido ativada, o anexo afetado será movido para a quarentena e excluído (substituído por um texto padrão). O corpo do email é entregue. O anexo afetado pode ser entregue posteriormente pelo Gerenciador de quarentena.

Ignorar

Se essa opção for ativada, um email afetado será entregue apesar da detecção de um vírus ou programa indesejado.

Padrão

Esse botão permite selecionar uma ação que é ativada na caixa de diálogo por padrão quando um vírus é detectado. Selecione a ação que deve ser ativada por padrão e clique no botão "**Padrão**".

Automático

Se essa opção for ativada, você não será mais notificado quando um vírus ou programa indesejado for encontrado. A Mail Protection reage de acordo com as configurações definidas nesta seção.

emails afetados

A ação escolhida para "*emails afetados*" é realizada quando a Mail Protection encontra um vírus ou um programa indesejado em um email. Se a opção "**Ignorar**" for selecionada, também será possível, em "*Anexos afetados*", selecionar o processo para lidar com um vírus ou um programa indesejado detectado em um anexo.

Excluir

Se essa opção for ativada, o email afetado será excluído automaticamente caso um vírus ou programa indesejado seja encontrado. O corpo do email 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

Se essa opção for ativada, o email 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:

Mover para quarentena

Se essa opção for ativada, o email 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 email afetado propriamente dito é excluído. O corpo do email é substituído pelo [texto padrão](#) fornecido abaixo. O mesmo se aplica a todos os anexos incluídos; eles também são substituídos por um [texto padrão](#).

Anexos afetados

A opção "*Anexos afetados*" só poderá ser selecionada se a configuração "**Ignorar**" tiver sido selecionada em "*Anexos afetados*". 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](#).

Ignorar

Se essa opção for ativada, o anexo será ignorado apesar da detecção de um vírus ou programa indesejado e entregue.

Mover para quarentena

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.

Aviso

Se essa opção for selecionada, você não terá nenhuma proteção da Mail Protection contra vírus e programas indesejados. Selecione esse item somente se tiver certeza do que está fazendo. Desative a visualização em seu programa de email. Nunca abra anexos clicando duas vezes neles.

Mais ações

Essa seção de configuração contém outras configurações para as ações realizadas quando a Mail Protection encontra um vírus ou programa indesejado em um email ou anexo. (Opções disponíveis somente no modo de especialista.)

Observação

Essas ações são realizadas exclusivamente quando um vírus é detectado nos emails de entrada.

Texto padrão para emails excluídos e movidos

O texto dessa caixa é inserido no email como uma mensagem em vez do email afetado. Você pode editar essa mensagem. O texto pode ter no máximo 500 caracteres.

Você pode usar a seguinte combinação de teclas para formatação:

Ctrl + 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 email 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:

Ctrl + Enter = insere uma quebra de linha.

Padrão

O botão insere um texto padrão predefinido na caixa de edição.

Heurística

Essa seção de configuração contém as configurações de heurística do mecanismo de verificação. (Opções disponíveis somente no modo de especialista.)

Os produtos Avira 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

O produto Avira 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 (Web Protection)

“Ativar a Web Protection”

O programa Avira contém uma heurística muito poderosa na forma da tecnologia Avira AHeAD technology, 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.

11.8.2 Geral

Exceções

Exceções de varredura

Essa tabela mostra a lista de endereços de email excluídos da verificação da Mail Protection (lista de permissões).

Observação

A lista de exceções é usada exclusivamente pela Mail Protection com relação aos emails de entrada.

*Exceções de verificação***Caixa de entrada**

Nessa caixa, é possível inserir o endereço de email que deseja adicionar à lista de endereços de email que não devem ser verificados. Dependendo das configurações, o endereço de email não será mais verificado futuramente pela Mail Protection.

Adicionar

Com esse botão, é possível adicionar o endereço de email inserido na caixa de entrada à lista de endereços de email que não devem ser verificados.

Excluir

Esse botão exclui um endereço de email destacado da lista.

Endereço de email

email que não será mais verificado.

Malware

Quando essa opção é ativada, o endereço de email não é mais verificado quanto a malware.

Para cima

Você pode usar esse botão para mover um endereço de email 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 email destacado para uma posição inferior. Se nenhuma entrada estiver destacada ou o endereço destacado estiver na última posição da lista, esse botão estará desativado.

Cache

O cache da Mail Protection contém dados sobre os emails verificados que são exibidos como dados estatísticos no Centro de controle em **Mail Protection**. (Opções disponíveis somente no modo de especialista.)

Número máximo de emails a serem armazenados no cache

Esse campo é usado para definir o número máximo de emails que são armazenados pela Mail Protection no cache. Os emails mais antigos são excluídos primeiro.

Máximo de dias de armazenamento de email

O período máximo de armazenamento de um email em dias é inserido nessa caixa. Após esse período, o email é removido do cache.

Esvaziar cache

Clique nesse botão para excluir os emails armazenados no cache.

Rodapé

Em **Rodapé**, é possível configurar um rodapé de email que é exibido nos emails enviados. (Opções disponíveis somente no modo de especialista.)

Essa função requer a ativação da verificação feita pela Proteção de email dos emails de saída (consulte a opção **Fazer verificação nos emails de saída (SMTP)** em [Configuração > Mail Protection > Verificar](#)). Você pode usar o rodapé definido pelo Avira Mail Protection 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 Avira Mail Protection.

Rodapé para emails a serem enviados

Anexar rodapé da Mail Protection

Se essa opção for ativada, o rodapé do Avira Mail Protection será exibido abaixo do texto da mensagem do email enviado. O rodapé do Avira Mail Protection confirma que o email enviado foi verificado pelo Avira. O rodapé do Avira Mail Protection contém o seguinte texto: "*Verificado com o Avira Mail Protection [versão do produto] [iniciais e número da versão do mecanismo de pesquisa] [iniciais e número da versão do arquivo de definição de vírus]*".

Anexar o seguinte 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.

11.8.3 Relatório

A Mail Protection inclui uma função de registro abrangente para fornecer ao usuário ou administrador observações exatas sobre o tipo e a maneira de uma detecção. (Opções disponíveis somente no modo de especialista.)

Relatório

Este grupo permite determinar o conteúdo do arquivo do relatório.

Desativado

Se essa opção for ativada, a Mail Protection 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, a Mail Protection 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.

Estendido

Se essa opção for ativada, a Mail Protection registrará informações menos importantes no arquivo de relatório também.

Concluído

Se essa opção for ativada, a Mail Protection 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. Para saber qual é o local de salvamento, consulte [Configuração > Geral > Diretórios > Diretório do relatório](#).

Gravar configuração no arquivo de relatório

Se essa opção for ativada, a configuração da Mail Protection 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.

11.9 Geral

11.9.1 Categorias de ameaça

Seleção de categorias de ameaça estendida (Opções disponíveis somente no modo de especialista)

Seu produto Avira protege seu computador contra vírus. Além disso, você pode fazer a verificação de acordo com as seguintes categorias de ameaça estendidas.

- [Adware](#)
- [Adware/Spyware](#)
- [Aplicativo](#)
- [Clientes back-door](#)
- [Discador](#)
- [Arquivos com extensão dupla](#)
- [Fraudulent software](#)
- [Jogos](#)
- [Piadas](#)
- [Phishing](#)
- [Programa que viola o domínio privado](#)
- [Compactadores de tempo de execução incomuns](#)

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.

Observação

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.

11.9.2 Senha

Você pode proteger o produto Avira em [diferentes áreas](#) com uma senha. Se uma senha for criada, você terá que inseri-la sempre que desejar abrir a área protegida.

Password

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".

Confirmação

Confirme a senha inserida acima inserindo-a aqui novamente. Por motivos de segurança, os caracteres reais digitados neste espaço são substituídos por asteriscos (*).

Observação

A senha diferencia maiúsculas de minúsculas.

Áreas protegidas por senha (Opções disponíveis somente no modo de especialista)

Seu produto Avira 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 a Realtime Protection	Se essa opção for ativada, a senha predefinida será necessária para ativar ou desativar a AntiVir Realtime Protection.
Ativar/desativar a Proteção de email	Se essa opção for ativada, a senha predefinida será necessária para ativar/desativar a Proteção de email.
Ativar/desativar o FireWall	Se essa opção for ativada, a senha predefinida será necessária para ativar/desativar o FireWall.
Ativar/desativar a Web Protection	Se essa opção for ativada, a senha predefinida será necessária para ativar/desativar a Web Protection.
Quarentena	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.
Baixe o CD de resgate da Internet	Se essa opção for ativada, a senha predefinida será necessária para iniciar o download do CD do Avira Rescue.
Configuração	Se essa opção for ativada, a configuração do programa só poderá ser feita depois que a senha predefinida for inserida.

Alternar manualmente a configuração	Se essa opção for ativada, a senha predefinida será necessária se você desejar alternar manualmente para um perfil de configuração diferente.
Instalação/Desinstalação	Se essa opção for ativada, a senha predefinida será necessária para a instalação ou desinstalação do programa.

11.9.3 Segurança

Opções disponíveis somente no modo de especialista.

Início automático

Bloquear função de início automático

Se essa opção for ativada, a execução da função de início automático do Windows será bloqueada em todas as unidades conectadas, incluindo pendrives, unidades de CD e DVD e unidades de rede. Com a função de 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 de início automático é crítica especialmente para pendrivers, pois os dados de um pendrive podem ser alterados a qualquer momento.

Excluir CDs e DVDs

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

Aviso

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

Proteção do sistema

Proteger arquivos host do Windows contra alterações

Se essa opção for definida como ativada, os arquivos de host do Windows serão protegidos contra gravação. A manipulação não é mais permitida. Por exemplo, o malware não pode redirecionar você para sites indesejados. Essa opção é ativada como configuração padrão.

Proteção do produto

Observação

As opções de proteção do produto não estarão disponíveis se a Realtime Protection não tiver sido instalada 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 do processo. A opção é ativada como configuração padrão. Para desativar essa opção, é necessário reiniciar o computador.

Observação

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.

Observação

A proteção de arquivos e entradas de registro não está disponível para o Windows XP de 64 bits.

11.9.4 WMI

Opções disponíveis somente no modo de especialista.

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 produto Avira oferece suporte para WMI e fornece dados (informações de status, dados estatísticos, relatórios, solicitações planejadas etc.), bem como eventos e métodos (processos de início e término) em uma interface. O WMI fornece a você a condição de baixar dados operacionais do programa e controlar o programa. Você pode solicitar um guia de referência completo da interface da WMI para o fabricante do WMI. O arquivo de referência é disponibilizado em formato PDF quando você assina um contrato de confidencialidade.

Ativar suporte para WMI

Quando essa opção está ativada, é possível baixar dados operacionais do programa via WMI.

Permitir ativação/desativação de serviços

Quando essa opção está ativada, é possível ativar e desativar serviços do programa via WMI.

11.9.5 Configurações de 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 proxy

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 proxy** 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

11.9.6 Alertas

Alertas de rede

Você pode enviar alertas configuráveis individualmente do [System Scanner](#) ou da [Proteção em tempo real](#) para qualquer estação de trabalho em sua rede.

Observação

Verifique se o "Serviço de mensagem" foi iniciado. Você encontrará o serviço (por exemplo, no Windows XP) em **Iniciar > Configurações > Controle de sistema > Administração > Serviços**.

Observação

Um alerta sempre é enviado para os computadores, **não** para um usuário específico.

Aviso

Essa funcionalidade **não tem mais suporte** nos seguintes sistemas operacionais:

Windows Server 2008 e superior

Windows Vista e superior

Enviar mensagem para

A lista dessa janela mostra nomes de computadores que recebem uma mensagem quando um vírus ou programa indesejado é encontrado.

Observação

Um computador sempre pode ser inserido só uma vez nessa lista.

Inserir

Com esse botão, é possível adicionar outro computador. Uma janela é aberta, na qual é possível inserir os nomes dos novos computadores. O nome do computador pode ter no máximo 15 caracteres.



O botão abre uma janela na qual você pode selecionar, se desejar, um computador diretamente no seu ambiente de computador.

Excluir

Com esse botão, é possível excluir a entrada atualmente selecionada da lista.

Alertas de rede na Realtime Protection**Alertas de rede**

Se essa opção for ativada, os alertas de rede serão enviados. Essa opção é desativada como configuração padrão.

Observação

Para ativar essa opção, é necessário inserir pelo menos um destinatário em [Configuração > Geral > Alertas > Rede](#).

Mensagem a ser enviada

A janela mostra a mensagem enviada para a estação de trabalho selecionada quando um vírus ou programa indesejado é detectado. Você pode editar essa mensagem. O texto pode ter no máximo 500 caracteres.

Você pode usar as seguintes combinações de tecla para formatar a mensagem:

Atalho	Descrição
Ctrl + Tab	Inserir uma guia. A linha atual é recuada vários caracteres à direita.
Ctrl + Enter	Inserir uma quebra de linha.

A mensagem pode incluir caracteres curinga para as informações encontradas durante a pesquisa. Esses caracteres curinga são substituídos pelo texto real quando a mensagem é enviada.

Os seguintes caracteres curinga podem ser usados:

Caractere curinga	Descrição
%VIRUS%	contém o nome do vírus ou programa indesejado detectado
%FILE%	contém o caminho e o nome do arquivo afetado
%COMPUTER%	contém o nome do computador no qual a Realtime Protection está em execução
%NAME%	contém o nome do usuário que acessou o arquivo afetado
%ACTION%	contém a ação realizada após a detecção do vírus
%MACADDR%	contém o endereço MAC do computador no qual a Realtime Protection está em execução

Padrão

O botão restaura o texto padrão predefinido de um alerta.

Alertas de rede do System Scanner

Ativar alertas de rede

Se essa opção for ativada, os alertas de rede serão enviados. Essa opção é desativada como configuração padrão.

Observação

Para ativar essa opção, é necessário inserir pelo menos um destinatário em [Configuração > Geral > Alertas > Rede](#).

Mensagem a ser enviada

A janela mostra a mensagem enviada para a estação de trabalho selecionada quando um vírus ou programa indesejado é detectado. Você pode editar essa mensagem. O texto pode ter no máximo 500 caracteres.

Você pode usar as seguintes combinações de tecla para formatar a mensagem:

Atalhos	Descrição
Ctrl + Tab	Inserir uma guia. A linha atual é recuada vários caracteres à direita.
Ctrl + Enter	Inserir uma quebra de linha.

A mensagem pode incluir caracteres curinga para as informações encontradas durante a pesquisa. Esses caracteres curinga são substituídos pelo texto real quando a mensagem é enviada.

Os seguintes caracteres curinga podem ser usados:

Caractere curinga	Descrição
%VIRUS%	contém o nome do vírus ou programa indesejado detectado
%NAME%	contém o nome do usuário conectado que está usando o System Scanner
%FILE%	contém o caminho e o nome do arquivo afetado
%COMPUTER%	contém o nome do computador em que o System Scanner está em execução

%ACTION%	contém a ação realizada após a detecção do vírus
%MACADDR%	contém o endereço MAC do computador em que o System Scanner está em execução

Padrão

O botão restaura o texto padrão predefinido de um alerta.

E-mail

Alertas de email na Realtime Protection

A Realtime Protection da Avira pode enviar alertas por email para um ou mais destinatários para determinados eventos.

Alertas de email

Se essa opção for ativada, a Realtime Protection da Avira enviará mensagens de email com as informações mais importantes quando ocorrer um determinado evento. Essa opção é desativada como configuração padrão.

Mensagens de email para os seguintes eventos

A verificação durante o acesso detectou um vírus ou programa indesejado

Se essa opção for ativada, você sempre receberá um email com o nome do vírus ou programa indesejado e o arquivo afetado quando a verificação de acesso detectar um vírus ou programa indesejado.

Editar

O botão "**Editar**" abre a janela "**Modelo de email**", na qual é possível configurar a notificação para um evento de Detecção durante o acesso. Você pode inserir texto na linha de assunto e no corpo do email. É possível usar variáveis para esse objetivo. (Consulte [Modelo de email](#))

Ocorreu um erro crítico na Realtime Protection

Se essa opção for ativada, você receberá um email sempre que detectar um erro crítico interno.

Nota

Nesse caso, entre em contato com nosso [suporte técnico](#) e inclua os dados fornecidos no email. O arquivo especificado também deve ser enviado para análise.

Editar

O botão "**Editar**" abre o "**Modelo de email**" na qual é possível configurar a notificação para um evento de "Erro crítico na Realtime Protection". Você pode inserir texto na linha de assunto e no corpo do email. É possível usar variáveis para essa finalidade. (consulte [Modelo de email](#))

Destinatário(s)

Insira os endereços de email dos destinatários nessa caixa. Os endereços individuais são separados por vírgulas. Todos os endereços juntos devem ter no máximo 260 caracteres (isto é, o total de caracteres).

Alertas de email do System Scanner

Para alguns eventos, a verificação sob demanda pode enviar alertas e mensagens por email para um ou mais destinatários.

Alertas de email

Se essa opção for ativada, o programa enviará mensagens de email com as informações mais importantes quando ocorrer um determinado evento. Essa opção é desativada como configuração padrão.

Mensagens de email para os seguintes eventos

A verificação por solicitação detectou um vírus ou programa indesejado

Se essa opção for ativada, você receberá um email com o nome do vírus ou programa indesejado e o arquivo afetado sempre que a verificação sob demanda detectar um vírus ou programa indesejado.

Editar

O botão "**Editar**" abre a janela "**Modelo de email**", na qual é possível configurar a notificação para um evento de "Detecção durante a verificação". Você pode inserir texto na linha de assunto e no corpo do email. É possível usar variáveis para essa finalidade. (consulte [Modelo de email](#))

Fim da verificação programada

Quando essa opção está ativada, um email é enviado quando um trabalho de verificação é executado. O email contém dados sobre o local e a duração do trabalho de verificação, as pastas e os arquivos verificados, bem como sobre os vírus encontrados e avisos.

Editar

O botão "**Editar**" abre a janela "**Modelo de email**", na qual é possível configurar a notificação para um evento de "Fim da verificação". Você pode inserir texto na linha de assunto e no corpo do email. É possível usar variáveis para essa finalidade. (consulte [Modelo de email](#))

Adicionar arquivo de relatório como anexo

Se essa opção for ativada, o arquivo de relatório atual do componente System Scanner será adicionado a um email como um anexo ao enviar notificações do System Scanner.

Destinatário(s)

Insira os endereços de email dos destinatários nessa caixa. Os endereços individuais são separados por vírgulas. Todos os endereços juntos devem ter no máximo 260 caracteres (isto é, o total de caracteres).

Alertas de email do atualizador

O componente Atualizador pode enviar notificações por email para um ou mais destinatários para eventos específicos.

Alertas de email

Se essa opção for ativada, o componente Atualizador enviará mensagens de email com os dados mais importantes quando ocorrer um evento específico. Essa opção é desativada como configuração padrão.

Mensagens de email para os seguintes eventos

Nenhuma atualização é necessária. O seu programa está atualizado

Se essa opção for ativada, um email será enviado caso o Atualizador consiga estabelecer uma conexão com o servidor de download, mas nenhum arquivo novo esteja disponível no servidor. Isso significa que o produto Avira está atualizado.

Editar

O botão "**Editar**" abre a janela "**Modelo de email**", na qual é possível configurar a notificação para um evento de "Nenhuma atualização necessária". Você pode inserir texto na linha de assunto e no corpo do email. É possível usar variáveis para essa finalidade. (consulte [Modelo de email](#))

Atualização concluída com êxito. Novos arquivos foram instalados

Se essa opção for ativada, um email será enviado para todas as atualizações executadas: Pode ser a atualização de um produto, do arquivo de definição de vírus ou do mecanismo de verificação.

Editar

O botão "**Editar**" abre a janela "**Modelo de email**", na qual é possível configurar a notificação para um evento de "Atualização bem-sucedida - novos arquivos instalados". Você pode inserir texto na linha de assunto e no corpo do email. É possível usar variáveis para essa finalidade. (consulte [Modelo de email](#))

Atualização concluída. Uma nova atualização de produto está disponível

Se essa opção for ativada, um email será enviado somente se uma atualização do mecanismo de verificação ou do arquivo de definição de vírus tiver sido executada sem uma atualização de produto, mas a atualização de um produto estiver disponível.

Editar

O botão "**Editar**" abre a janela "**Modelo de email**", na qual é possível configurar a notificação para um evento de "Atualização bem-sucedida atualização de produto disponível". Você pode inserir texto na linha de assunto e no corpo do email. É possível usar variáveis para essa finalidade. (consulte [Modelo de email](#))

Falha de atualização

Se essa opção for ativada, um email será enviado caso haja uma falha de atualização devido a um erro.

Editar

O botão "**Editar**" abre a janela "**Modelo de email**", na qual é possível configurar a notificação para um evento de "Falha de atualização". Você pode inserir texto na linha de assunto e no corpo do email. É possível usar variáveis para essa finalidade. (consulte [Modelo de email](#))

Adicionar arquivo de relatório como anexo

Se essa opção for ativada, o arquivo de relatório atual do componente Atualizador será adicionado a um email como um anexo ao enviar notificações do Atualizador.

Destinatário(s)

Insira os endereços de email dos destinatários nessa caixa. Os endereços individuais são separados por vírgulas. Todos os endereços juntos devem ter no máximo 260 caracteres (isto é, o total de caracteres).

Observação

Os alertas sempre serão enviados por email para os seguintes eventos se um servidor SMTP e um endereço de destinatário tiverem sido configurados para notificações do Atualizador:

Uma atualização de produto é necessária para cada nova atualização do programa.

Uma atualização do mecanismo de verificação ou do arquivo de definição de vírus não foi executada, visto que uma atualização de produto é necessária.

Esses alertas são enviados independentemente das configurações de aviso de email do componente Atualizador.

Modelo de email

Na janela **Modelo de email**, é possível configurar as notificações de email dos componentes individuais para os eventos ativados. Você pode inserir texto com no

máximo 128 caracteres na linha de assunto e no máximo 1024 caracteres no campo de mensagem.

As seguintes variáveis podem ser usadas na linha de assunto e na mensagem de email:

Variáveis aceitas globalmente

Variável	Valor
Variáveis do ambiente Windows	O componente de notificações de email aceita todas as variáveis do ambiente Windows.
%SYSTEM_IP%	Endereço IP do computador
%FQDN%	Nome de domínio totalmente qualificado
%TIMESTAMP%	Carimbo de data e hora do evento: o formato de data e hora segue as configurações de idioma do sistema operacional
%COMPUTERNAME%	Nome do computador NetBIOS
%USERNAME%	Nome do usuário que acessa o componente
%PRODUCTVER%	Versão do produto
%PRODUCTNAME%	Nome do produto
%MODULENAME%	Nome do componente que envia o email
%MODULEVER%	Versão do componente que envia o email

Variáveis específicas do componente

Variável	Valor	O componente envia emails
%ENGINEVER%	Versão do mecanismo de verificação usado	Proteção em tempo real System Scanner
%VDFVER%	Versão do arquivo de definição de vírus usado	Proteção em tempo real System Scanner
%SOURCE%	Nome de arquivo totalmente qualificado	Proteção em tempo real
%VIRUSNAME%	Nome do vírus ou programa indesejado	Proteção em tempo real
%ACTION%	Ação executada após a detecção	Proteção em tempo real
%MACADDR%	Endereço MAC da primeira placa de rede registrada	Proteção em tempo real
%UPDFILESLIST%	Lista de arquivos atualizados	Atualizador
%UPDATETYPE%	Tipo de atualização: Atualização do mecanismo de verificação e do arquivo de definição de vírus ou atualização do produto com atualização do mecanismo de verificação e do arquivo de definição de vírus	Atualizador

%UPDATEURL%	URL do servidor de download usado para atualização	Atualizador
%UPDATE_ERROR%	Erro de atualização em palavras	Atualizador
%DIRCOUNT%	Número de diretórios verificados	System Scanner
%FILECOUNT%	Número de arquivos verificados	System Scanner
%MALWARECOUNT%	Número de vírus ou programas indesejados detectados	System Scanner
%REPAIREDCOUNT%	Número de arquivos infectados reparados	System Scanner
%RENAMEDCOUNT%	Número de arquivos infectados renomeados	System Scanner
%DELETEDCOUNT%	Número de arquivos infectados excluídos	System Scanner
%WIPECOUNT%	Número de arquivos infectados substituídos e excluídos	System Scanner
%MOVEDCOUNT%	Número de arquivos infectados movidos para a quarentena	System Scanner
%WARNINGCOUNT%	Número de avisos	System Scanner
%ENDTYPE%	Status da varredura: terminado/concluído com êxito	System Scanner

%START_TIME%	Hora inicial da varredura: Hora inicial da atualização	System Scanner, Atualizador
%END_TIME%	Término da varredura Término da atualização	System Scanner, Atualizador
%TIME_TAKEN%	Duração da verificação em minutos Duração da atualização em minutos	System Scanner, Atualizador
%LOGFILEPATH%	Caminho e nome do arquivo de relatório	System Scanner, Atualizador

Alertas acústicos

Opções disponíveis somente no modo de especialista.

Quando um vírus ou malware é detectado pelo System Scanner ou a Realtime Protection, 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 System Scanner é definido na configuração em [System Scanner > Verificar > Ação para detecção](#). O modo de ação da Realtime Protection é definido na configuração em [Realtime Protection > Verificar > Ação para detecção](#).

Nenhum aviso

Quando essa opção for ativada, nenhum alerta acústico será emitido quando um vírus for detectado pelo System Scanner ou pela Realtime Protection.

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 System Scanner ou pela Realtime Protection. 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 System Scanner ou pela Realtime

Protection. 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.

Alertas

O produto Avira 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 **Alertas**, 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 na janela de configuração **Alertas**. (Opções disponíveis somente no modo de especialista).

Atualizar

Alertar 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).

Avisos/Notificações por email com as seguintes circunstâncias

É usada conexão discada

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](#))

Arquivos foram atualizados

Se essa opção for ativada, você receberá uma notificação de área de trabalho sempre que uma atualização for realizada e os arquivos forem atualizados.

Falha de 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.

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.

11.9.7 Eventos

Opções disponíveis somente no modo de especialista.

Limitar tamanho do banco de dados de eventos

Limitar tamanho a no máximo 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 todos os 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.

Sem limite

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.

11.9.8 Relatórios

Opções disponíveis somente no modo de especialista.

Limitar relatórios

Limitar número para no máximo n peças.

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.

Sem limite

Se essa opção for ativada, o número de relatórios não será restrito.

11.9.9 Diretórios

Opções disponíveis somente no modo de especialista.

Caminho temporário

Usar configurações padrão do sistema

Se essa opção for ativada, as configurações do sistema serão usadas para manipular arquivos temporários.

Observação

Você pode ver onde o sistema (por exemplo, o Windows XP) salva os arquivos temporários em: **Iniciar > Configurações > Painel de controle > Sistema > Indexar placa** botão "**Avançado**" "**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.

Caixa de entrada

Nesta caixa de entrada, insira o caminho onde o programa armazenará seus arquivos temporários.



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.

Diretório do relatório

Caixa de entrada

Esta caixa de entrada contém o caminho até o diretório de relatório.



O botão abre uma janela na qual é possível selecionar o diretório desejado.

Padrão

O botão restaura o caminho predefinido até o diretório do relatório.

Diretório da quarentena

Caixa de entrada

Esta caixa contém o caminho até o diretório da quarentena.



O botão abre uma janela na qual é possível selecionar o diretório desejado.

Padrão

O botão restaura o caminho predefinido até o diretório da quarentena.

Este manual foi elaborado com extremo cuidado. Mesmo assim, é impossível garantir que não haja erros na sua formatação 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 Q4-2011

Todos os nomes de marcas e produtos são marcas comerciais ou marcas registradas de seus respectivos proprietários. As marcas comerciais protegidas não estão identificadas neste manual mas tal não implica que estas possam ser utilizadas livremente.



live free.™