Avira

Professional Security

Manual do usário

Marcas Registradas e Direitos Autorais

Marcas Registradas

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

Informações sobre direitos autorais

Um código fornecido por provedores de terceiros foi usado para o Avira Professional Security. Agradecemos os detentores dos direitos autorais por disponibilizar o código para nós.
Para informações detalhadas sobre direitos autorais, consulte Licenças de Terceiros.

Contrato de Licença de Usuário Final - EULA

http://www.avira.com/pt-br/license-agreement

Política de privacidade

http://www.avira.com/pt-br/general-privacy

Sumário

1. Introdução

Seu produto Avira protege seu computador contra vírus, worms, cavalos de Troia, adware e spyware e outros riscos. Neste manual, eles são referidos como vírus ou malware (software nocivo) e programas indesejados.

O manual descreve a instalação e a operação do programa.

Para obter opções e informações adicionais, visite nosso site:
http://www.avira.com/pt-br/

O site da Avira permite:

- acessar informações sobre outros programas da área de trabalho da Avira
- fazer download dos programas da área de trabalho da Avira mais recentes
- fazer download dos manuais de produto mais recentes no formato PDF
- fazer download de ferramentas gratuitas de suporte e reparo
- acessar nosso abrangente banco de dados de conhecimento e perguntas frequentes para solução de problemas
- acessar endereços de suporte específicos do país.

Sua 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 ação executada por você.
↪	Colocado antes de um evento que segue a ação anterior.
Aviso	Colocado antes de um aviso quando pode ocorrer a perda de dados críticos.

Observação	Colocado antes de um link para informações particularmente importantes ou uma dica que torna o produto Avira mais fácil de usar.

As seguintes ênfases são usadas:

Ênfase	Explicação
Itálico	Dados do nome de arquivo ou do caminho.
	Elementos de interface de software exibidos (por exemplo, seção da janela ou mensagem de erro).
Negrito	Elementos de interface de software clicáveis (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 de seu produto Avira:

- consulte o Capítulo: Escopo da Entrega
- consulte o Capítulo: Requisitos do Sistema
- consulte o Capítulo: Licenciamento e Atualização
- consulte o Capítulo: Gerenciador de Licença

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

▸ Observe o seguinte:

Aviso
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 seu produto Avira está atualizado com atualizações automáticas. Configure o programa conforme necessário.

2.1 Escopo da Entrega

Seu produto Avira possui as seguintes funções:

- Centro de Controle para monitorar, gerenciar e controlar o programa inteiro
- Configuração centralizada com opções padrão e avançadas amigáveis e ajuda contextual
- Scanner (varredura por demanda) com varredura configurável e controlada por perfis de todos os tipos conhecidos de vírus e malwares
- A integração no Controle de Conta de Usuário do Windows permite que você realize tarefas que exigem direitos de administrador.
- Real-Time Protection (varredura no acesso) para monitoramento contínuo de todas as tentativas de acesso ao arquivo

- Componente ProActiv para o monitoramento permanente de ações de programa (apenas para sistemas de 32 bits)
- Mail Protection (Scanner de POP3 , Scanner de IMAP e Scanner de SMTP) para a varredura permanente de e-mails em busca de vírus e malwares, incluindo a varredura de anexos de e-mail
- Web Protection para monitorar dados e arquivos transferidos da internet usando o protocolo HTTP (monitoramento das portas 80, 8080 e 3128)
- Gerenciamento de quarentena integrado para isolar e processar arquivos suspeitos
- Rootkits Protection para detectar malware oculto instalado em seu sistema de computador (rootkits)
  (Não disponível no Windows XP de 64 bits)
- Acesso direto para informações detalhadas sobre os vírus e malwares detectados via Internet
- Atualizações simples e rápidas para o programa, definições de vírus e mecanismo de procura por meio da Atualização de Único Arquivo e atualizações incrementais de VDF por meio de um servidor da web na Internet ou em uma intranet
- Licenciamento amigável no Gerenciador de Licença
- Agendamento Integrado para planejar trabalhos individuais ou recorrentes, como atualizações ou verificações
- Altíssima taxa de detecção de vírus e malware com uma inovadora tecnologia de varredura (mecanismo de varredura), incluindo o método de varredura 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 (varredura simultânea de vários arquivos em alta velocidade)
- FireWall para proteger seu computador contra acesso não autorizado da Internet ou de outra rede e contra acesso não autorizado à Internet/rede por usuários não autorizados

2.2 Requisitos do Sistema

2.2.1 Requisitos do sistema do Avira Professional Security

O Avira Professional Security tem os seguintes requisitos necessários para o uso bem sucedido do sistema:

Sistema operacional

- Windows 8, SP mais recente (32 ou 64 bits) ou
- Windows 7, SP mais recente (32 ou 64 bits) ou
- Windows XP, SP mais recente (32 ou 64 bits)

Hardware

- Computador com processador Pentium ou superior de pelo menos 1 GHz
- Pelo menos 150 MB de espaço livre de memória no disco rígido (mais se for usada a quarentena para armazenamento temporário)
- Pelo menos 1024 MB de RAM no Windows 8, Windows 7
- Pelo menos 512 MB de RAM no Windows XP

Outros requisitos

- 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 Preparando para instalação)

2.2.2 Direitos de Administrador (a partir do Windows Vista)

No Windows XP, muitos usuários trabalham com direitos de administrador. No entanto, isso não é desejável do ponto de vista de segurança, pois facilita a invasão de vírus e programas indesejados nos computadores.

Por isso, a Microsoft introduziu o "Controle de Conta de Usuário" (UAC). O Controle de Conta de Usuário é parte dos seguintes sistemas operacionais:

- Windows Vista
- Windows 7
- Windows 8

O Controle de Conta de Usuário oferece maior proteção a usuários que estão conectados como administradores. No entanto, o administrador possui apenas os privilégios de um usuário normal, a princípio. Ações para as quais os direitos de administrador são necessárias estão claramente marcadas no sistema operacional com um ícone de informações. Além disso, o usuário deve confirmar explicitamente a ação necessária. Os privilégios aumentam e a tarefa administrativa é realizada pelo sistema operacional após a obtenção dessa permissão.

O Avira Professional Security requer direitos de administrador para algumas ações. Essas ações são marcadas com o símbolo a seguir:  . Se esse símbolo também aparecer em um botão, os direitos de administrador serão necessários para realizar essa ação. Se a sua conta de usuário atual não tem direitos de administrador, a caixa de diálogo de Controle de Conta de Usuário do Windows solicitará a inserção da senha de administrador. Se você não tiver uma senha de administrador, não poderá realizar essa ação.

2.2.3 Incompatibilidade com outros programas

Avira Professional Security

No momento, o Avira Professional Security não pode ser usado com estes produtos:

- PGP Desktop Home
- PGP Desktop Professional 9.0
- CyberPatrol

Um erro nos produtos mencionados acima pode fazer com que o Avira Mail Protection (scanner de POP3) no product_name_long$ não funcione ou deixar o sistema instável. Avira está trabalhando com a PGP e a CyberPatrol para solucionar o problema. Até que uma solução seja encontrada, recomendamos que você desinstale os produtos mencionados acima antes de instalar o Avira Professional Security.

Avira Web Protection

Avira Web Protection não é compatível com estes produtos:

- Bigfoot Networks Killer Ethernet Controller
- Teleport Pro da Tennyson Maxwell, Inc
- CHIPDRIVE® Time Recording da SCM Microsystems
- MSN Messenger da Microsoft

Desse modo, todos os dados enviados ou solicitados por esses produtos serão ignorados pelo Avira Web Protection.

Observação
Avira Mail Protection não funcionará se um servidor de e-mail (por exemplo, AVM KEN, Exchange) já estiver instalado no computador.

2.3 Licenciamento e Atualização

2.3.1 Licenciamento

Para poder usar seu produto Avira, é necessária uma licença. Ao usar a licença, você aceita os termos da licença.

A licença é emitida através de uma licença digital na forma de um arquivo.*KEY*. Esse arquivo 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. Portanto, o arquivo de licença digital também pode conter a licença de mais de um produto.

Se você adquiriu seu produto Avira na Internet, ou por meio de um CD/DVD do programa, o arquivo de licença digital será enviado para você por e-mail. Você pode carregar a chave de licença durante a instalação do programa ou instalá-la posteriormente no Gerenciador de Licença.

2.3.2 Extensão de uma licença

Quando sua licença estiver prestes a expirar, a Avira vai lhe mandar uma notificação suspensa para relembrar você de estender sua licença. Para fazer isso, você apenas tem que clicar em um link e você será encaminhado à loja on-line da Avira.

Se você se tiver registrado no portal de licenciamento da Avira, você pode também estender sua licença diretamente on-line através da **Visão Geral da Licença** ou selecionar a renovação automática da sua licença.

> **Observação**
> Se seu produto Avira for gerenciado no AMC, seu administrador executará a atualização. Será perguntado se você deseja salvar seus dados e reinicializar o computador, caso contrário, você não estará protegido.

2.3.3 Gerenciador de licença

O Gerenciador de licença do Avira Professional Security permite uma instalação muito simples da licença do Avira Professional Security.

Gerenciador de Licença do Avira Professional Security

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

Observação
O Gerenciador de licença 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. Neste caso, o arquivo existente é sobrescrito pelo novo arquivo de licença.

3. Instalação e desinstalação

Este capítulo contém informações relacionadas à instalação do Avira Professional Security.

3.1 Preparando para instalação

- ✓ Antes da instalação, verifique se seu computador preenche todos os Requisitos mínimos do sistema.
- ✓ Feche 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 umas nas outras (para opções automáticas, consulte Removendo software incompatível).
- ✓ Se necessário, desinstale quaisquer barras de ferramenta de pesquisa instaladas anteriormente antes de instalar o Avira SearchFree Toolbar. Caso contrário, você não conseguirá instalar o Avira SearchFree Toolbar.
- ✓ Estabeleça uma conexão com a Internet.

- A conexão é necessária para realizar as seguintes etapas de instalação:
  - Download do arquivo do programa e do mecanismo de pesquisa atuais, bem como dos arquivos de definição de vírus mais recentes através do programa de instalação (para instalação baseada na Internet)
  - Ativando o programa
  - Registrando como um usuário
  - Quando apropriado, realizar uma atualização após a conclusão da instalação
- ✓ Mantenha o código de ativação ou arquivo de licença para o seu Avira Professional Security acessível para quando desejar ativar o programa.
- ✓ Para ativação ou registro do produto, o Avira Professional Security usa protocolo HTTP e Porta 80 (comunicação na Web), bem como protocolo de criptografia SSL e Porta 443 para comunicaçã com os servidores Avira. Se estiver usando um firewall, certifique-se de que as conexões necessárias e/ou os dados de entrada ou de saída

não estejam bloqueados pelo firewall.

3.2 Instalando a partir do CD quando online

- Insira o CD do Avira Professional Security.

  Se o início automático estiver ativado, clique em **Abrir pasta** para visualizar os arquivos.
  OU

  Navegue pela unidade de CD, clique com o botão direito do mouse em AVIRA e selecione **Abrir pasta** para visualizar os arquivos.

  Clique duas vezes no arquivo *autorun.exe*.

  No menu do CD, escolha a instalação da versão online.

  O programa verifica softwares incompatíveis (mais informações aqui: Removendo software incompatível).

  Clique em **Avançar** na tela de *Boas-vindas*.

  Selecione o idioma e clique em **Avançar**. Todos os arquivos necessários para instalação são baixados dos servidores da Web do Avira.

  Continue com Escolhendo um tipo de instalação.

3.3 Instalando a partir do CD quando offline

- Insira o CD do Avira Professional Security.

  Se o início automático estiver ativado, clique em **Abrir pasta** para visualizar os arquivos.
  OU

  Navegue pela unidade de CD, clique com o botão direito do mouse em AVIRA e selecione **Abrir pasta** para visualizar os arquivos.

  Clique duas vezes no arquivo *autorun.exe*.

  No menu do CD, escolha a instalação da versão offline.

  O programa verifica softwares incompatíveis (mais informações aqui: Removendo software incompatível).

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

  Continue com Escolhendo um tipo de instalação.

3.4 Instalando software baixado do Avira Shop

- Vá para www.avira.com/download.

  Selecione o produto e clique em **Download**.

  Salve o arquivo baixado no seu sistema.

Clique duas vezes no arquivo de instalação avira_professional_security_en.exe.

Se a janela de Controle de conta do usuário aparecer, clique em Sim

O programa verifica softwares incompatíveis (mais informações aqui: Removendo software incompatível).

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

Continue com Selecionando um tipo de instalação.

3.5 Removendo software incompatível

O Avira Professional Security procurará qualquer sotware incompatível possível em seu computador. Se algum software potencialmente incompatível for detectado, o Avira Professional Security gerará uma lista desses programas. É recomendado remover esses programas de software para não arriscar a estabilidade de seu computador.

- Selecione na lista as caixas de seleção de todos os programas que devem ser removidos automaticamente de seu computador e clique em **Avançar**.

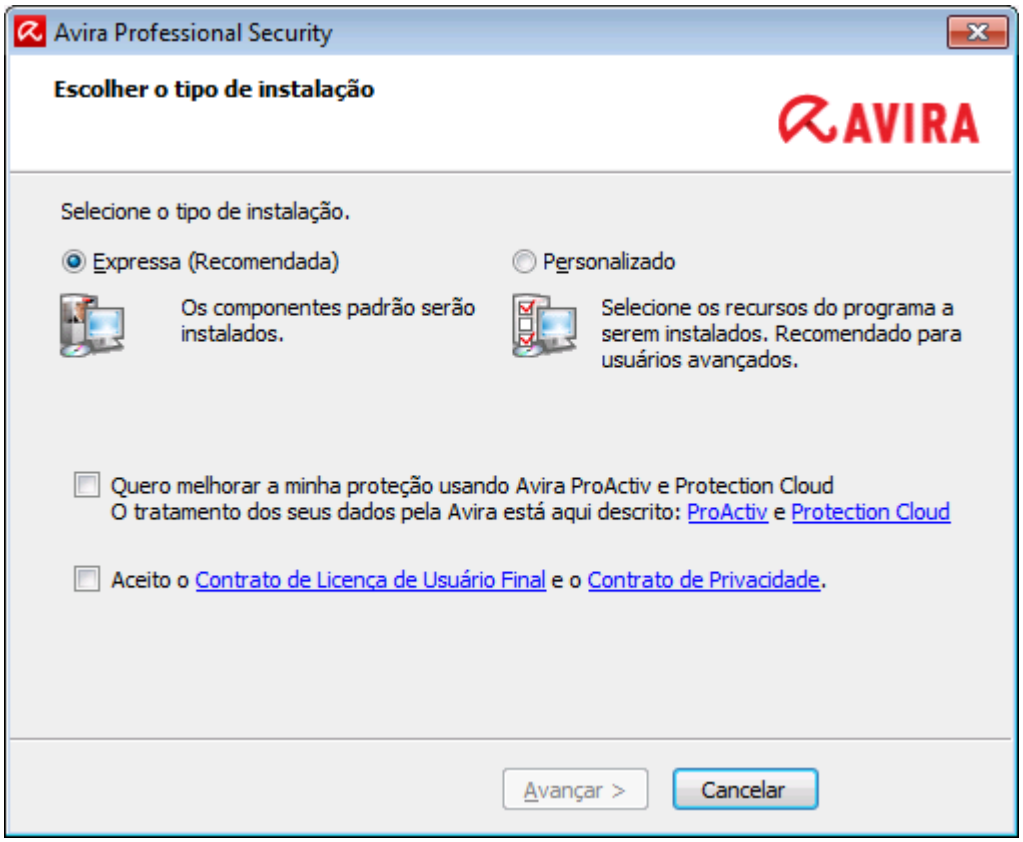
  Para alguns produtos, a desinstalação precisa ser confirmada manualmente.

  Selecione os programas e clique em **Avançar**.

  A desinstalação de um ou mais programas selecionados pode requerer a reinicialização do computador. Após a reinicialização, a instalação começará.

3.6 Selecionando um tipo de instalação

Durante a instalação, você pode escolher um tipo de instalação no assistente de instalação. O assistente de instalação é projetado para guiá-lo de modo fácil na instalação.



Tópicos relacionados:

- consulte Executando uma Instalação Expressa
- consulte Executando uma instalação personalizada

3.6.1 Executando uma Instalação Expressa

A *Instalação Expressa* é a rotina de instalação recomendada.

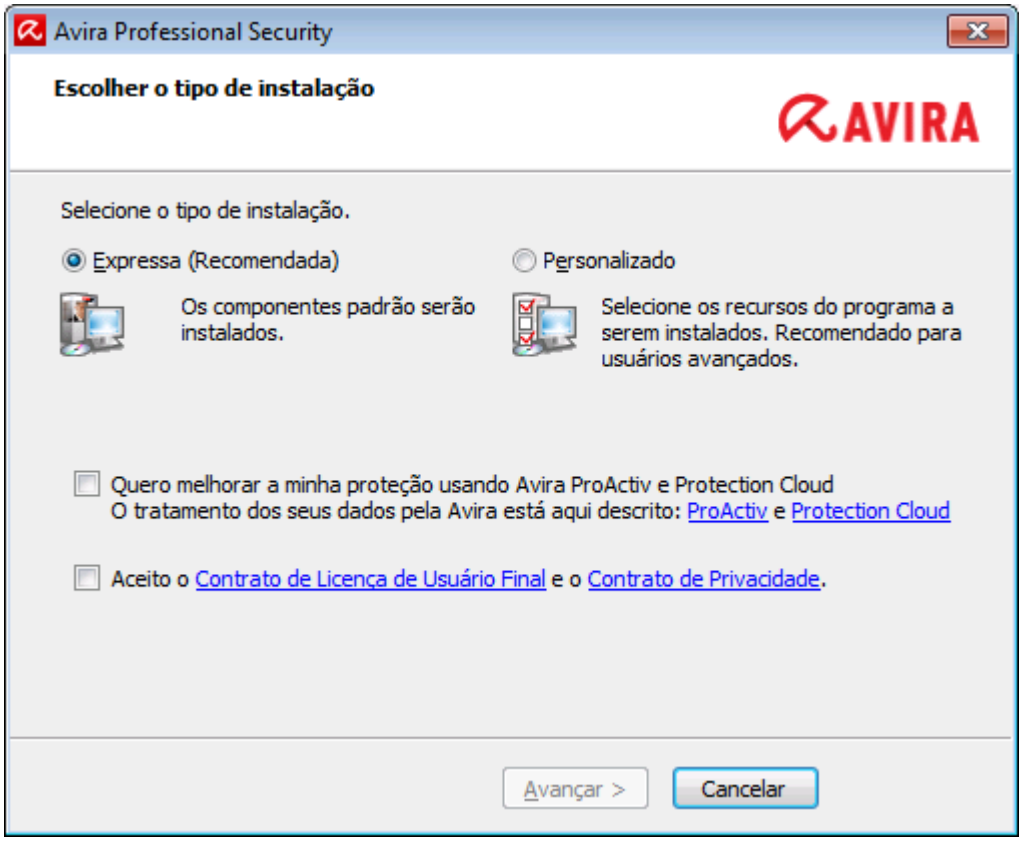
- Ela instala todos os componentes padrão do Avira Professional Security. As configurações de nível de segurança recomendadas do Avira são usadas.
- Como padrão, um dos caminhos de instalação a seguir é escolhido:
  - *C:\Program Files\Avira* (para versões Windows 32 bits) ou
  - *C:\Program Files (x86)\Avira* (para versões Windows 64 bits)
- Aqui, você pode encontrar todos os arquivos relacionados ao Avira Professional Security.
- Se escolher este tipo de instalação, você poderá efetuar uma instalação apenas clicando em **Avançar** até concluir.
- Este tipo de instalação é projetado especialmente para os usuários que não se sentem confortáveis em configurar ferramentas de software.

3.6.2 Executando uma instalação personalizada

A *Instalação Personalizada* permite configurar a instalação. Isso só é recomendado para usuários avançados que estejam bem familiarizados com softwares e hardwares, assim como com questões de segurança.

- Você pode escolher instalar componentes de programa individuais.
- 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 grupo de programa no menu Iniciar**.
- Usando o assistente de configuração, você pode definir as configurações para o Avira Professional Security. Você também pode escolher o nível de segurança com o qual esteja confortável.
- Após a instalação, você pode iniciar uma pequena varredura de sistema que é efetuada automaticamente após a instalação.

3.7 Instalando o Avira Professional Security



- Se você não quiser participar da Comunidade Avira, desmarque a caixa de marcação **Eu quero melhorar minha proteção usando o Avira ProActiv e o Protection Cloud**, marcados por padrão.

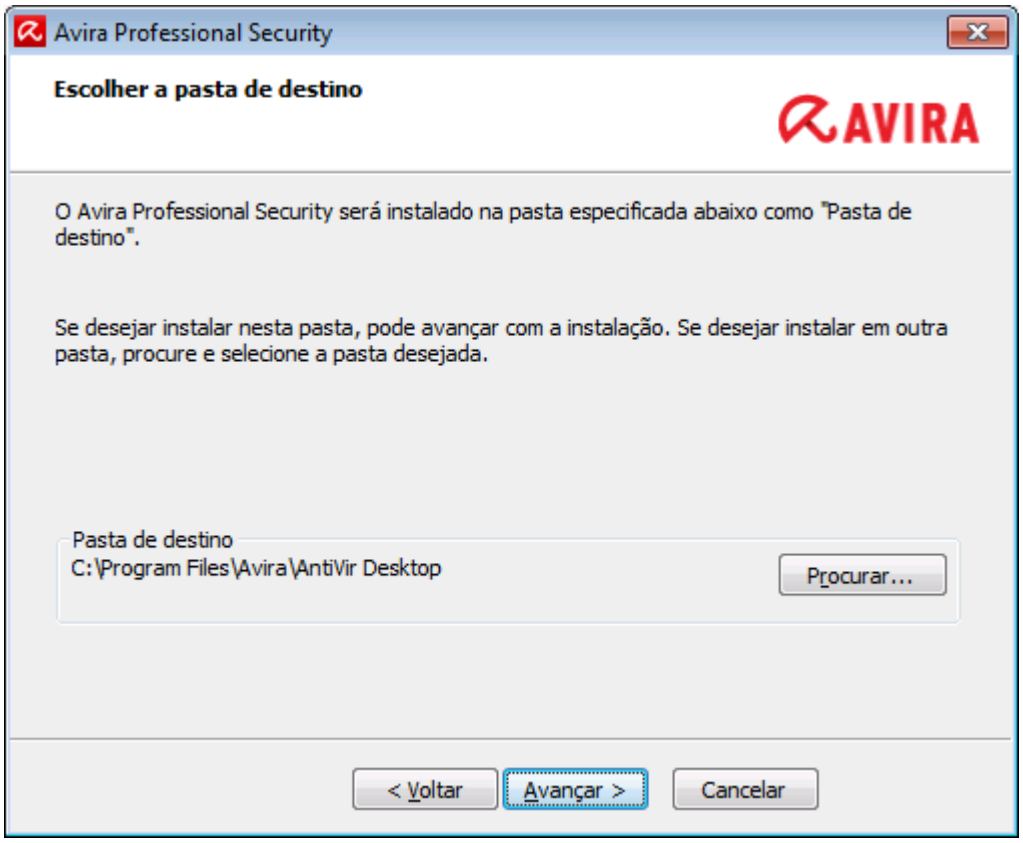
Se você confirmar sua participação na Comunidade Avira, o Avira Professional Security enviará dados sobre programas suspeitos detectados ao Avira Malware Research Center. Os dados são usados somente para uma varredura online avançada e para expandir e aperfeiçoar a tecnologia de detecção.

Você pode clicar nos links **ProActiv** e **Protection Cloud** para obter mais detalhes sobre a varredura online expandida e em nuvem.

Confirme se aceita o **Contrato de Licença do Usuário Final**. Para ler o texto detalhado do **Contrato de Licença do Usuário Final**, clique no link.

3.7.1 Escolhendo uma pasta de destino

A instalação personalizada permite escolher a pasta na qual deseja instalar o Avira Professional Security.



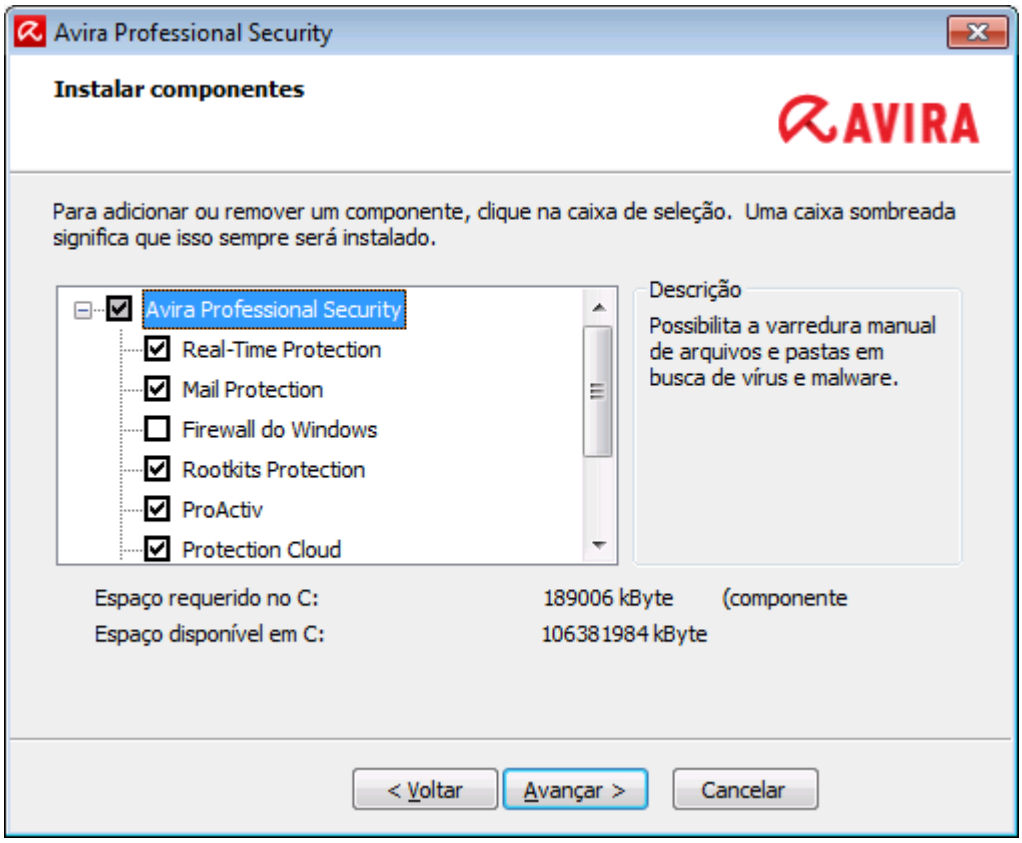
- Clique em **Procurar** e navegue até o local onde deseja instalar o Avira Professional Security.

  Selecione a pasta na qual deseja instalar o Avira Professional Security na janela **Escolher pasta de destino**.

  Clique em **Avançar**.

3.7.2 Escolhendo componentes de instalação

Em uma instalação personalizada ou uma modificação de instalação, os componentes de instalação a seguir podem ser selecionados, adicionados ou removidos.



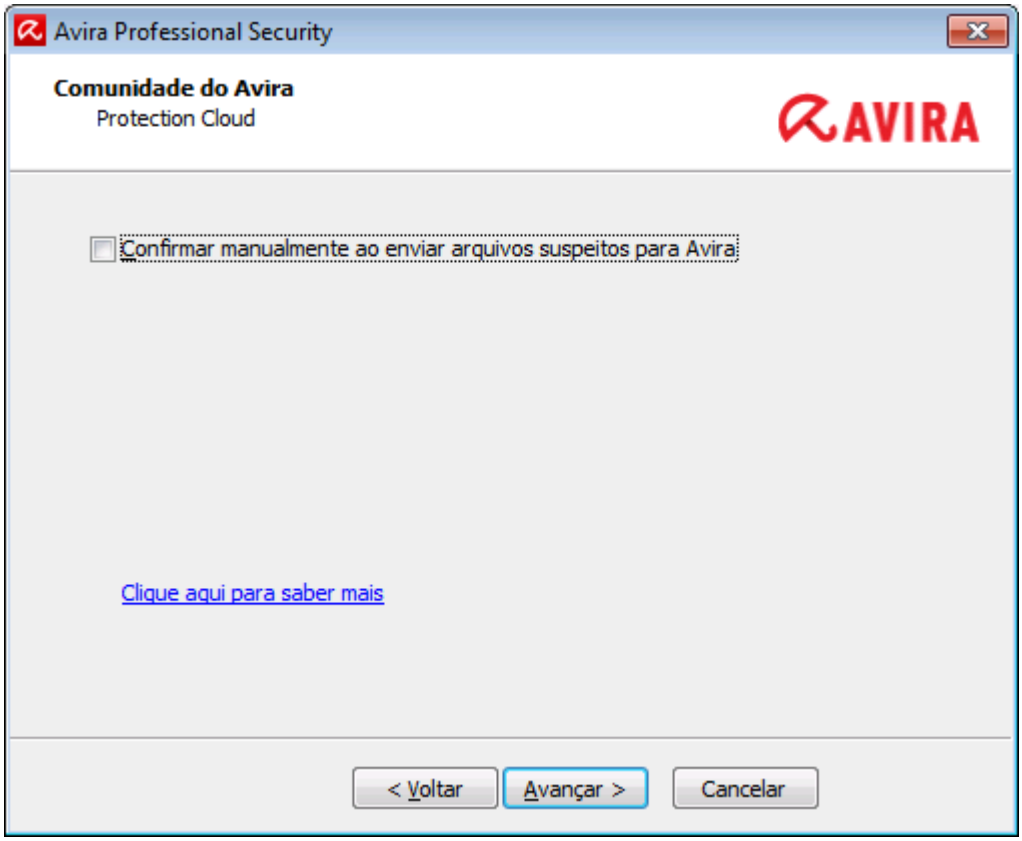
Selecione ou cancele componentes da lista na caixa de diálogo de Instalar componentes.

- **Avira Professional Security**
  Ele contém todos os componentes necessários para uma instalação bem-sucedida do Avira Professional Security.
  - **Real-Time Protection**
    O Avira Real-Time Protection é executado em segundo plano. Ele monitora e repara, se possível, os arquivos durante operações como abrir, gravar e copiar no "modo de acesso". O modo de acesso significa que, sempre que o usuário realiza uma operação de arquivo (por exemplo, carregar documento, executar, copiar), o Avira Professional Security verifica o arquivo automaticamente. Renomear o arquivo, entretanto, não dispara uma verificação pelo Avira Real-Time Protection.
  - **Mail Protection**
    O Mail Protection é a interface entre seu computador e o servidor de e-mail a partir da qual seu programa de e-mail (cliente de e-mail) baixa os e-mails. O Mail Protection é conectado como um proxy entre o programa de e-mail e o servidor de e-mail. Todos os e-mails recebidos passam por esse proxy, é feita a verificação de vírus e programas indesejados, e depois encaminhados ao programa de e-mail. Dependendo da configuração, o programa processa os e-mails afetados automaticamente ou solicita a você uma determinada ação.

- **Avira FireWall** (até o Windows XP)
  o Avira FireWall controla a comunicação de entrada e saída do computador. Ele permite ou nega comunicações com base em políticas de segurança.
- **Firewall do Windows** (a partir do Windows 7)
  Este componente gerencia o Firewall do Windows a partir do Avira Professional Security.
- **Rookits Protection**
  O Avira Rookits Protection verifica se há software já instalado no computador que não possa mais ser detectado com métodos convencionais de proteção contra malware depois da invasão do sistema do computador.
- **ProActiv**
  O componente ProActiv monitora ações do aplicativo e alerta os usuários quanto ao comportamento de aplicativo suspeito. Esse reconhecimento baseado em comportamento permite que você se proteja contra malware desconhecido. O componente ProActiv está integrado ao Avira Real-Time Protection.
- **Protection Cloud**
  O componente Protection Cloud é um módulo para detecção online dinâmica de malware ainda desconhecido. Isso significa que os arquivos são carregados em um local remoto e comparados a arquivos conhecidos, assim como a outros arquivos que estão sendo enviados e analisados em tempo real (não programado e sem atraso). Desta forma, o banco de dados é atualizado constantemente e, consequentemente, um nível mais alto de segurança pode ser fornecido.
  Se você escolheu instalar o componente Protection Cloud mas deseja confirmar manualmente quais arquivos devem ser enviados para a Nuvem para análise, você pode ativar a opção **Confirmar manualmente ao enviar arquivos suspeitos para Avira**.
- **Web Protection**
  Ao navegar pela Internet, você está usando seu navegador da Web 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 são movidos diretamente no cache do navegador para serem exibidos no navegador da Web, de forma que uma verificação de acesso realizada pelo Avira Real-Time Protection não é possível. Isso poderia permitir o acesso de vírus e programas indesejados ao sistema do computador. O Web Protection é um proxy HTTP que monitora as portas usadas para transferência de dados (80, 8080, 3128) e verifica os dados transferidos em busca de vírus e programas indesejados. Dependendo da configuração, o programa pode processar os arquivos afetados automaticamente ou solicitar uma ação específica ao usuário.
- **Extensão do shell**
  O Extensão do shell gera uma entrada **Varredura de arquivos selecionados com o Avira** no menu contextual do Windows Explorer (botão direito do mouse). Com essa entrada, é possível verificar arquivos ou diretórios diretamente.

Tópicos relacionados:
Alterando uma instalação

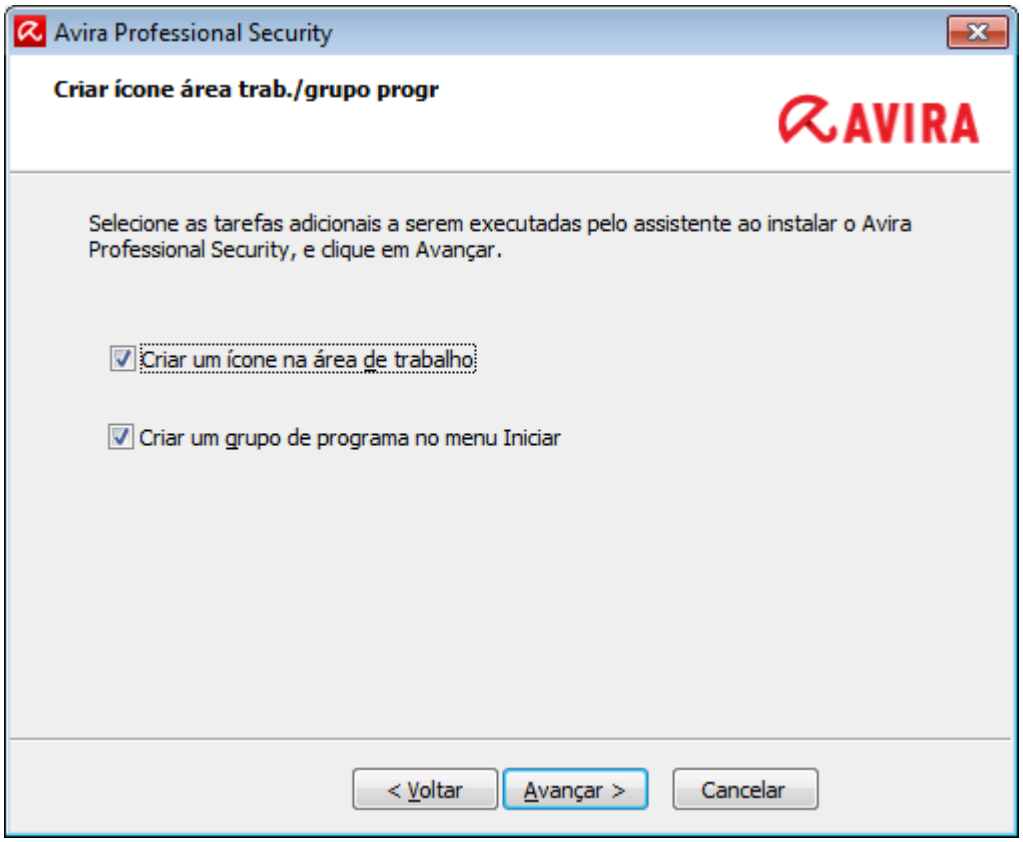
Se você decidiu participar da Comunidade da Avira, você pode escolher confirmar manualmente o carregamento cada vez que um arquivo for enviado para o Malware Research Center Avira.



- Para que o Avira Professional Security peça sempre confirmação, ative a opção **Confirme manualmente ao enviar arquivos suspeitos para a Avira**.

3.7.3 Criando atalhos para o Avira Professional Security

Um ícone na área de trabalho e/ou um grupo de programa no menu Iniciar ajudam você a acessar o Avira Professional Security de modo mais fácil e rápido.



- Para criar um atalho na área de trabalho para o Avira Professional Security e/ou um grupo de programa no **menu Iniciar** deixe a opção ativada.

3.7.4 Ativando o Avira Professional Security

Há várias formas de ativar o Avira Professional Security.

Se você já recebeu um código de ativação, insira-o nos campos fornecidos.

- Se você ainda precisa obter um código de ativação, clique no link compre uma chave de ativação.

  Você será encaminhado para o site do Avira, onde poderá adquirir o código de ativação.

- Se você deseja apenas testar o produto, selecione **Testar produto** e insira seus dados nos campos necessários para registro.

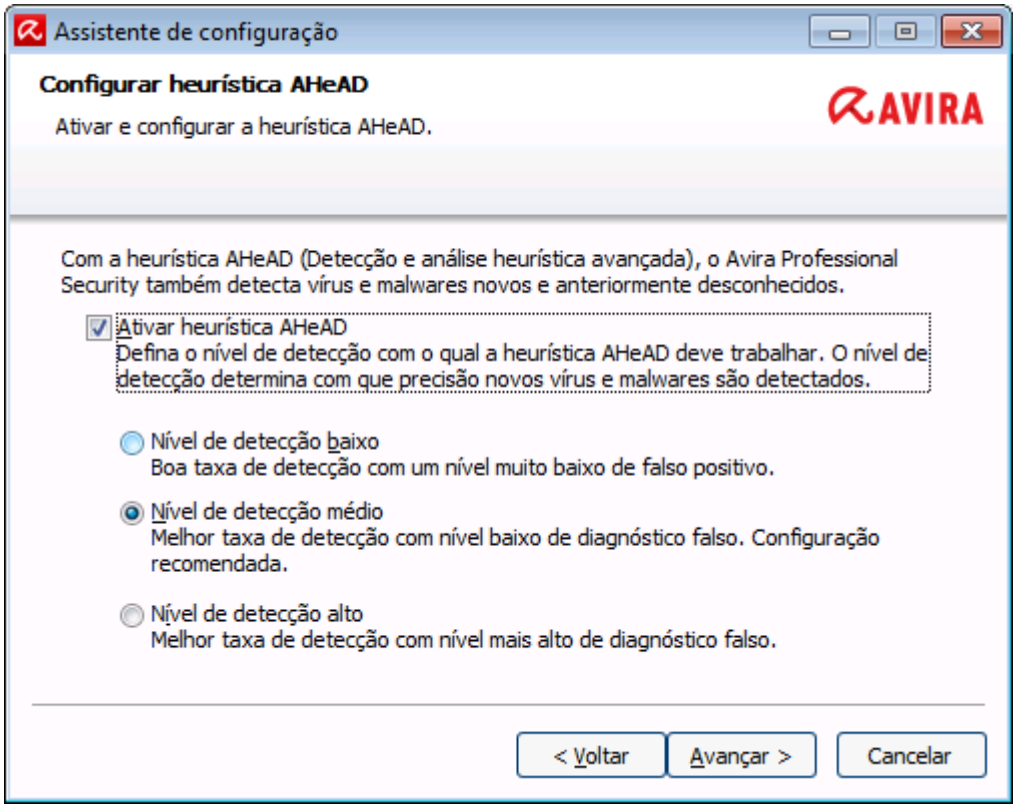
  Sua licença de avaliação é válida por 31 dias.

- Se você já tiver ativado um produto e desejar reinstalar o produto Avira, selecione a opção **Eu já tenho um arquivo de licença válido**.

  Uma janela do navegador se abrirá e você poderá navegar para o arquivo *hbedv.key* no seu sistema.

3.7.5 Configurando o nível de detecção heurística (AHeAD)

O Avira Professional Security possui uma ferramenta muito poderosa na forma de tecnologia Avira AHeAD (*Análise e Detecção Heurística Avançada*). Essa tecnologia usa técnicas de reconhecimento de padrões para detectar malwares desconhecidos (novos) a partir da análise anterior de outros malwares.

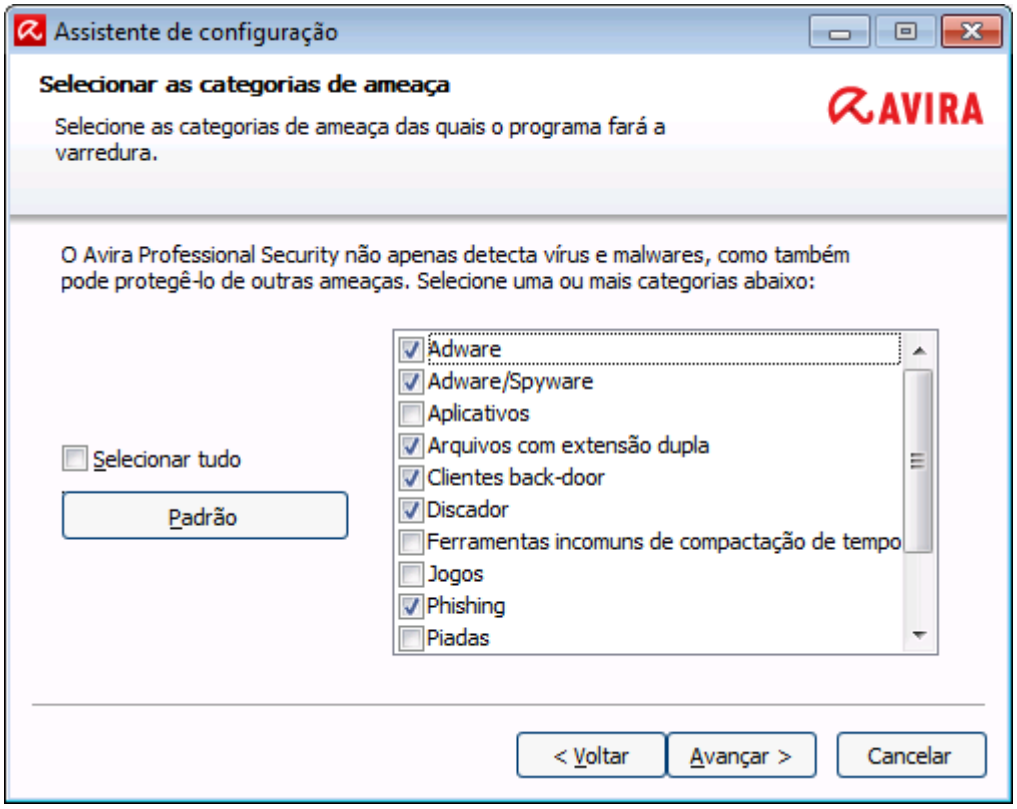


- Selecione um nível de detecção na caixa de diálogo **Configurar AHeAD** e clique em **Avançar**.

  O nível de detecção selecionado é usado para as configurações da tecnologia AHeAD System Scanner (verificação por demanda) e Real-Time Protection (verificação por acesso).

3.7.6 Selecionando categorias de ameaça estendida

Vírus e malware não são ameaças que representam perigo apenas ao sistema do computador. Nós definimos uma lista de riscos e os classificamos em categorias de ameaça estendida para você.



- Um número de categorias de ameaças já é pré-selecionado por padrão.

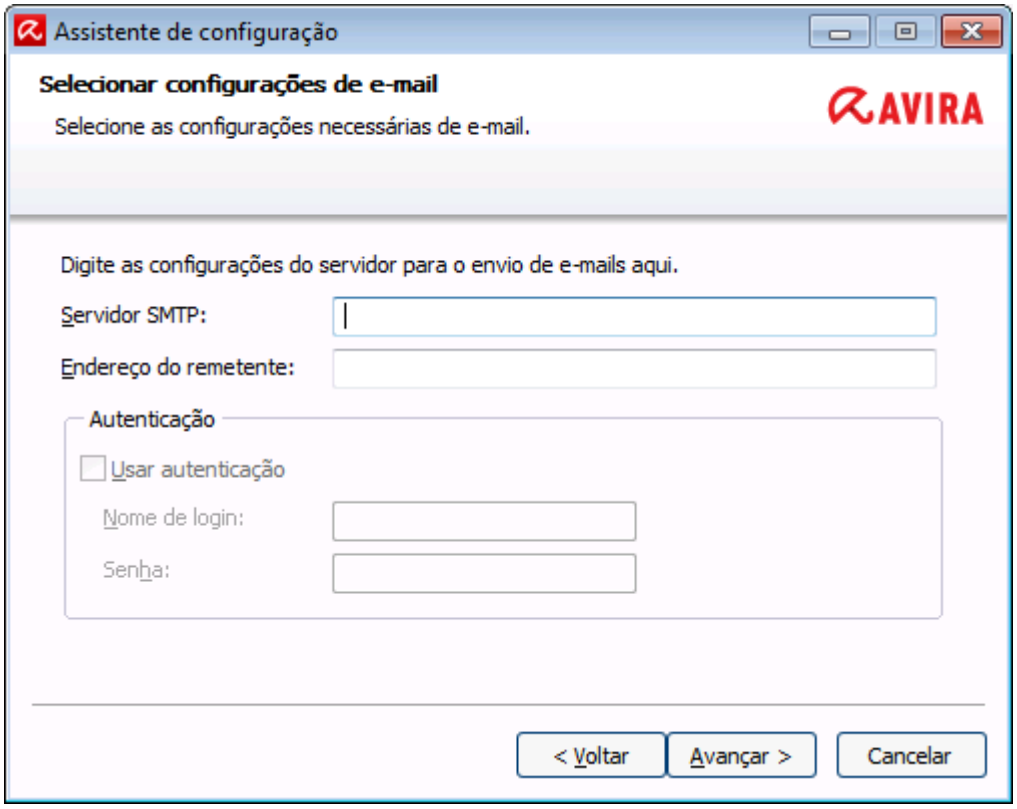
  Onde seja adequado, ative mais categorias de ameaça na caixa de diálogo **Selecionar categorias de ameaça estendida**.

  Se você mudar de ideia, reverta para os valores recomendados clicando no botão **Valores padrão**.

  Continue a instalação clicando em **Avançar**.

3.7.7 Selecionando as configurações de e-mail

O Avira Professional Security usa SMTP para enviar e-mails, encaminhar objetos suspeitos da Quarentena para o Avira Malware Research Center, bem como enviar alertas de e-mail.



- Se você quiser enviar esses e-mails automáticos através de SMTP, defina as configurações do servidor para o envio de e-mails na caixa de diálogo **Selecionar configurações de e-mail**.

Servidor SMTP

Insira o nome do computador ou o endereço IP do servidor SMTP que deseja usar.

Exemplos:

Endereço: smtp.company.com

Endereço: 192.168.1.100

Endereço do remetente

Insira o endereço de e-mail do remetente.

Autenticação

Alguns servidores de e-mail esperam que um programa verifique o servidor (faça login) antes que o e-mail seja enviado. Alertas podem ser transmitidos com autenticação para um servidor SMTP via e-mail.

Autenticação de usuário

Se essa opção for ativada, um nome de usuário e uma senha podem ser inseridos nas caixas relevantes para logon (autenticação).

Nome de logon:

Insira seu nome de usuário aqui.

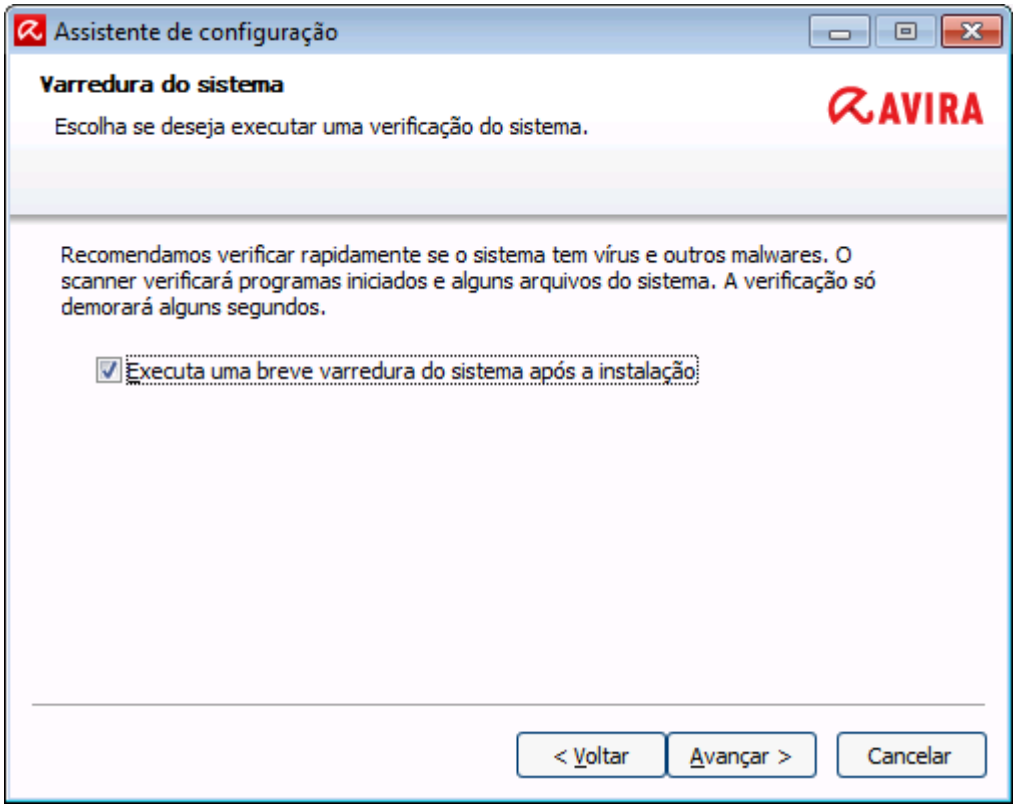
Senha:

Insira a senha relevante aqui. A senha é salva na forma criptografada. Por motivos de segurança, os caracteres reais digitados neste espaço são substituídos por asteriscos (*).

Clique em **Avançar**.

3.7.8 Iniciando uma varredura após a instalação

Para verificar o estado de segurança atual do computador, uma varredura rápida do sistema pode ser efetuada após a configuração ser concluída e antes do computador ser reinicializado. O System Scanner verifica os programas em execução e os arquivos de sistema mais importantes em busca de vírus e malware.



- Se você quiser efetuar uma varredura rápida do sistema, deixe a opção **Varredura rápida do sistema** ativada.

  Clique em **Avançar**.

  Complete a configuração clicando em **Concluir**.

  Se você não desativar a opção **Varredura rápida do sistema**, a janela *Luke Filewalker* abre.

  O System Scanner executa uma varredura rápida do sistema.

3.7.9 Instalação na rede

Para simplificar a instalação de produtos Avira em uma rede com diversos computadores de cliente para o administrador do sistema, seu produto Avira possui um procedimento especial para a instalação inicial e a instalação de modificação.

Para 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
Observe que um arquivo de licença é obrigatório para a instalação inicial na rede.

Observação
Observe que um pacote de instalação para o produto Avira é necessário para 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 facilmente na rede com um script de logon do servidor ou via SMS.

Para obter informações sobre instalação e desinstalação na rede:

- consulte o Capítulo: Parâmetros da linha de comandos 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 uma 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/

Instalação na Rede

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 atualizar

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

Observação
Ao instalar em um sistema operacional de servidor, o Real-Time Protection e a proteção de arquivos não estão disponíveis.

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 logon do servidor.

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

  ↪ A instalação é iniciada automaticamente.

Parâmetros de linha de comandos para o programa de instalação

Observação
Parâmetros contendo caminhos ou nomes de arquivo devem ser colocados entre 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:\logfiles\unsetup.log"`

Parâmetros do arquivo *setup.inf*

No arquivo de controle *setup.inf*, você pode configurar os parâmetros a seguir no campo [DATA] para a instalação automática do produto Avira. A sequência dos parâmetros não é importante. Se uma configuração de parâmetro estiver ausente ou incorreta, a rotina de instalação é interrompida e uma mensagem de erro é exibida.

> **Observação**
> Parâmetros contendo caminhos ou nomes de arquivo devem ser colocados entre aspas duplas (Exemplo: `InstallPath="%PROGRAMFILES%\Avira\AntiVir Server\"`).

- `DestinationPath`

  Caminho de destino no qual o programa é instalado. Deve ser incluído no script. Observe que a configuração 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:\Arquivos de Programas\Avira\AntiVir Desktop`

- `ProgramGroup`

  Cria um grupo de programas para todos os usuários do computador no menu Iniciar do Windows.
  `1`: Criar grupo de programas
  `0`: Não criar grupo de programas
  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 da área de trabalho

0: Não criar ícone da 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 malware através do menu contextual do botão direito do mouse.
  1: Registrar extensão do shell
  0: Não registrar extensão do shell
  Exemplo: ShellExtension=1

- Guard

  Instala o Avira Real-Time Protection (Scanner no acesso).
  1: Instalar Avira Real-Time Protection
  0: Não instalar Avira Real-Time Protection
  Exemplo: Guard=1

- MailScanner

  Instala o Avira Mail Protection.
  1: Instalar Avira Mail Protection
  0: Não instalar Avira Mail Protection
  Exemplo: MailScanner=1

- KeyFile

  Especifica o caminho para o arquivo de licença que é copiado durante a instalação. Para a instalação inicial: obrigatório. O nome do arquivo deve ser especificado por completo (totalmente qualificado). (Para uma instalação de modificação: 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. Esta entrada tem uma prioridade mais alta do que ShowRestartMessage.
  1: Reiniciar computador
  0: Não reiniciar 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 realizada. Especifica o tipo de instalação. Se uma instalação já estiver disponível, ela precisará ser indicada no `SetupMode` se esta instalação for apenas uma atualização ou uma instalação de modificação (reconfiguração) ou uma desinstalação.
  `Atualizar`: Atualiza uma instalação existente. Nesse caso, os parâmetros de configuração, por exemplo Guard, são ignorados.
  `Modificar`: Modifica (reconfigura) uma instalação existente. No processo, nenhum arquivo é copiado no caminho de destino.
  `Remover`: Desinstala seu produto Avira do sistema.
  Exemplo: `SetupMode=Update`

- `AVWinIni (opcional)`

  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`

- `Senha`

  Essa opção atribui a senha que foi definida para a instalação (modificação) e desinstalação para a rotina de configuração. 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: `Senha=Password123`

- `WebGuard`

  Instala o Avira Web Protection.
  `1`: Instalar Avira Web Protection
  `0`: Não instalar Avira Web Protection
  Exemplo: `WebGuard=1`

- `RootKit`

  Instala o módulo do Avira Rootkits Protection. Sem o Avira Rootkits Protection, o Scanner não conseguirá verificar rootkits no sistema!
  `1`: Instalar Avira Rootkits Protection
  `0`: Não instalar Avira Rootkits Protection
  Exemplo: `RootKit=1`

- `ProActiv`

  Instala o componente Avira ProActiv. Avira ProActiv é uma tecnologia de detecção baseada em padrão que permite que malware ainda desconhecido seja detectado.
  `1`: Instalar ProActiv
  `0`: Não instalar ProActiv
  Exemplo: `ProActiv=1`

- `FireWall`

Instala o componente Avira FireWall (até o Windows 7). O Avira FireWall monitora e controla o tráfego de dados recebidos e enviados no seu sistema de computador e protege seus computadores contra ameaças originadas da Internet ou de outros ambientes de rede.
`1`: Instalar FireWall
`0`: Não instalar FireWall
Exemplo: `FireWall=1`

- `MgtFirewall`

  Instala o componente de gerenciamento do Firewall do Windows. A partir do Windows 8, o Avira Professional Security não inclui o Avira FireWall. O Firewall do Windows agora é gerenciado com o produto Avira.
  `1`: Instala o componente de gerenciamento do Firewall do Windows
  `0`: Não instala o componente de gerenciamento do Firewall do Windows
  Exemplo: `MgtFirewall=1`

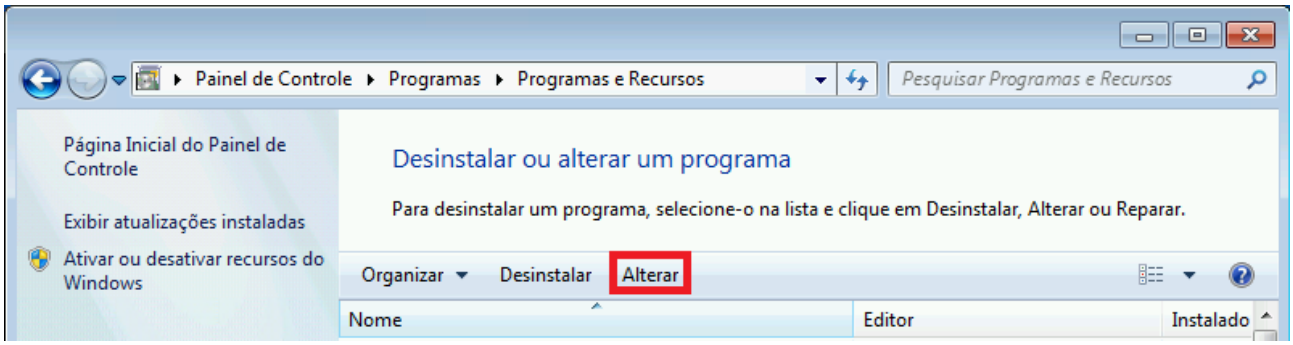
3.8 Alterando a instalação

Se quiser adicionar ou remover módulos da instalação atual, você pode fazer isso sem precisar desinstalar o Avira Professional Security. Segue o guia:

- Alterando uma instalação no Windows 8
- Alterando uma instalação no Windows 7
- Alterando uma instalação no Windows XP

3.8.1 Alterando uma instalação no Windows 8

Você tem a opção de adicionar ou remover componentes de programa individuais na instalação do Avira Professional Security (consulte Escolhendo componentes de instalação).



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

- Clique com o botão direito do mouse na tela.

O símbolo **Todos os aplicativos** aparecerá.

Clique no símbolo e procure na seção *Aplicativos - Sistema Windows* o **Painel de Controle**.

Clique duas vezes no símbolo do **Painel de Controle**.

Clique em **Programas - Desinstalar um programa**.

Clique em **Programas e Recursos - Desinstalar um programa**.

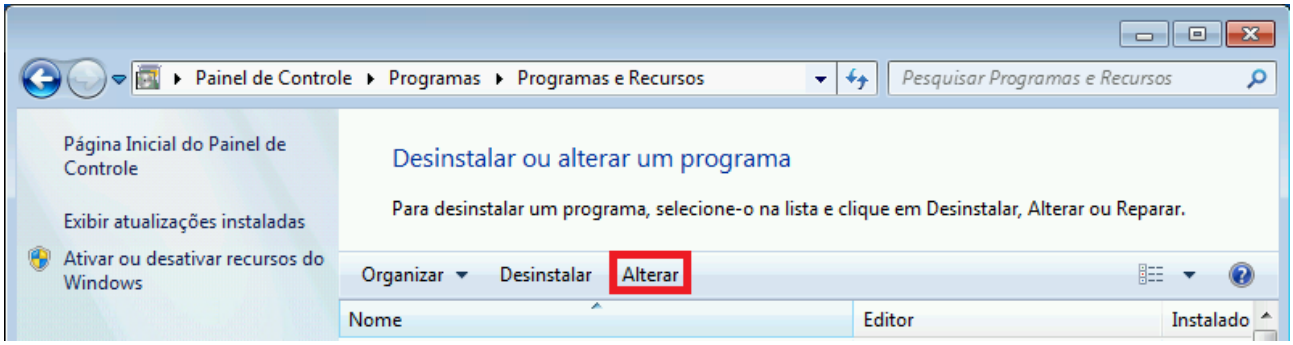
Selecione Avira Professional Security e clique em **Alterar**.

No diálogo **Bem-vindo** do programa, selecione a opção **Modificar**. Você será orientado pelas alterações de instalação.

Tópicos relacionados:
Escolhendo componentes de instalação

3.8.2 Alterando uma instalação no Windows 7

Você tem a opção de adicionar ou remover componentes de programa individuais na instalação do Avira Professional Security (consulte Escolhendo componentes 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.

- Abra o **Painel de Controle** através do menu **Iniciar** do Windows.

  Clique duas vezes em **Programas e Recursos**.

  Selecione Avira Professional Security e clique em **Alterar**.

  No diálogo **Bem-vindo** do programa, selecione a opção **Modificar**. Você será orientado pelas alterações de instalação.

Tópicos relacionados:
Escolhendo componentes de instalação

3.8.3 Alterando uma instalação no Windows XP

Você tem a opção de adicionar ou remover componentes de programa individuais na instalação do Avira Professional Security (consulte Escolhendo 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.

- Abra o **Painel de Controle** através do menu **Iniciar > Configurações** do Windows.

  Clique duas vezes em **Adicionar ou Remover Programas**.

  Selecione Avira Professional Security e clique em **Alterar**.

  No diálogo **Bem-vindo** do programa, selecione a opção **Modificar**. Você será orientado pelas alterações de instalação.

Tópicos relacionados:
Escolhendo componentes de instalação

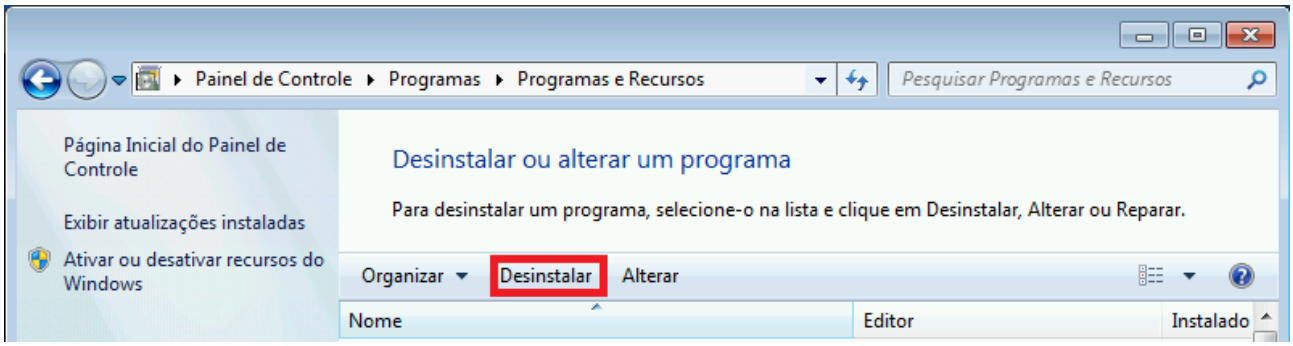
3.9 Desinstalação

Se você achar que precisa desinstalar o Avira Professional Security, aqui está como fazer isso:

- Desinstalando Avira Professional Security no Windows 8
- Desinstalando Avira Professional Security no Windows 7
- Desinstalando Avira Professional Security no Windows XP

3.9.1 Desinstalando o Avira Professional Security no Windows 8

Para desinstalar o Avira Professional Security do seu computador, use a opção **Programas e Recursos** no Painel de Controle do Windows.



- Clique com o botão direito do mouse na tela.

  O símbolo **Todos os aplicativos** aparecerá.

  Clique no símbolo e procure na seção *Aplicativos - Sistema Windows* o **Painel de Controle**.

Clique duas vezes no símbolo do **Painel de Controle**.

Clique em **Programas - Desinstalar um programa**.

Clique em **Programas e Recursos - Desinstalar um programa**.

Selecione Avira Professional Security na lista e clique em **Desinstalar**.

Ao ser perguntado se deseja realmente remover o aplicativo e todos os seus componentes, clique em **Sim** para confirmar.

Ao ser perguntado se deseja ativar o Firewall do Windows (o Avira FireWall será desinstalado), clique em **Sim** para confirmar e manter ao menos alguma proteção no seu sistema.

Todos os componentes do programa serão removidos.

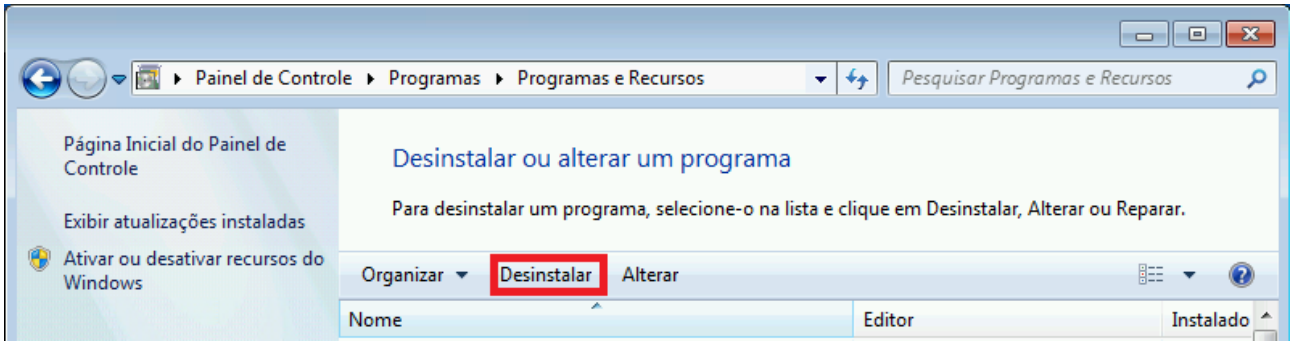
Clique em **Concluir** para concluir a desinstalação.

Se uma caixa de diálogo aparecer recomendando a reinicialização do computador, clique em **Sim** para confirmar.

O Avira Professional Security agora está desinstalado e todos os diretórios, arquivos e entradas de registro para o programa serão excluídos quando o computador for reiniciado.

3.9.2 Desinstalando o Avira Professional Security no Windows 7

Para desinstalar o Avira Professional Security do seu computador, use a opção **Programas e Recursos** no Painel de Controle do Windows.



- Abra o **Painel de Controle** através do menu **Iniciar** do Windows.

  Clique em **Programas e Recursos**.

  Selecione Avira Professional Security na lista e clique em **Desinstalar**.

  Ao ser perguntado se deseja realmente remover o aplicativo e todos os seus componentes, clique em **Sim** para confirmar.

  Ao ser perguntado se deseja ativar o Firewall do Windows (o Avira FireWall será desinstalado), clique em **Sim** para confirmar e manter ao menos alguma proteção no seu sistema.

  Todos os componentes do programa serão removidos.

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

Se uma caixa de diálogo aparecer recomendando a reinicialização do computador, clique em **Sim** para confirmar.

O Avira Professional Security agora está desinstalado e todos os diretórios, arquivos e entradas de registro para o programa serão excluídos quando o computador for reiniciado.

3.9.3 Desinstalando o Avira Professional Security no Windows XP

Para desinstalar o Avira Professional Security do seu computador, use a opção **Alterar ou Remover Programas** no Painel de Controle do Windows.

- Abra o **Painel de Controle** através do menu **Iniciar > Configurações** do Windows.

  Clique duas vezes em **Adicionar ou Remover Programas**.

  Selecione Avira Professional Security na lista e clique em **Remover**.

  Ao ser perguntado se deseja realmente remover o aplicativo e todos os seus componentes, clique em **Sim** para confirmar.

  Todos os componentes do programa serão removidos.

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

  Se uma caixa de diálogo aparecer recomendando a reinicialização do computador, clique em **Sim** para confirmar.

  O Avira Professional Security agora está desinstalado e todos os diretórios, arquivos e entradas de registro para o programa serão excluídos quando o computador for reiniciado.

3.9.4 Desinstalação na Rede

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 logon do servidor.

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

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

  ↪ A desinstalação é iniciada automaticamente.

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

4. Visão geral do Avira Professional Security

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

- consulte o Capítulo Interface de Usuário e Operação
- consulte o Capítulo Como...?

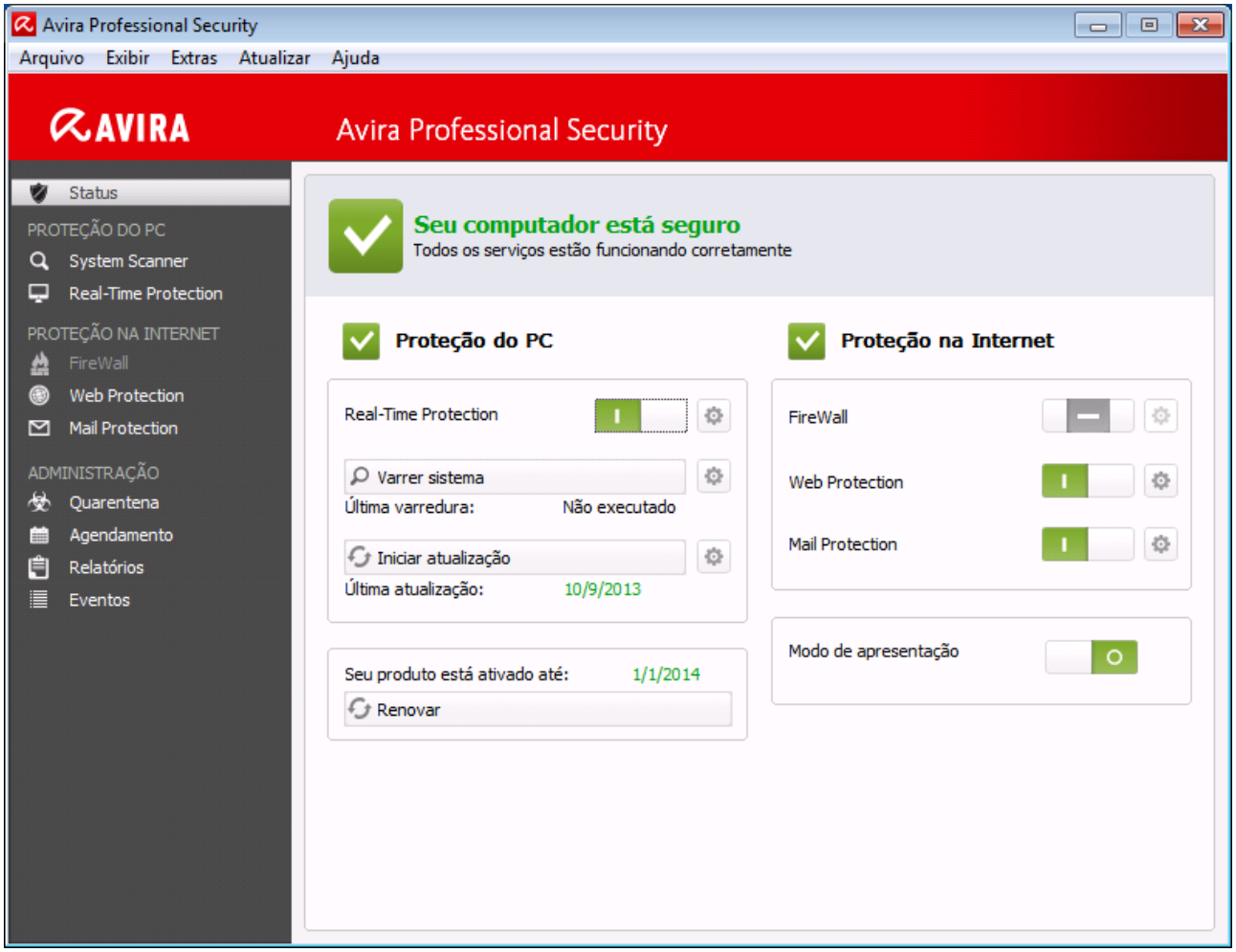
4.1 Interface de Usuário e Operação

Você opera seu produto Avira por meio de três elementos da interface do programa:

- Centro de Controle: monitorando e controlando o produto Avira
- Configuração: Configurando o produto Avira
- Ícone de Bandeja na bandeja do sistema da barra de tarefas: Abrindo 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 **Área de Navegação** e a janela de detalhes **Status**:

- **Barra de Menus:** Na barra de menus do Centro de Controle, você pode acessar funções gerais do programa e informações sobre o programa.
- **Área de Navegação:** Na área de navegação, você pode alternar facilmente 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 DO PC* - Seção **Real-Time Protection**.
- **Status:** O Centro de Controle é aberto com a exibição **Status**, na qual você pode ver rapidamente se seu computador está saguro e você tem uma visão geral dos módulos ativos, a data do último backup e a data da última varredura do sistema. A exibição **Status** também contém botões para iniciar recursos ou ações, tal como iniciar ou parar o **Real-Time Protection**.

Iniciando e fechando o Centro de Controle

Para iniciar o Centro de controle, as seguintes opções estão disponíveis:

- Clique duas vezes no ícone do programa na área de trabalho

- Através da entrada do programa no menu **Iniciar > Programas**.
- Através do Ícone da Bandeja de seu produto Avira.

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

Operar o Centro de Controle

Para navegar no Centro de Controle

- Selecione uma atividade na barra de navegação.
  - ↪ A atividade é aberta e outras seções são exibidas. A primeira seção da atividade é selecionada e exibida na visualização.
- Se necessário, clique em outra seção para exibi-la na janela de detalhes.

> **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 **Voltar** você ativa o item de menu ativo.
> Para abrir ou fechar menus no Centro de Controle ou para navegar dentro dos menus, você também pode usar as seguintes combinações de teclas: [**Alt**] + letra sublinhada no menu ou 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 destacar vários elementos (elementos nas colunas), mantenha pressionada a tecla **Ctrl** ou **Shift** enquanto seleciona os elementos.
- Clique no botão apropriado na barra superior da janela de detalhes para editar o objeto.

Visão Geral do Centro de Controle

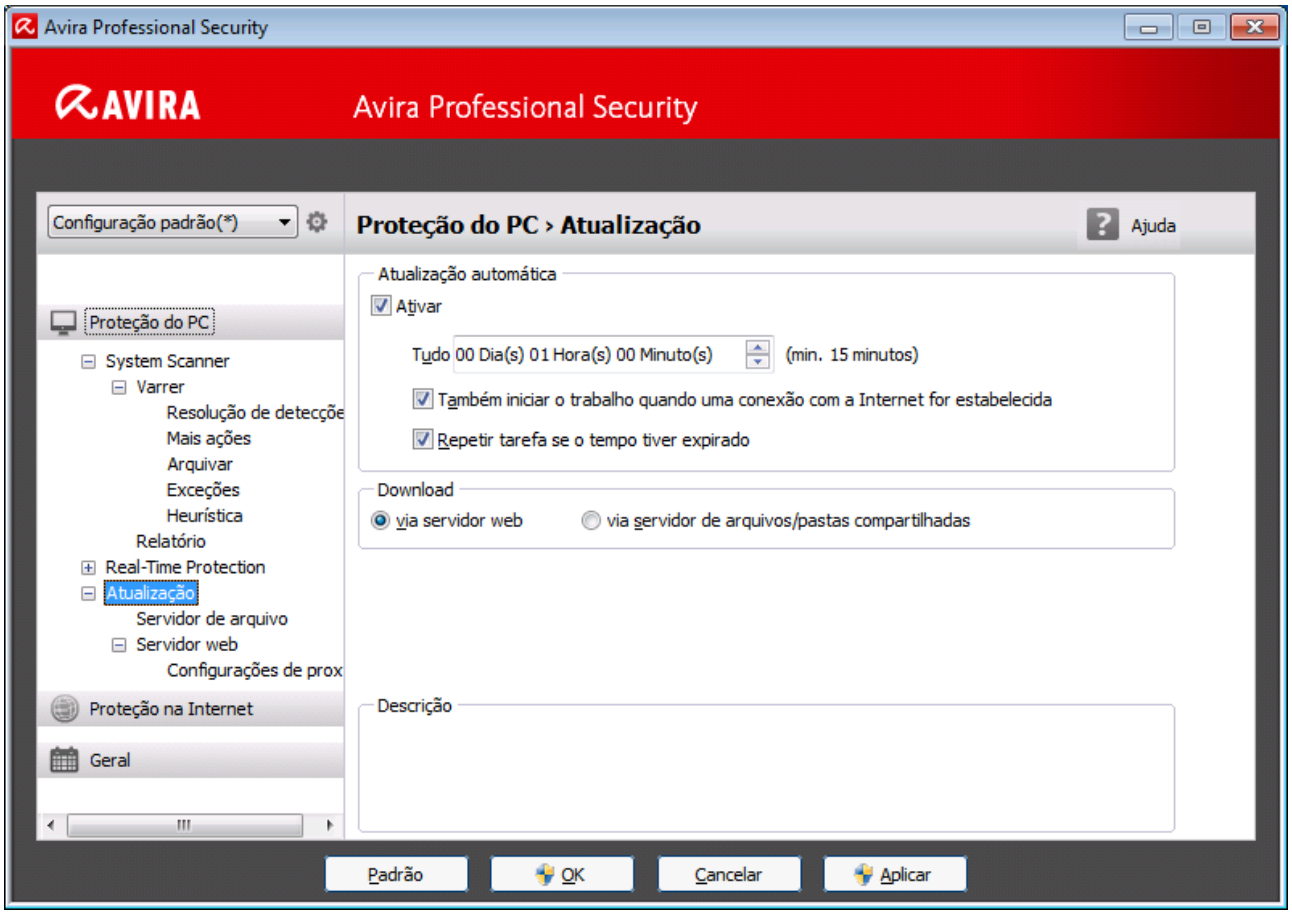
- **Status**: Clicar na barra **Status** fornece uma visão geral da funcionalidade do produto e do desempenho (consulte Status).
  - A seção **Status** permite ver rapidamente quais módulos estão ativos e fornece informações sobre a última atualização realizada.
- *PROTEÇÃO DO PC*: Nesta seção você localizará os componentes para verificar os arquivos em seu sistema do computador em busca de vírus e malwares.
  - A seção Scanner permite configurar e iniciar facilmente uma varredura por demanda. Perfis predefinidos ativa uma varredura com opções padrão já adaptadas. Do mesmo modo, é possível adaptar a varredura de vírus e programas indesejados de acordo com seus requisitos pessoais com a ajuda da seleção manual (será salva) ou com a criação de perfis definidos pelo usuário.

- A seção Real-Time Protection exibe informações sobre arquivos verificados, assim como outros dados estatísticos, que podem ser redefinidos a qualquer momento e permite acesso ao arquivo de relatório. Informações mais detalhadas sobre o último vírus ou programa indesejado detectado podem ser obtidas praticamente "com o clicar de um botão".

- *PROTEÇÃO NA INTERNET*: Nesta seção você localizará os componentes para proteger seu sistema do computador contra vírus e malwares da Internet e contra acesso à rede não autorizado.
  - A seção FireWall permite configurar as configurações básicas do FireWall. Além disso, são exibidos a taxa de transferência de dados atual e todos os aplicativos ativos que usam uma conexão de rede.
  - A seção Web Protection apresenta informações sobre URLs verificados e vírus detetados e outros dados estatísticos, que podem ser redefinidos a qualquer momento e permite o acesso ao arquivo de relatório. Informações mais detalhadas sobre o último vírus ou programa indesejado detectado podem ser obtidas praticamente "com o clicar de um botão".
  - A seção Mail Protection mostra todos os e-mails verificados pelo Mail Protection, suas propriedades e outros dados estatísticos. Também é possível excluir endereços de e-mail da futura varredura de malware ou spam. Os e-mails também podem ser excluídos do buffer do Mail Protection.
- *ADMINISTRAÇÃO*: Nesta seção você localizará ferramentas para isolar e gerenciar arquivos suspeitos ou infectados e para planejar tarefas recorrentes.
  - A seção Quarentena contém o conhecido gerenciador de quarentena. Este é o ponto central para os arquivos já colocados na quarentena ou para os arquivos suspeitos que deseja colocar na quarentena. Também é possível enviar um arquivo selecionado para o Avira Malware Research Center por e-mail.
  - A seção Agendamento permite configurar trabalhos programados de varredura e atualização, bem como trabalhos de backup, e adaptar ou excluir os trabalhos existentes.
  - A seção Relatórios permite visualizar os resultados de ações executadas.
  - A seção Eventos permite visualizar os eventos gerados por determinados módulos do programa.

4.1.2 Configuração

Você pode definir configurações para seu produto Avira na Configuração. Após a instalação. seu produto Avira é definido com configurações padrão, assegurando a proteção ideal para seu sistema do computador. No entanto, seu sistema do computador ou seus requisitos específicos para o produto Avira podem exigir que você adapte os componentes de proteção do programa.



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

Acessando a Configuração

Você tem várias opções para acessar a configuração:

- por meio do Painel de Controle do Windows.
- através da Central de Segurança do Windows - no Windows XP Service Pack 2.
- por meio do Ícone da Bandeja de seu 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

Operação de Configuração

Navegue na janela de configuração como 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 na frente da entrada para expandir a seção de configuração e exibir subseções de configuração na estrutura em árvore.
- Para ocultar subseções de configuração, clique no símbolo de subtração na frente da seção de configuração expandida.

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

Para confirmar as definições de Configuração:

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

  - OU -
- Clique em **Aplicar**.
  - ↪ As configurações são aplicadas. A janela de configuração permanece aberta.

Para concluir a configuração sem confirmar as definições:

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

Para restaurar todas as definições de configurações aos valores padrão:

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

Perfis de configuração

Você pode salvar suas opções de configuração como perfis de configuração. No perfil de configuração, por exemplo, de uma 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 tem a opção de definir regras para alternar para uma configuração específica:
Ao alternar a configuração usando um procedimento baseado em regra, a configuração pode ser vinculada ao uso de uma LAN ou conexão com a Internet (identificação através

do gateway padrão). Desse modo, os perfis de configuração podem ser criados para diferentes cenários de uso de notebooks:

- Usar em redes da empresa: Atualizar através do servidor de intranet, Web Protection desativado
- Usar em casa: Atualizar através do servidor da web da Avira, Web Protection ativado

Se nenhuma regra de comutação tiver sido definida, você poderá alternar para uma configuração manualmente no menu contextual do ícone da 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 contextual na seção de configuração.

Nota
O Controle de Conta de Usuário vai pedir a você permissão para habilitar ou desabilitar a Real-Time Protection, FireWall, Web Protection e serviços de Mail Protection nos sistemas operacionais a partir do Windows Vista.

Visão geral das opções de configuração

As seguintes opções de configuração estão disponíveis:

- **Scanner**: Configuração da varredura por demanda
  - Opções de varredura
  - Resolução de na detecções
  - Mais ações
  - Opções de varredura do arquivo
  - Exceções de varredura do sistema
  - Heurística de varredura do sistema
  - Configuração da função de registro
- **Real-Time Protection**: configuração de uma varredura durante o acesso
  - Opções de varredura
  - Resolução de na detecções
  - Mais ações
  - Exceções de varredura durante o acesso
  - Heurística de varredura durante o acesso
  - Configuração da função de registro
- **Atualização**: Configuração das configurações de atualização, faça o download através do Servidor Web ou servidor de arquivos
  - Fazer download através do servidor de arquivos
  - Fazer download através do servidor Web
  - Configurações de proxy

- **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 regra automática, parar o Firewall do Windows, notificações
  - Configurações de pop-up (alertas para acesso de rede por parte dos aplicativos)
- **Web Protection**: Configuração da Web Protection
  - Opções de varredura, ativação e desativação da Web Protection
  - Resolução de na detecções
  - Acesso bloqueado: Tipos de arquivo e tipos MIME indesejados, filtro da Web para URLs indesejados (malware, phishing etc.)
  - Exceções de varredura da Web Protection: URLs, tipos de arquivo, tipos MIME
  - Heurística de Web Protection
  - Configuração da função de registro
- **Mail Protection**: Configuração da Mail Protection
  - Opções de varredura: ativar o monitoramento das contas POP3, das contas IMAP, dos e-mails enviados (SMTP)
  - Ações na detecção
  - Mais ações
  - Heurística de varredura da Mail Protection
  - Função AntiBot: servidores SMTP permitidos, remetentes de e-mail permitidos
  - Exceções de varredura da Mail Protection
  - Configuração do cache, limpar cache
  - Configuração de um rodapé nos e-mails enviados
  - Configuração da função de registro
- **Geral**:
  - Configuração de e-mail usando SMTP
  - Categorias de ameaça para o Scanner e o Real-Time Protection
  - Proteção avançada: Opções para ativar os recursos do ProActiv e do Protection Cloud.
  - Filtro de aplicativos: bloquear ou permitir aplicativos
  - Proteção com senha para acesso ao Centro de controle e à Configuração
  - Segurança: bloquear função autostart, proteção do produto, proteger arquivo hosts do Windows
  - WMI: Ativar o suporte a WMI
  - Configuração do registro de eventos
  - Configuração das funções de registro
  - Configuração dos diretórios usados

- Alertas:

  Configuração de alertas de rede para componente(s):

  - Scanner
  - Real-Time Protection

  Configuração de alertas de e-mail para componente(s):

  - Scanner
  - Real-Time Protection
  - Atualizador
- Configuração de alertas acústicos emitidos quando malwares são detectados

4.1.3 Ícone de bandeja

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

Ícone	Descrição
	O Avira Real-Time Protection é ativado e o FireWall é ativado
	O Avira Real-Time Protection é desativado ou o FireWall é desativado

O ícone de bandeja exibe o status do serviço do Real-Time Protection e do FireWall.

As funções centrais de seu produto Avira podem ser acessadas rapidamente através do menu contextual do **ícone de bandeja**. Para abrir o menu contextual, clique no **ícone de bandeja** com o botão direito do mouse.

Entradas no menu contextual

- **Ativar Real-Time Protection**: Ativa ou desativa o Avira Real-Time Protection.
- **Ativar Mail Protection**: Ativa ou desativa o Avira Mail Protection.
- **Ativar Web Protection**: Ativa ou desativa o Avira Web Protection.
- **FireWall**:
  - **Ativar FireWall**: Ativa ou desativa o Avira FireWall
  - **Ativar Firewall do Windows**: Ativa ou desativa o Firewall do Windows (esta funcionalidade está disponível a partir do Windows 8).

  - **Bloquear todo o tráfego**: ativado. Bloqueia todas as transferências de dados, exceto as transferência para o sistema do computador host (host local/IP 127.0.0.1).
- **Iniciar Avira Professional Security**: Abre o Centro de Controle.
- **Configurar Avira Professional Security**: 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 já foram definidas regras para comutação automática para uma configuração.
- **Ajuda**: abre a ajuda online.
- **Sobre o Avira Professional Security:** Abre uma caixa de diálogo com informações sobre seu produto Avira: Informações do produto, Informações da versão, Informações de licença.
- **Avira na Internet**: Abre o portal da Web da Avira na Internet. Para isso, é necessário ter uma conexão ativa com a Internet.

4.2 Como...?

Os capítulos "Como...?" Oferecem instruções breves sobre a licença e a ativação do produto e informações sobre as funções mais importantes do seu produto Avira. Os artigos resumidos selecionados servem como uma visão geral sobre a funcionalidade do produto Avira. Elas não substituem as informações detalhadas de cada seção deste centro de ajuda.

4.2.1 Ativar Licença

Para ativar a licença de seu produto Avira:

Ative a licença do seu Avira com o arquivo de licença *.KEY* . Você Você pode obter o arquivo de licença por e-mail 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 seu produto Avira.
- Durante a instalação, insira o local de salvamento do arquivo de licença.

Se você já possuir o produto Avira instalado:

- 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 do seu produto Avira, selecione o item de menu **Ajuda > Carregar arquivo de licença…**

Observação
No Windows Vista, a caixa de diálogo Controle da Conta do Usuário é exibida. Faça logon 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 atualizações automáticas

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

- No Centro de Controle, selecione a seção *ADMINISTRAÇÃO* **> Agendamento**.
- 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**
- **Daily**
- **Semanalmente**
- **Intervalo**
- **Única**
- **Logon**

Observação
Recomendamos atualizações automáticas periódicas. 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):

- **Repita o trabalho se o tempo expirou**
  São executados trabalhos passados que não puderam ser realizados no momento apropriado, por exemplo, porque o computador estava desligado.
- **Inicie o trabalho enquanto conectado à Internet (discado)**
  Além da frequência definida, o trabalho é realizado 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**: Nenhuma janela de backup
- **Minimizar**: Somente barra de progresso
- **Maximizar**: Janela de trabalho inteira

- Clique em **Concluir**.
  ↳ Seu trabalho recém-criado aparece na página inicial da seção *ADMINISTRAÇÃO* **> Agendamento** com o status ativado (marca de seleção).
- Quando apropriado, desative os trabalhos que não devem ser realizados.

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 varredura são sempre atualizados.

Para iniciar uma atualização de seu produto Avira manualmente:

- Com o botão direito do mouse, clique no ícone de bandeja do Avira na barra de tarefas.
  - ↪ Um menu contextual é exibido.
- Selecione **Iniciar atualização**.
  - ↪ A caixa de diálogo **Atualizador** é exibida.

- OU -

- No Centro de Controle, selecione **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 atualizações automáticas periódicas. O intervalo de atualização recomendado é: 60 minutos.

Observação
Você também pode realizar uma atualização manual diretamente por meio da Central de Segurança do Windows.

4.2.4 Usando 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 de verificação:

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:

   Este ícone inicia a verificação através de um perfil.

- No Windows Vista:

  No Microsoft Windows Vista, o Centro de Controle possui 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 de verificação. Somente os diretórios e arquivos aos quais o sistema operacional 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 de verificação selecionado são verificados.

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

1. Vá para o Centro de Controle e selecione a seção *PROTEÇÃO DO PC* **> System Scanner**.
   ↳ Os perfis de verificação predefinidos são exibidos.
2. Selecione um dos perfis de verificação predefinidos.

   -OU-

   Adapte o perfil de verificação **Seleção Manual**.

   -OU-

   Criar um novo perfil de verificação
3. Clique no ícone (Windows XP:  ou Windows Vista:  :).
4. A janela **Luke Filewalk**er é exibida e uma verificação por demanda é iniciada.
   ↳ Quando a verificação termina, os resultados são exibidos.

Se desejar adaptar um perfil de verificação:

1. 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 de diretório é exibido.
   - Clique no ícone **-**: O próximo nível de diretório é ocultado.
2. 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 varredura preta)
- Subdiretórios de apenas um diretório (marca de varredura cinza; os subdiretórios têm marcas de varredura pretas)
- Nenhum diretório (sem marca de varredura)

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 varredura preta)
- Subdiretórios de apenas um diretório (marca de varredura cinza; os subdiretórios têm marcas de varredura pretas)
- Nenhum diretório (sem marca de varredura)

4.2.5 Verificar presença de vírus e malware usando arrastar e soltar

Para verificar a presença de vírus e malware sistematicamente usando arrastar e soltar:

- ✓ O Centro de Controle de seu produto Avira foi aberto.
- Realce o arquivo ou diretório que deseja verificar.
- Use o botão esquerdo do mouse para arrastar o arquivo ou diretório realçado no **Centro de Controle**.
  - ↪ A janela **Luke Filewalker** aparece 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 contextual

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

- 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 contextual do Windows Explorer é exibido.
- Selecione **Verificar arquivos selecionados com o Avira** no menu contextual.
  - ↪ A janela **Luke Filewalker** aparece 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
Após a instalação, o trabalho de verificação **Verificação completa do sistema** é criado no Agendamento: Uma verificação completa do sistema é realizada automaticamente 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* **> Agendamento**.
- 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**
- **Logon**

- 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

São realizados os trabalhos antigos que não puderam ser realizados no tempo necessário, por exemplo porque 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**: Nenhuma janela de backup
- **Minimizado**: somente barra de progresso
- **Maximizado**: Janela de trabalho inteira
- Selecione a opção **Desligar o computador se o trabalho for concluído** se desejar que o computador seja desligado automaticamente quando a verificação for concluída. Essa opção está disponível apenas se o modo de exibição está definido como minimizado ou maximizado.
- Clique em **Concluir**.

  ↳ Seu trabalho recém-criado aparece na página inicial da seção *ADMINISTRAÇÃO* **> Agendamento** com o status ativado (marca de seleção).
- Quando apropriado, desative os trabalhos que não devem ser realizados.

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 para 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 para o Centro de Controle e selecione a seção *PROTEÇÃO DO PC* **> System Scanner**.

  ↳ Os perfis de verificação predefinidos são exibidos.
- Selecione 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 Filewalkerr** é exibida e uma verificação por demanda 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 seu produto Avira reage a um vírus ou programa indesejado detectado na **Configuração** na seção **Resolução de detecções**.

Nenhuma opção de ação configurável está disponível para o componente ProActiv do Real-Time Protection: A notificação de uma deteção é sempre fornecida na janela **Real-Time Protection: Comportamento do Aplicativo Suspeito** .

Opções de ação para o Scanner:

Interativo

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

No caso de uma **varredura do Scanner**, você receberá um alerta com uma lista dos arquivos afetados quando a varredura 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 infectados ou cancelar o Scanner.

Automático

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

Opções de ação para o Real-Time 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 Scanner usando o botão **Detalhes** para o gerenciamento futuro do vírus. O Scanner abre a janela contendo a notificação da detecção, que fornece a você várias opções para o gerenciamento do arquivo afetado por meio do menu contextual (consulte Detecção > Scanner):

Automático

No modo de ação automática, quando um vírus ou programa indesejado é detectado, a ação selecionada nessa área é executada automaticamente. Se você ativar a opção **Exibir alertas de detecção**, receberá uma notificação de desktop sempre que um vírus for detectado.

Opções de ação para Mail 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 a configuração padrão.

Automático

No modo de ação automática, quando um vírus ou programa indesejado é detectado, a ação selecionada nessa área é executada automaticamente. Se você ativar a opção **Mostrar barra de progresso**, receberá um alerta quando um vírus for detectado. 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
Quais ações estão disponíveis para seleção depende do sistema operacional, dos componentes de proteção (Avira Real-Time Protection, Avira Scanner, Avira Mail Protection, Avira Web Protection) que relatam a deteção e do tipo de malware detectado.

Ações do Scanner e do Real-Time 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 aos arquivos (por exemplo, com clique duplo) não será 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 de setor de inicialização for detectado, ele poderá ser excluído por meio da exclusão do setor de inicialização. Um novo setor de inicialização é gravado.

Ignorar

Nenhuma ação adicional é executada. 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
Isto poderá resultar na perda de dados e em danos ao sistema operacional! Selecione a opção **Ignorar** somente em casos excepcionais.Selecione a opção Ignorar somente em casos excepcionais.

Sempre Ignorar

Opção de ação para detecções do Real-Time Protection: nenhuma outra ação é executada pelo Real-Time Protection. O acesso ao arquivo é permitido. Todo acesso posterior a esse arquivo é permitido e nenhuma outra notificação será fornecida até o computador ser reiniciado ou o arquivo de definição de vírus ser atualizado.

Copiar para quarentena

A opção de ação para a detecção de rootkits: a detecção é copiada na quarentena.

Reparar setor de inicialização | Baixar ferramenta de reparo

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

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

Ações do Real-Time Protection para detecções feitas pelo componente ProActiv (notificação de ações suspeitas de um aplicativo):

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*. Isto significa que o aplicativo é excluído do monitoramento pelo componente ProActiv somente se o conteúdo permanecer inalterado (consulte Filtro do Aplicativo: Aplicativos Permitidos).

Bloquear programa uma vez

O aplicativo é bloqueado, isto é, ele é encerrado. As ações do aplicativo continuam a ser 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 Filtro do Aplicativo: Aplicativos a serem bloqueados).

Ignorar

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

Ações de Mail Protection: E-mails Recebidos

Mover para quarentena

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

Excluir e-mail

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

Excluir anexo

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

Mover anexo para a quarentena

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

Ignorar

O e-mail afetado é entregue.

> **Aviso**
> Isto pode permitir que vírus e programas indesejados acessem seu sistema do computador. Selecione a opção **Ignorar** somente em casos excepcionais. Desative a visualização em seu cliente de e-mail, nunca abra nenhum anexo clicando duas vezes nele!

Ações de Mail Protection: E-mails Enviados

Mover e-mail para quarentena (não enviar)

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

Bloquear envio de e-mails (não enviar)

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

Ignorar

O e-mail afetado é enviado.

> **Aviso**
> Vírus e programas indesejados podem penetrar no sistema do computador do destinatário do e-mail desta maneira.

Ações de 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 valor informativo ou, se necessário, enviado para o Centro de pesquisa de malware da Avira.

Ignorar

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

Aviso
Isto pode permitir que vírus e programas indesejados acessem seu sistema do computador. Selecione a opção **Ignorar** somente em casos excepcionais.

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

Observação
Você também pode enviar-nos arquivos relatados pela heurística para análise. Por exemplo, pode carregar esses arquivos para o nosso website:
http://www.avira.com/pt-br/sample-upload
Pode identificar arquivos relatados pela heurística a partir da designação *HEUR/* ou *HEURISTIC/* que aparece como prefixo do nome de 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 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 usando as configurações de 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  .
- Você precisa confirmar sua opção com **Sim**.

Se você quiser carregar o arquivo para um servidor da web do Avira Malware Research Center para análise:

- Realce o arquivo que deseja carregar.
- 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 de resposta: **HTML**, **Texto**, **HTML e Texto**.
- Clique em **OK.**
  - ↳ O arquivo é carregado em um servidor da web do Avira Malware Research Center em formato compactado.

Observação
Nos casos a seguir, a análise pelo Avira Malware Research Center é recomendada:
Ocorrências de Heurística (Arquivo Suspeito): Durante uma verificação, um arquivo foi classificado como suspeito por seu produto Avira e movido para a quarentena: A análise do arquivo pelo Avira Malware Research Center foi recomendada na caixa de diálogo de detecção do vírus ou no arquivo de relatório gerado pela verificação.
Arquivo Suspeito: Você considera que um arquivo é suspeito e, portanto, move este arquivo para quarentena, mas uma verificação do arquivo em busca de vírus e malwares é negativa.
Suspeita de Falso-positivo: Você assume que uma detecção de vírus é um falso-positivo: Seu produto Avira registra uma detecção em um arquivo, que é muito pouco provável de ter sido infectado por malware.

Observação
O tamanho dos arquivos carregados é limitado a 20 MB descompactados ou 8 MB compactados.

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

- Realce o objeto em quarentena e clique em  .
  - ↳ O diálogo *Procurar Pasta* é aberto, a partir do qual você pode selecionar um diretório.
- Selecione um diretório em que deseja salvar uma cópia do objeto em quarenta 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 desejar exportar as propriedades de um objeto em quarentena para um arquivo de texto:

- Realce o objeto em quarentena e clique em  .
  - ↳ O arquivo de texto *Quarentena - Bloco de Notas* é aberto contendo os dados do objeto em quarentena selecionado.
- Salve o arquivo de texto.

Você também pode restaurar os arquivos em quarentena (consulte Capítulo: Quarentena: Restaurar os 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:
  -  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 possui 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
Isto poderá resultar na perda de dados e em danos ao sistema operacional do computador! Use a função **Restaurar objeto selecionado** somente 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

Emails e anexos de email podem ser restaurados usando a opção  somente se a extensão do arquivo for **.eml*.

Para restaurar um arquivo ao seu local original:

▸ Realce o arquivo e clique no ícone (Windows XP:  , Windows Vista ).

Essa opção não está disponível para emails.

Observação

Emails e anexos de email podem ser restaurados usando a opção  somente se a extensão do arquivo for **.eml*.

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

▸ Clique em **Sim**.

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

Para restaurar um arquivo em um diretório especificado:

- 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 para o 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 com **Abrir**.
  - ↪ O arquivo é movido para a quarentena.

Você pode verificar arquivos na quarentena com o Avira System Scanner (consulte o Capítulo: Quarentena: Manipulando arquivos em quarentena (*.qua)).

4.2.13 Corrigir ou excluir tipo de arquivo em um perfil de varredura

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

- ✓ No Centro de Controle, vá para a seção *PROTEÇÃO DO PC* **> System Scanner**.
- Com o botão direito do mouse, clique no perfil de verificação que deseja editar.
  - ↪ Um menu contextual é exibido.
- Selecione **Filtro de arquivo**.
- Expanda o menu contextual ainda mais clicando no pequeno triângulo à direita do menu contextual.
  - ↪ As entradas **Padrão**, **Verificar todos os arquivos** e **Definido pelo usuário** são exibidas.
- Selecione **Definido pelo usuário**.
  - ↪ A caixa de diálogo **Extensões do 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. 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 a partir de sua área de trabalho através de um atalho na área de trabalho para um perfil de verificação sem acessar o Centro de Controle de seu produto Avira.

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

✓ No Centro de Controle, vá para a seção *PROTEÇÃO DO 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

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

- FireWall
- Serviço de ajuda
- Mail Protection
- Real-Time Protection
- Agendamento
- Scanner
- Atualizador
- Web Protection
- ProActiv

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 estes eventos.

4.2.16 Excluir endereços de email da verificação

Para definir quais endereços de email (emissores) são excluídos da verificação do Mail Protection (listagem branca):

- Vá para 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 do 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 do emissor do email é incluído na lista de exclusões e não será mais verificado em busca de vírus, malwares .

Aviso
Exclua endereços de email da verificação do Mail Protection somente se os emissores forem completamente confiáveis.

Observação
Na Configuração, em Mail Protection > Geral > Exceções, você pode incluir outros endereços de email na lista de exclusões ou remover endereços de email da lista de exclusõe.

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

Flooding e varredura de porta são detectadas.

Meio

Os pacotes TCP e UDP suspeitos são descartados.

Flooding e varredura de porta são evitadas.

(Configurar como nível padrão.)

Alto

O computador não está visível na rede.

Novas conexões externas não são permitidas.

Flooding e varredura de porta são evitadas.

Personalizado

Regras definidas pelo usuário: Se este nível de segurança for selecionado, o programa reconhecerá automaticamente que as regras do adaptador foram modificadas.

Bloquear tudo

Todas as conexões de rede existente serão fechadas.

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

Para definir o nível de segurança para o FireWall:

- Vá para 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. Detecção

5.1 Visão Geral

Quando um vírus é detectado, o Avira pode executar automaticamente algumas ações ou responder de forma interativo. No modo de ação interativa, uma caixa de diálogo é aberta quando um vírus é detectado; nessa caixa é possível controlar ou iniciar as etapas subsequentes de manipulação do vírus (excluir, ignorar etc). No modo automático, existe uma opção para exibir um alerta quando um vírus é detectado. A ação que foi executada automaticamente é exibida na mensagem.

Este capítulo contém informações abrangentes sobre as mensagens de detecção, organizadas de acordo com o módulo.

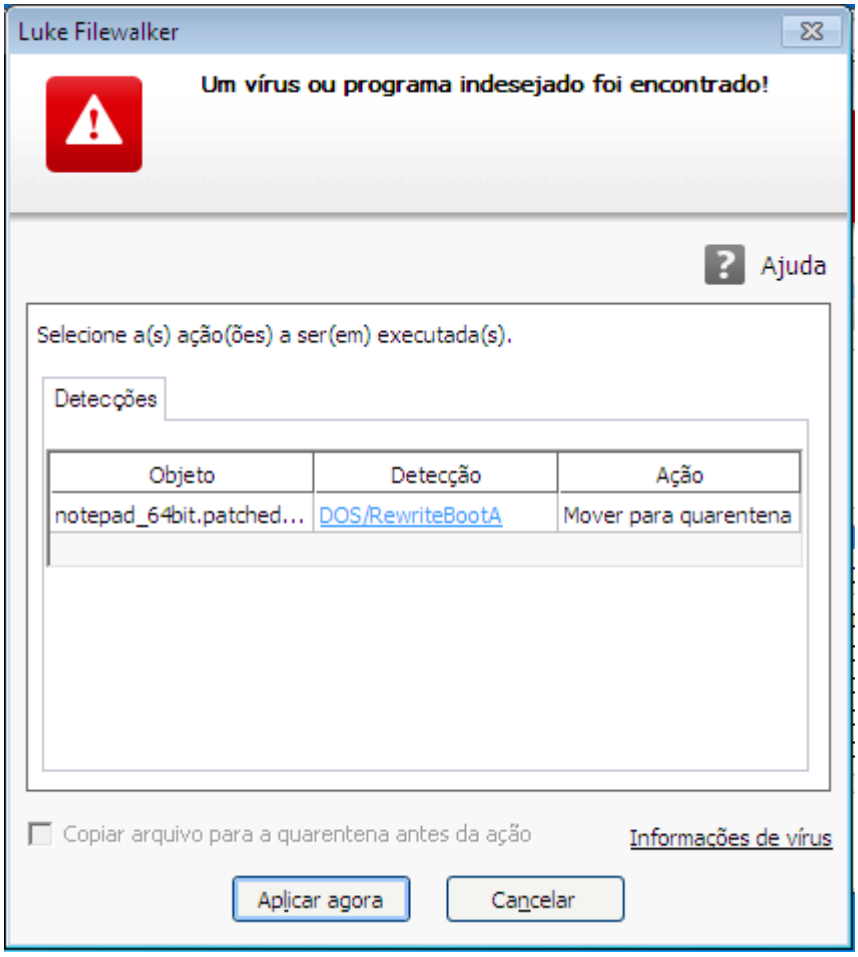
- consulte o Capítulo Scanner: Modo de ação interativa
- consulte o Capítulo Scanner: Modo de ação automática
- consulte o Capítulo Scanner: Enviando arquivos para Protection Cloud
- consulte o Capítulo Real-Time Protection
- consulte o Capítulo Real-Time Protection: Comportamento suspeito
- consulte o Capítulo Mail Protection: E-mails recebidos
- consulte o Capítulo Mail Protection: E-mails enviados
- consulte o Capítulo E-mail enviado: remetente
- consulte o Capítulo consulte o Capítulo E-mail enviado: remetente
- consulte o Capítulo Web Protection

5.2 Modo de ação interativa

Se você tiver selecionado o modo *Interativo* como o modo de ação, quando um vírus é detectado, receberá um alerta contendo uma lista de arquivos afetados, quando a varredura for concluída (consulte a seção de configuração Scanner > Varredura > Ação para detecção).
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 infectados ou cancelar o Scanner.

Nota
Se relatório for ativado, o Scanner insere cada detecção no Arquivo de relatório.

5.2.1 Alerta



5.2.2 Detecção, Erros, Avisos

Informações detalhadas, opções de ação para vírus detectados e mensagens serão exibidas nas guias **Detecção**, **Erros** e **Avisos**:

- **Detecção:**
  - *Objeto:* Nome de arquivo do arquivo afetado
  - *Detecção:* nome do vírus ou programa indesejado detectado
  - *Ação:* ação selecionada com a qual o arquivo afetado deve ser manipulado
    Você pode escolher outras ações para lidar com o malware no menu contextual associado à ação exibida.
- **Erro:** mensagens sobre os erros que ocorreram durante a varredura
- **Alertas:** alertas relacionados aos vírus que foram detectados

> **Nota**
> As seguintes informações são exibidas na dica de ferramenta do objeto: nome

do arquivo ou afetado e caminho completo, nome do vírus e ação que deve ser executada com o botão **Aplicar agora**.

Nota
A ação padrão do Scanner é exibida como a ação a ser executada. A ação padrão do Scanner para manipular os arquivos afetados pode ser definida na seção de configuração Scanner > Varredura > Ação para detecção na área *Ações Permitidas*.

5.2.3 Ações do menu contextual

Nota
Se a detecção for um acesso heurístico (HEUR/), uma ferramenta de compactação de tempo de execução incomum (PCK/) ou um arquivo com uma extensão de arquivo oculta (HEUR-DBLEXT/), no modo interativo somente as opções Mover para quarentena e Ignorar estarão disponíveis. No modo automático a detecção é movida automaticamente para Quarentena.
. Essa restrição impede que os arquivos detectados, que podem ser um alarme falso, sejam removidos (excluídos) diretamente do computador. O arquivo pode ser recuperado a qualquer momento com a ajuda do Gerenciador de Quarentena.
Dependendo da configuração, várias opções talvez não estejam disponíveis.

Reparar

Se essa opção for ativada, o Scanner reparará o arquivo afetado.

Nota
A opção **Reparar** somente poderá ser ativada se for possível reparar o arquivo detectado.

Quarentena

Se essa opção for ativada, o 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 podem estar disponíveis no Gerenciador de quarentena.

Excluir

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

Substituir e excluir

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

Renomear

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

Ignorar

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

Sempre Ignorar

Opção de ação para detecções do Real-Time Protection: nenhuma outra ação é executada pelo Real-Time Protection. O acesso ao arquivo é permitido. Todo acesso posterior a esse arquivo é permitido e nenhuma outra notificação será fornecida até o computador ser reiniciado ou o arquivo de definição de vírus ser atualizado.

Aviso
Se você ignorar as opções ou selecionar **Sempre ignorar**, os arquivos afetados permanecem ativos no computador! Isso pode causar danos graves à estação de trabalho!

5.2.4 Recursos especiais quando setores de inicialização infectados, rootkits e malware ativo são detectados

As opções de ação estão disponíveis para reparar setores de inicialização infectados quando forem detectados:

Reparar setor de inicialização de 722 KB | 1,44 MB | 2,88 MB | 360 KB | 1,2 MB

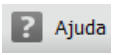
Essas opções estão disponíveis para unidades de disquete.

Download do CD de resgate

Essa opção o levará ao site da Avira, onde você pode baixar uma ferramenta especial para detectar e remover vírus do setor de inicialização.

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

5.2.5 Botões e links

Botão / link	Descrição
Aplicar agora	As ações selecionadas são executadas para manipular todos os arquivos afetados.
Cancelar	O Scanner é fechado sem nenhuma outra ação. Os arquivos afetados não são alterados no sistema do seu computador.
	Esta página da ajuda on-line é aberta por meio deste botão ou link.

Aviso
Execute a ação *Cancelar* somente em casos excepcionais. Os arquivos afetados permanecem ativos na estação de trabalhos após o cancelamento! Isso pode causar danos graves à estação de trabalho!

5.2.6 Recursos especiais quando malware for detectado enquanto Web Protection estiver inativo

Se você desativou o Web Protection, o Scanner relata malware ativo que detectou por meio de um slide-up durante a varredura do sistema. Antes de reparar o sistema é possível criar um ponto de restauração.

✓ Primeiro é necessário ativar o System Restore no sistema Windows.

- Clique em **Detalhes** no slide up.
  - ↪ A janela *O sistema está sendo verificado* é exibida.
- Ative **Criar ponto de restauração do sistema antes do reparo**.
- Clique em **Aplicar**.
  - ↪ Um ponto de restauração do sistema foi criado. Agora você pode executar uma restauração do sistema usando o Painel de controle do Windows se necessário.

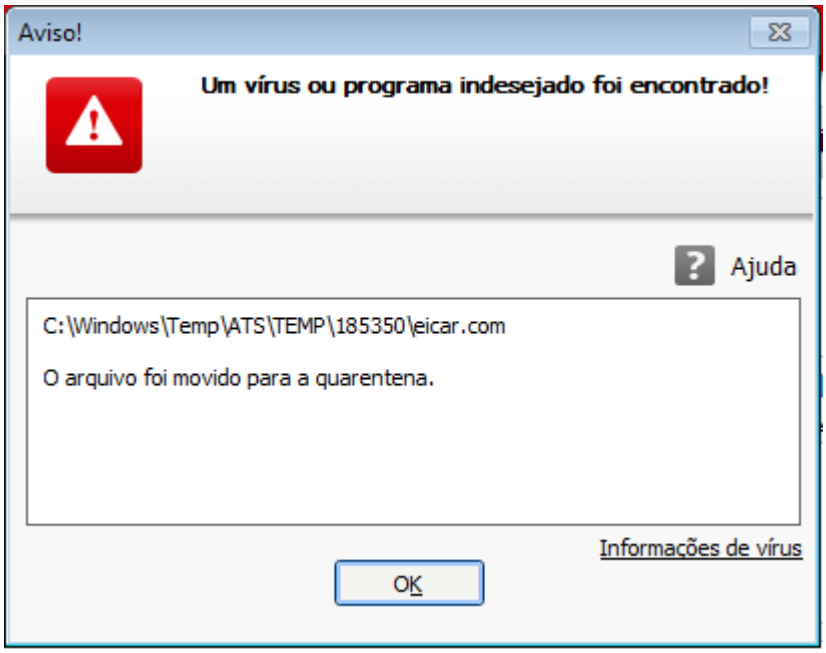
5.3 Modo de ação automática

Se você selecionou o modo *Automático* e a opção *Exibir alerta* como o modo de ação quando um vírus for detectado, receberá um alerta toda vez que o System Scanner detectar um vírus no arquivo (consulte a seção de configuração System Scanner > Verificar > Ação na detecção). Não há nenhuma opção de seleção para manipular o vírus detectado no modo automático com alerta. A ação que foi selecionada na configuração

para lidar com um vírus é executada. A ação que foi executada automaticamente é exibida na mensagem.

> **Nota**
> Se relatório for ativado, o System Scanner insere cada detecção no Arquivo de relatório.

5.3.1 Alerta



5.3.2 Botões e links

Botão / link	Descrição
Ajuda	Esta página da ajuda on-line é aberta por meio deste botão ou link.

5.4 Enviando arquivos para Protection Cloud

Uma lista de locais que são destino frequente do malware é gerada quando o trabalho **Verificação rápida do sistema** é executado. A lista inclui processos em execução, programas que executam na inicialização e serviços. Arquivos de programa desconhecidos são carregados para o Avira Protection Cloud para análise.

Se você ativar a opção **Confirmar manualmente quando enviar arquivos suspeitos para Avira** durante a instalação personalizada ou mais tarde na configuração de **Advanced Protection**, é exibida uma lista dos arquivos suspeitos que devem ser

enviados ao Protection Cloud e você pode escolher quais arquivos deseja enviar. Por padrão, todos os arquivos suspeitos são marcados para ser enviados ao Avira Protection Cloud para mais análise.

> **Nota**
> Se você ativou o modo de relatório **Estendido**, o System Scanner registra cada detecção no arquivo de relatório e adiciona o sufixo *(Cloud)* às detecções feita pelo Protection Cloud.

5.4.1 Informações exibidas

A lista de arquivos suspeitos a ser enviados ao Avira Protection Cloud.

- *Enviar:* você pode selecionar quais arquivos serão enviados ao Avira Protection Cloud.
- *Arquivo:* o nome do arquivo suspeito.
- *Caminho:* o caminho do arquivo suspeito.

Enviar arquivos sempre automaticamente

Se essa opção for ativada, os arquivos suspeitos serão enviados ao Protection Cloud para análise diretamente após cada **Verificação rápida do sistema** sem pedir confirmação manual.

5.4.2 Botões e links

Botão / link	Descrição
Enviar	Os arquivos selecionados são enviados ao Avira Protection Cloud.
Cancelar	O System Scanner é fechado sem outra ação. Os arquivos suspeitos são deixados inalterados no sistema do computador.
Ajuda	Esta página da ajuda on-line é aberta.
Sobre o Protection Cloud	A página da web do Avira Protection Cloud é aberta.

Tópicos relacionados:

- Configuração do Advanced Protection
- Instalação personalizada
- Configuração do relatório

- Visualização dos relatórios

5.5 Real-Time Protection

Se vírus forem detectados pelo Real-Time Protection, o acesso ao arquivo será negado e uma notificação de desktop será exibida , se você selecionou o modo *interativo* como o modo de ação para detecção de vírus ou o modo *automático* com a opção **Exibir alerta** (consulte a seção Configuração Real-Time Protection > Verificar > Ação para detecção).

Notificação

As informações a seguir são exibidas na notificação:

- Data e hora da detecção
- Caminho e nome do arquivo afetado
- Nome do malware

> **Nota**
> Quando o modo de partida padrão do Real-Time Protection (Partida normal) foi escolhido e o processo de logon na partida for executado com rapidez, os programas configurados para iniciar automaticamente na partida poderão não ser verificados porque poderão estar ativos e em execução antes de o Real-Time Protection ter iniciado completamente.

No modo interativo existem as seguintes opções:

Remover

O arquivo afetado é transferido para o componente Scanner e é excluído pelo Scanner. Nenhuma mensagem adicional é exibida.

Detalhes

O arquivo afetado é transferido para o componente Scanner. O Scanner abre uma janela que contém a notificação da detecção e diversas opções de gerenciamento do arquivo afetado.

> **Nota**
> Veja as informações sobre gerenciamento de vírus em Detecção > Scanner.

> **Nota**
> Para gerenciamento de vírus, a ação selecionada como padrão na

Configuração em Real-Time Protection > Verificar > Resolução de detecções é exibida. Outras ações podem ser selecionadas via menu contextual.

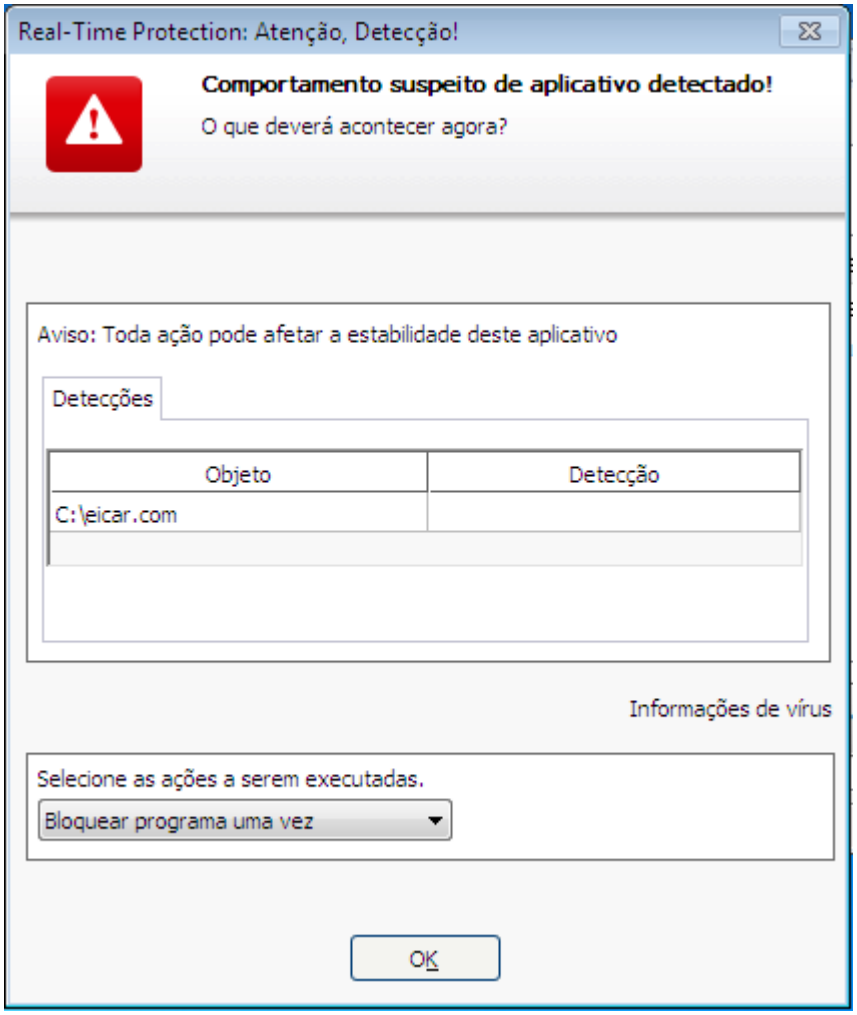
Fechar

A mensagem é fechada. O gerenciamento de vírus é finalizado.

5.6 Comportamento suspeito

Se você ativar o componente ProActiv do Real-Time Protection, as ações do aplicativo serão monitoradas e verificadas quanto a comportamento suspeito típico de malware. Você receberá um alerta se comportamento suspeito for detectado em um aplicativo. Você tem várias opções para lidar com a detecção.

5.6.1 Alerta do Real-Time Protection: Comportamento suspeito de aplicativo detectado



5.6.2 Nome e caminho do programa suspeito detectado atualmente

O nome e o caminho do aplicativo que executa ações suspeitas são exibidos na janela central da mensagem.

5.6.3 Opções

Programa confiável

Se essa opção estiver ativada, o aplicativo continuará sendo 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 será excluído do monitoramento feito pelo componente ProActiv somente se o conteúdo permanecer inalterado (consulte Configuração > Geral > Proteção avançada > Filtro de aplicativos: aplicativos permitidos).

Bloquear programa uma vez

Se essa opção estiver ativada, o aplicativo será bloqueado, isto é, ele será finalizado. As ações do aplicativo continuam a ser monitoradas pelo componente ProActiv.

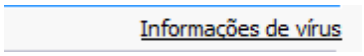
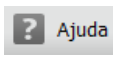
Sempre bloquear este programa

Se essa opção estiver ativada, o aplicativo será bloqueado, isto é, ele será finalizado. O programa é adicionado à lista de aplicativos bloqueados e não pode mais ser executado (consulte Configuração > Geral > Proteção avançada > Filtro de aplicativos: aplicativos a ser bloqueados).

Ignorar

Se essa opção estiver ativada, o aplicativo continuará sendo executado. As ações do aplicativo continuam a ser monitoradas pelo componente ProActiv.

5.6.4 Botões e links

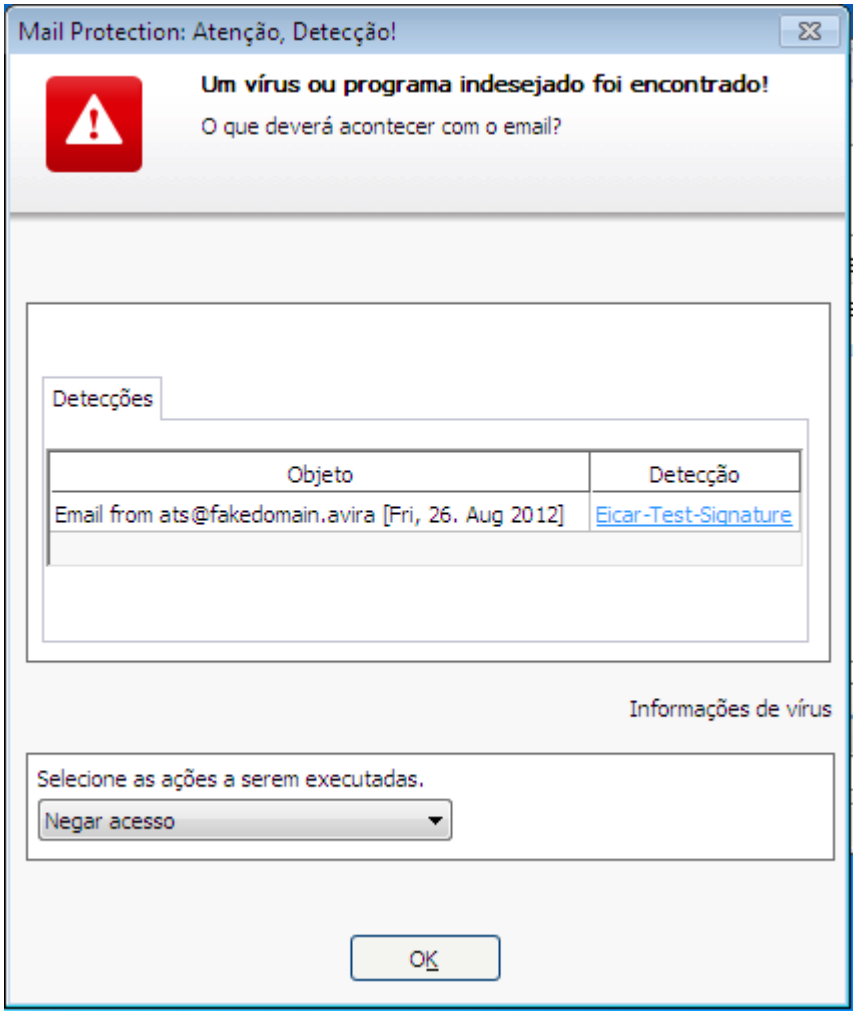
Botão / link	Descrição
	Com esse link - e com uma conexão ativa com a Internet - é possível acessar uma página da Internet com mais informações sobre esse vírus ou programa indesejado.
	Esta página da ajuda on-line é aberta por meio deste botão ou link.

5.7 Emails recebidos

Se o Mail Protection detectar um vírus, você receberá uma alerta se tiver selecionado o modo *interativo* como o modo de ação quando um vírus for detectado (consulte a seção de configuração Mail Protection > Verificar > Ação para detecção). No modo interativo você pode escolher o que deve ser feito com o email ou anexo na caixa de diálogo.

você receberá o alerta mostrado a seguir se um vírus for detectado em um email recebido.

5.7.1 Alerta



5.7.2 Detecções, Erros, Avisos

Mensagens e informações mais detalhadas sobre os emails em questão serão exibidas nas guias **Detecções**, **Erros** e **Avisos**:

- **Detecções:** Objeto: o email em questão que mostra o nome do remetente e o horário do email foi enviado

  Detecção: nome do vírus ou programa indesejado detectado

- **Erro:** mensagens sobre os erros que ocorreram durante a verificação do Mail Protection
- **Alertas:** alertas relacionados aos objetos afetados

5.7.3 Opções

> **Nota**
> Se a detecção for um acesso heurístico (HEUR/), uma ferramenta de compactação de tempo de execução incomum (PCK/) ou um arquivo com uma extensão de arquivo oculta (HEUR-DBLEXT/), no modo interativo somente as opções Mover para quarentena e Ignorar estarão disponíveis. No modo automático a detecção é movida automaticamente para Quarentena.
> Essa restrição impede que os arquivos detectados, que podem ser um alarme falso, sejam removidos (excluídos) diretamente do computador. O arquivo pode ser recuperado a qualquer momento com a ajuda do Gerenciador de quarentena.

Mover para quarentena

Se essa opção for ativada, o email que inclui todos os anexos é movido para quarentena. Ele pode ser enviado depois 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 é 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 é substituído por um texto padrão. Se o corpo do email for afetado, ele é excluído e também substituído por um texto padrão. O email propriamente dito é entregue.

Mover anexo para quarentena

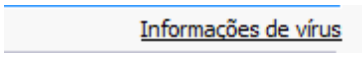
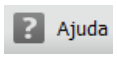
Se essa opção for ativada, o anexo afetado é movido para quarentena e excluído (substituído por um texto padrão). O corpo do email é entregue. O anexo afetado pode ser entregue posteriormente pelo Gerenciador de quarentena.

Ignorar

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

Aviso
Isso pode permitir o acesso de vírus e programas indesejados ao sistema do 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!

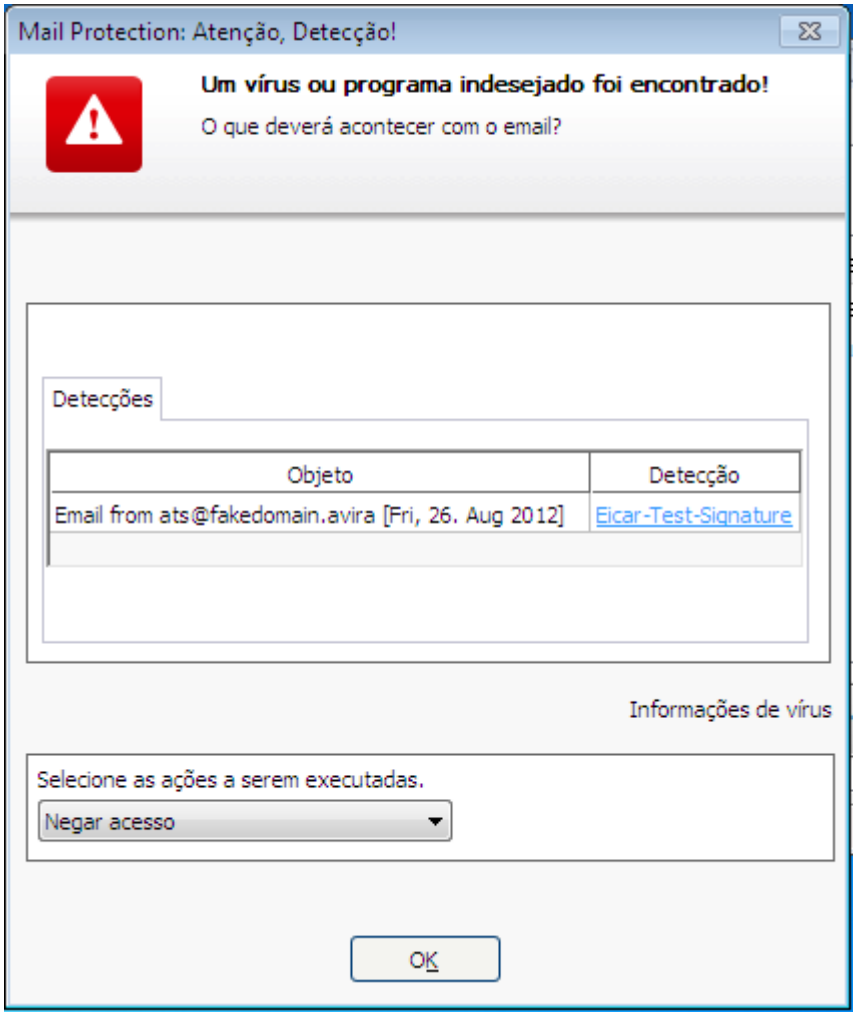
5.7.4 Botões e links

Botão / link	Descrição
	Com esse link - e com uma conexão ativa com a Internet - é possível acessar uma página da Internet com mais informações sobre esse vírus ou programa indesejado.
	Esta página da ajuda on-line é aberta por meio deste botão ou link.

5.8 Emails enviados

Se o Mail Protection detectar um vírus, você receberá uma alerta se tiver selecionado o modo *interativo* como o modo de ação quando um vírus for detectado (consulte a seção de configuração Mail Protection > Verificar > Ação para detecção). No modo interativo você pode escolher o que deve ser feito com o email ou anexo na caixa de diálogo.

5.8.1 Alerta



5.8.2 Detecções, Erros, Avisos

Mensagens e informações mais detalhadas sobre os emails em questão serão exibidas nas guias **Detecções**, **Erros** e **Avisos**:

- **Detecções:** Objeto: o email em questão que mostra o nome do remetente e o horário do email foi enviado

  Detecção: nome do vírus ou programa indesejado detectado
- **Erro:** mensagens sobre os erros que ocorreram durante a verificação do Mail Protection
- **Alertas:** alertas relacionados aos objetos afetados

5.8.3 Opções

Mover email para quarentena (não enviar)

Se essa opção for ativada, o email junto com todos os anexos é copiado em Quarentena e não é enviado. O email permanece na caixa de saída do cliente de email. Você recebe uma mensagem de erro no programa de email. Todos os outros emails enviados da sua conta de email serão verificados em busca de malwares.

Bloquear envio de emails (não enviar)

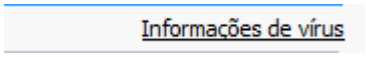
O email não é enviado e permanece na caixa de saída do cliente de email. Você recebe uma mensagem de erro no programa de email. Todos os outros emails enviados da sua conta de email serão verificados em busca de malwares.

Ignorar

Se essa opção for ativada, o email infectado é enviado apesar da detecção de um vírus ou programa indesejado.

Aviso
Vírus e programas indesejados podem penetrar no sistema do computador do destinatário do email dessa maneira.

5.8.4 Botões e links

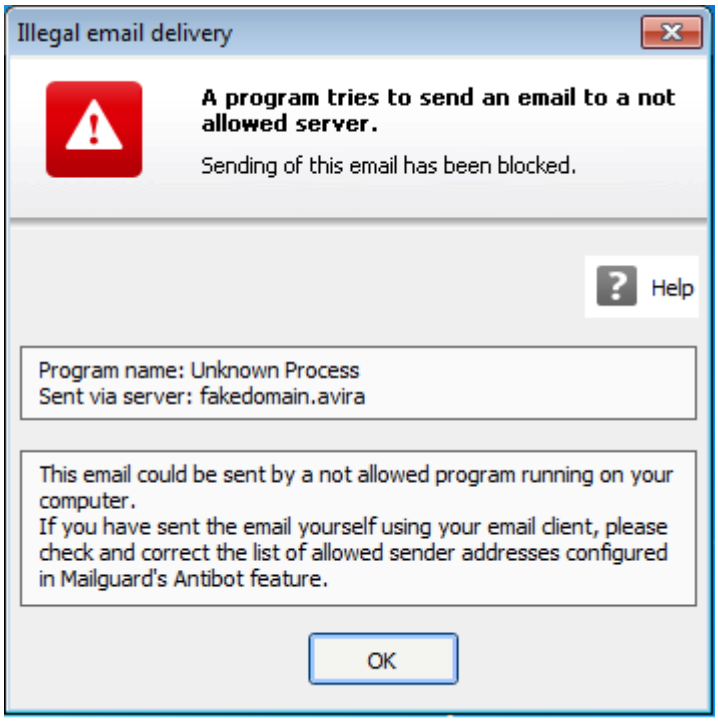
Botão / link	Descrição
	Com esse link - e com uma conexão ativa com a Internet - é possível acessar uma página da Internet com mais informações sobre esse vírus ou programa indesejado.
	Esta página da ajuda on-line é aberta por meio deste botão ou link.

5.9 Remetente

Se você estiver usando a função AntiBot do Mail Protection, os emails de remetentes não autorizados serão bloqueados pelo Mail Protection. O remetente é verificado usando a

lista de remetentes autorizados que você criou na configuração em Mail Protection > Verificar > AntiBot. O email bloqueado é exibido em uma caixa de diálogo.

5.9.1 Alerta



5.9.2 Programa usado, servidor SMTP usado e endereço do remetente do email

As seguintes informações são exibidas na janela central da mensagem:

- Nome do programa usado para enviar o email
- Nome do servidor SMTP usado para enviar o email
- Endereço do remetente do email

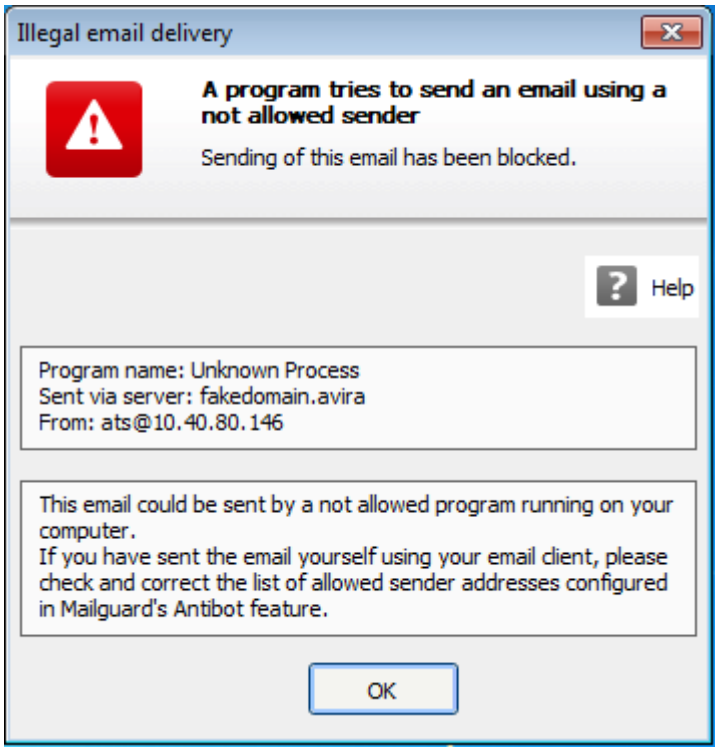
Se o email em questão foi enviado usando o programa de email, compare a lista de remetente permitidos na configuração em Mail Protection > Verificar > AntiBot com os endereços de remetentes que você usou nas contas de email no programa cliente de email. Se a lista de remetentes autorizados na configuração estiver incompleta, adicione à lista os outros endereços de remetente que você usa. Você encontrará o email bloqueado na caixa de saída do programa cliente de email. Para enviar o email bloqueado, conclua a configuração e envie o email novamente.

5.10 Servidor

Se você estiver usando a função AntiBot do Mail Protection, os emails de servidores SMTP não autorizados serão bloqueados pelo Mail Protection. A verificação do servidor SMTP que foi usado é feita usando a lista de servidores permitidos que você adicionou à

configuração em Mail Protection > Verificar > AntiBot. O email bloqueado é exibido em uma caixa de diálogo.

5.10.1 Alerta



5.10.2 Programa usado, servidor SMTP usado

As seguintes informações são exibidas na janela central da mensagem:

- Nome do programa usado para enviar o email
- Nome do servidor SMTP usado para enviar o email

Se você enviaou o email em questão usando o programa de email, compare a lista de servidores permitidos na configuração em Mail Protection > Verificar > AntiBot com os servidores SMTP que você usa para enviar emails. Você pode encontrar os servidores SMTP que são usados no programa cliente de email nas contas de email usadas. Se a lista de servidores autorizados na configuração estiver incompleta, adicione à lista os outros servidores SMTP que você usa. Você encontrará o email bloqueado na caixa de saída do programa cliente de email. Para enviar o email bloqueado, conclua a configuração e envie o email novamente.

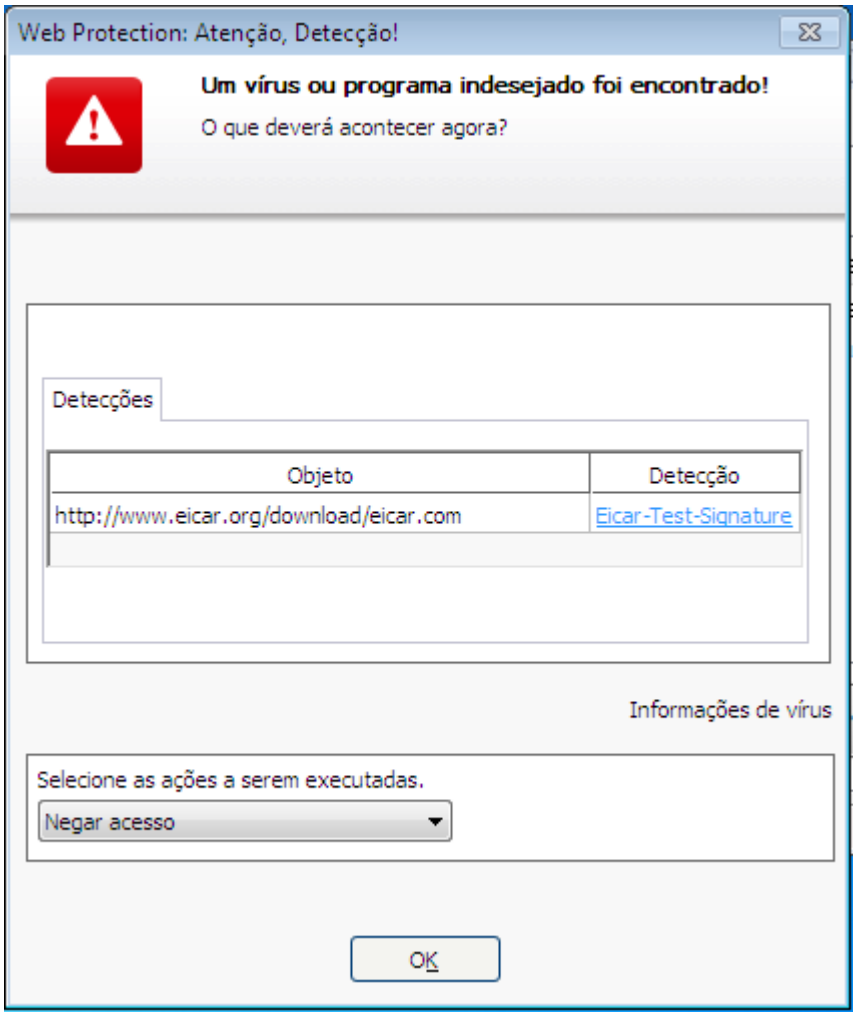
5.11 Web Protection

Se vírus forem detectados pelo Web Protection, você receberá um alerta se tiver selecionado o modo *interativo* ou modo *automático* como o modo de ação para detecção de vírus com a opção *Exibir alertas de detecção* (consulte a seção de configuração Web

Protection > Verificar > Ação na detecção). No modo interativo, você pode escolher o que deve ser feito com os dados enviados pelo servidor da Web na caixa de diálogo. Não há nenhuma opção de seleção para manipular o vírus detectado no modo automático com alerta. No alerta, você pode confirmar a ação que deve ser executada automaticamente ou cancelar o Web Protection.

Nota
A caixa de diálogo mostrada a seguir é uma mensagem sobre a detecção de um vírus no modo interativo.

Alerta



Detecção, Erros, Avisos

Mensagens e informações detalhadas relacionadas aos vírus detectados são exibidas nas guias **Detecção**, **Erros** e **Avisos**:

- **Detecção:** URL e o nome do vírus ou programa indesejado detectado

- **Erro:** mensagens sobre os erros que ocorreram durante a verificação do Web Protection scan
- **Alertas:** avisos relacionados aos vírus que foram detectados

Ações possíveis

> **Nota**
> Se a detecção for um acesso heurístico (HEUR/), uma ferramenta de compactação de tempo de execução incomum (PCK/) ou um arquivo com uma extensão de arquivo oculta (HEUR-DBLEXT/), no modo interativo somente as opções Mover para quarentena e Ignorar estarão disponíveis. No modo automático a detecção é movida automaticamente para Quarentena.
> Essa restrição impede que os arquivos detectados, que podem ser um alarme falso, sejam removidos (excluídos) diretamente do computador. O arquivo pode ser recuperado a qualquer momento com a ajuda do Gerenciador de quarentena.
> Dependendo da configuração, várias opções talvez não estejam disponíveis.

Negar acesso

O site solicitado do servidor da Web e/ou todos os dados ou arquivos transferidos não são enviados para o navegador. Uma mensagem de erro para notificar que o acesso foi negado é exibida no navegador. O Web Protection registra a detecção no arquivo de relatório se a função de registro estiver ativada.

Mover para quarentena

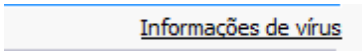
No caso um vírus ou malware ser detectado, o site solicitado do servidor da web e/ou os dados e arquivos transferidos são movidos para a quarentena. O arquivo afetado pode ser recuperado do Gerenciador de quarentena se tiver valor informativo ou, se necessário, enviado para o Centro de pesquisa de malware da Avira.

Ignorar

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

> **Aviso**
> Isso pode permitir o acesso de vírus e programas indesejados ao sistema do computador. Selecione a opção **Ignorar** somente em casos excepcionais.

Botões e links

Botão / link	Descrição
	Com esse link - e com uma conexão ativa com a Internet - é possível acessar uma página da Internet com mais informações sobre esse vírus ou programa indesejado.
	Esta página da ajuda on-line é aberta por meio deste botão ou link.

6. Scanner

6.1 Scanner

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

- **Varredura do Sistema via Menu Contextual**
  A varredura do sistema por meio do menu contextual (botão direito do mouse - entrada **Varredura de arquivos selecionados com o Avira**) é recomendada se, por exemplo, você deseja efetuar a varredura de arquivos e diretórios individuais. Uma outra vantagem é que não é necessário iniciar primeiro o Centro de Controle para uma varredura do sistema por meio do menu contextual.
- **Varredura do Sistema por meio de Arrastar e Soltar**
  Quando um arquivo ou diretório é arrastado na janela do programa do Centro de Controle, o Scanner efetua a varredura do arquivo ou diretório e todos os subdiretórios que ele contém. Esse procedimento é recomendado se você desejar efetuar a varredura de arquivos e diretórios individuais que foram salvos, por exemplo, em sua área de trabalho.
- **Varredura do Sistema Através de Perfis**
  Este procedimento é recomendado se você deseja efetuar a varredura de regularmente determinados diretórios e unidades (por exemplo, seu diretório de trabalho ou unidades nas quais você armazena novos arquivos regularmente). Você não precisa selecionar esses diretórios e unidades novamente em cada nova varredura, basta selecionar o perfil relevante.
- **Varredura do sistema via Agendamento**
  O Agendamento permite realizar verificações controladas pelo tempo.

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

- Varredura de rootkits por meio do perfil de varredura **Varredura de rootkits e malware ativo**
- Varredura de processos ativos através do perfil de varredura **Processos ativos**
- Varredura de vírus do setor de inicialização através do comando de menu **Varredura dos registros de inicialização...** no menu **Extras**

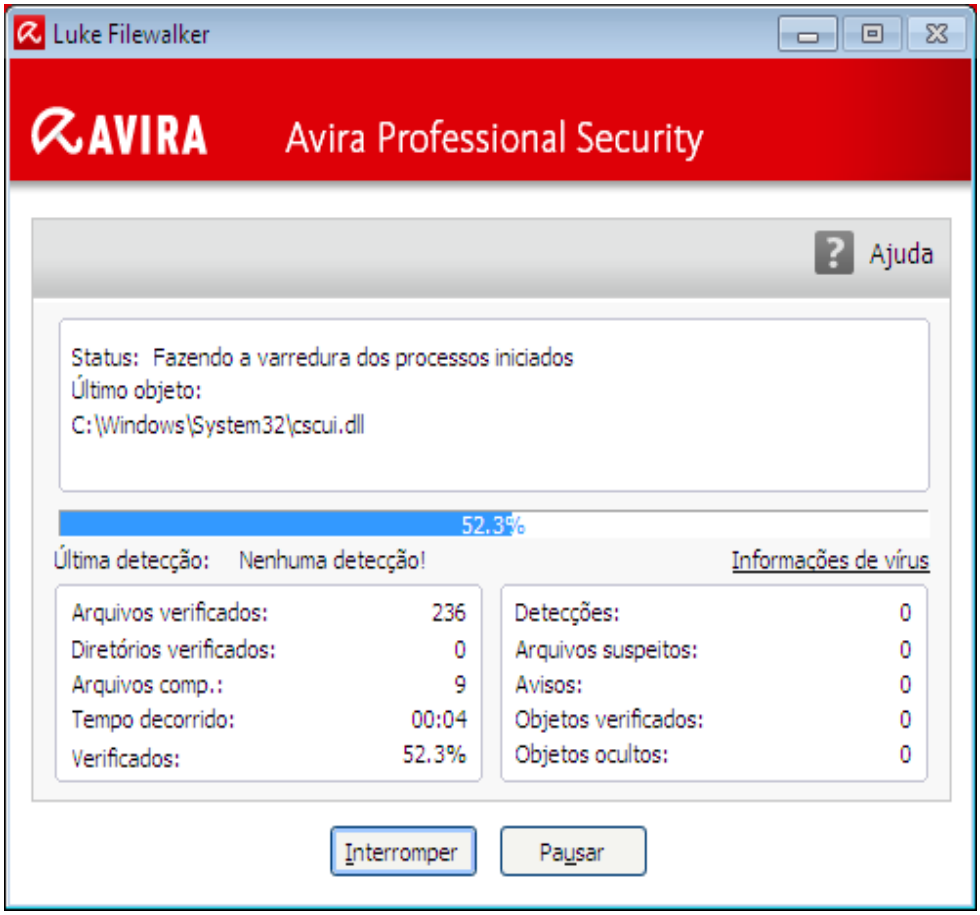
6.2 Luke Filewalker

Durante uma verificação do sistema, a janela de status **Luke Filewalker** aparece, a qual fornece informações exatas sobre o status da varredura.

Se a opção **interativa** estiver selecionada na configuração do System Scanner no grupo **Ação na Detecção**, será perguntado o que deve ser feito com um vírus ou programa indesejado detectado. Se a opção **automático** estiver selecionada, quaisquer detecções serão mostradas no Relatório do Scanner.

Quando a verificação for concluída, seu resultado (estatísticas), alertas e mensagens de erro serão exibidos em uma nova caixa de diálogo.

6.2.1 Luke Filewalker: Janela de Status da Verificação



Informações exibidas

Status: Há diferentes mensagens de status:

- *O programa será inicializado*
- *A pesquisa de objetos ocultos está em execução!*
- *Verificando os processos iniciados*
- *Verificando arquivo*
- *Inicializar arquivamento*
- *Liberar memória*
- *Arquivo está sendo descompactado*

- *Verificando setores de inicialização*
- *Verificando setores de inicialização mestres*
- *Verificando o registro*
- *O programa será encerrado!*
- *A verificação foi concluída*

Último Objeto: Nome e caminho do arquivo que está sendo verificado atualmente ou que foi verificado mais recentemente

Última Deteção: Há várias mensagens para a última detecção:

- *Nenhuma detecção!*
- Nome do vírus ou programa indesejado detectado mais recentemente

Arquivos Verificados: Número de arquivos verificados

Diretórios Verificados: Número de diretórios verificados

Arquivos Mortos Verificados: Número de arquivos mortos verificados

Tempo Utilizado: Duração da verificação do sistema

Verificado: Porcentagem da verificação já concluída

Detecções: Número de vírus e programas indesejados detectados

Arquivos Suspeitos: Número de arquivos relatados pela heurística

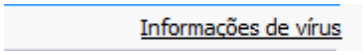
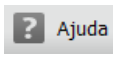
Avisos: Número de alertas sobre vírus detectados

Objetos Verificados: Número de objetos verificados durante a verificação de rootkits

Objetos Ocultos: Número total de objetos ocultos detectados

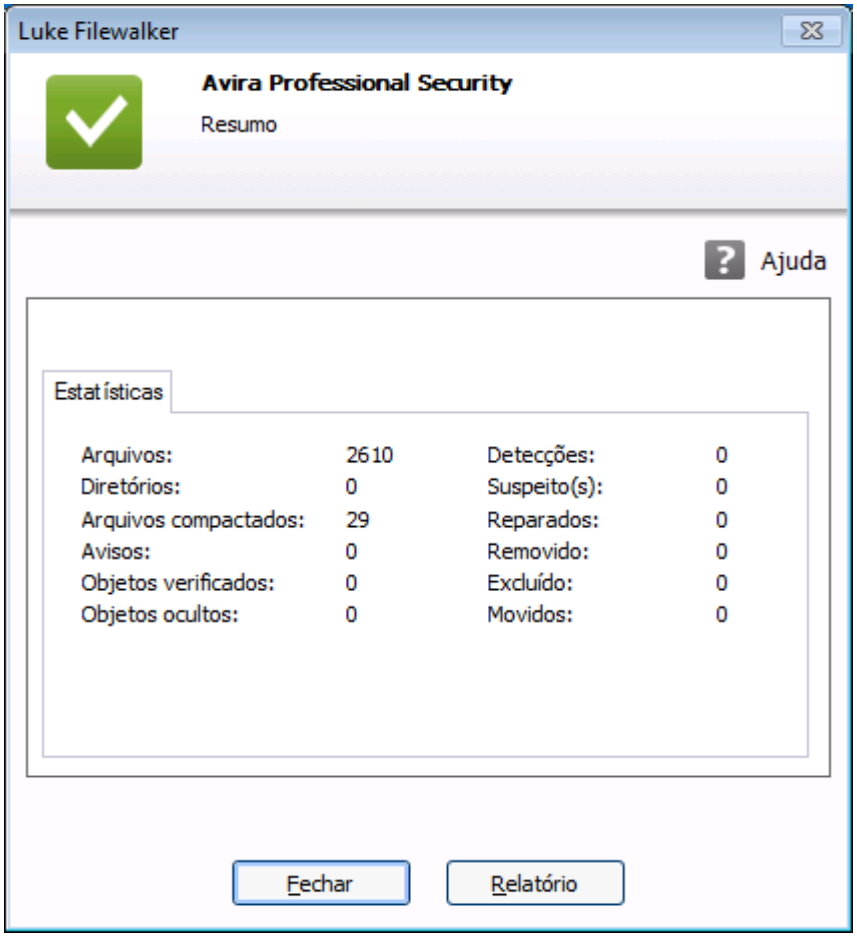
Observação
Os rootkits têm a capacidade de ocultar processos e objetos, tais como entradas de registro ou arquivos. No entanto, nem todo objeto oculto é necessariamente prova da existência de um rootkit. Os objetos ocultos também podem ser objetos inofensivos. Se uma verificação detectar objetos ocultos, mas não emitir um alerta de detecção de vírus, você deverá usar o relatório para determinar qual objeto é referido e obter mais informações sobre o objeto detectado.

Botões e links

Botão / Link	Descrição
	Com esse link - e com uma conexão ativa com a Internet - é possível acessar uma página da Internet com mais informações sobre esse vírus ou programa indesejado.
	Esta página da ajuda online é aberta por meio deste botão ou link.
Parar	O processo de verificação é interrompido.
Pausar	A verificação será interrompida e poderá ser retomada ao clicar no botão **Continuar**.
Continuar	A verificação interrompida continuará.
Finalizar	O System Scanner é fechado.

Relatório	O arquivo do relatório da verificação será mostrado.

6.2.2 Luke Filewalker: Estatísticas de Verificação



Informações exibidas: Estatísticas

Arquivos: Número de arquivos verificados

Diretórios: Número de diretórios verificados

Arquivo Morto: Número de arquivos mortos verificados

Avisos: Número de alertas sobre vírus detectados

Objetos Pesquisados: Número de objetos verificados durante a verificação de rootkits

Objetos Ocultos: Número de objetos ocultos detectados (rootkits)

Detecções: Número de vírus e programas indesejados detectados

Suspeito: Número de arquivos relatados pela heurística

Reparado: Número de arquivos reparados

Apagado: Número de arquivos substituídos

Excluído: Número de arquivos excluídos

Movido: Número de arquivos que são movidos para quarentena

Botões e links

Botão / Link	Descrição
	Esta página da ajuda online é aberta por meio deste botão ou link.
Fechar	A janela de resumo é fechada.
Relatório	O arquivo do relatório da verificação será mostrado.

7. Centro de Controle

7.1 Visão geral do Centro de controle

O Centro de controle é um centro de informações, configuração e gerenciamento. Além das seções que podem ser selecionadas individualmente, existem diversas opções que podem ser acessadas na barra de menus.Além das seções que podem ser selecionadas individualmente, existem diversas opções que podem ser acessadas na barra de menus.

Barra de menus

Todas as funções do Centro de Controle estão contidas na barra de menus.

Arquivo

- Sair (Alt + F4)

Exibir

- Status
- Proteção do PC
  - Scanner
  - Real-Time Protection
- Proteção na Internet
  - FireWall
  - Web Protection
  - Mail Protection
- Administração
  - Quarentena
  - Agendamento
  - Relatórios
  - Eventos
- Atualizar (F5)

Extras

- Varredura dos registros de inicialização...
- Lista de detecções...
- Download do CD de resgate
- Configuração (F8)

Atualização

- Iniciar atualização...
- Atualização manual...

Ajuda

- Sumário
- Leia-me
- Ajude-me
- Fazer download do manual
- Carregar arquivo de licença...
- Enviar feedback
- Sobre o Avira Professional Security

> **Nota**
> A navegação do teclado pode ser ativada na barra de menus com a ajuda da tecla [ALT]. Se a navegação estiver ativada, você poderá percorrer o menu com as teclas de seta. Com a tecla Voltar, você ativa o item de menu ativo.

Seções de navegação

Na barra de navegação esquerda são encontradas as seguintes seções:

- **Status**

PROTEÇÃO DO PC

- Scanner
- Real-Time Protection

PROTEÇÃO NA INTERNET

- FireWall
- Web Protection
- Mail Protection

ADMINISTRAÇÃO

- Quarentena
- Agendamento
- Relatórios
- Eventos

Descrição da navegação

- **Status**: Clicar na barra **Status** fornece uma visão geral da funcionalidade do produto e do desempenho (consulte Status).
  - A seção **Status** permite ver rapidamente quais módulos estão ativos e fornece informações sobre a última atualização realizada.
- *PROTEÇÃO DO PC*: Nesta seção você localizará os componentes para verificar os arquivos em seu sistema do computador em busca de vírus e malwares.
  - A seção Scanner permite configurar e iniciar facilmente uma varredura por demanda. Perfis predefinidos ativa uma varredura com opções padrão já adaptadas. Do mesmo modo, é possível adaptar a varredura de vírus e programas indesejados de acordo com seus requisitos pessoais com a ajuda da seleção manual (será salva) ou com a criação de perfis definidos pelo usuário.
  - A seção Real-Time Protection exibe informações sobre arquivos verificados, assim como outros dados estatísticos, que podem ser redefinidos a qualquer momento e permite acesso ao arquivo de relatório. Informações mais detalhadas sobre o último vírus ou programa indesejado detectado podem ser obtidas praticamente "com o clicar de um botão".
- *PROTEÇÃO NA INTERNET*: Nesta seção você localizará os componentes para proteger seu sistema do computador contra vírus e malwares da Internet e contra acesso à rede não autorizado.
  - A seção FireWall permite configurar as configurações básicas do FireWall. Além disso, são exibidos a taxa de transferência de dados atual e todos os aplicativos ativos que usam uma conexão de rede.
  - A seção Web Protection apresenta informações sobre URLs verificados e vírus detetados e outros dados estatísticos, que podem ser redefinidos a qualquer momento e permite o acesso ao arquivo de relatório. Informações mais detalhadas sobre o último vírus ou programa indesejado detectado podem ser obtidas praticamente "com o clicar de um botão".
  - A seção Mail Protection mostra todos os e-mails verificados pelo Mail Protection, suas propriedades e outros dados estatísticos. Também é possível excluir endereços de e-mail da futura varredura de malware ou spam. Os e-mails também podem ser excluídos do buffer do Mail Protection.
- *ADMINISTRAÇÃO*: Nesta seção você localizará ferramentas para isolar e gerenciar arquivos suspeitos ou infectados e para planejar tarefas recorrentes.
  - A seção Quarentena contém o conhecido gerenciador de quarentena. Este é o ponto central para os arquivos já colocados na quarentena ou para os arquivos suspeitos que deseja colocar na quarentena. Também é possível enviar um arquivo selecionado para o Avira Malware Research Center por e-mail.
  - A seção Agendamento permite configurar trabalhos programados de varredura e atualização, bem como trabalhos de backup, e adaptar ou excluir os trabalhos existentes.
  - A seção Relatórios permite visualizar os resultados de ações executadas.
  - A seção Eventos permite visualizar os eventos gerados por determinados módulos do programa.

Botões e links

Os botões e links a seguir pode estar disponíveis.

Botão / link	Atalho	Descrição
Configuração		Esse botão ou link é usado para acessar o diálogo de configuração correspondente da seção.
	F1	Esse botão ou link abre o tópico da ajuda on-line correspondente da seção.

7.2 Arquivo

7.2.1 Sair

O item de menu **Sair** no menu **Arquivo** fecha o Centro de Controle.

7.3 Exibir

7.3.1 Status

A tela inicial do Centro de controle, a seção **Status**, permite ver com uma visão rápida se o sistema do computador está protegido e quais módulos do Avira estão ativos. A janela **Status** também fornece informações sobre a última atualização realizada. Você também pode ver se possui uma licença válida.

- Proteção do PC: Proteção em Tempo Real, Última varredura, Última atualização, Seu produto está ativado
- Proteção na Internet : Web Protection, Mail Protection, FireWall, Modo de apresentação,

> **Nota**
> O Controle de Conta de Usuário vai pedir a você permissão para habilitar ou desabilitar a Real-Time Protection, FireWall, Web Protection e serviços de Mail Protection nos sistemas operacionais a partir do Windows Vista.

Proteção do PC

As informações sobre o status atual do serviço e das funções de proteção que protegem o computador localmente contra vírus e malware da Internet estão exibidas nessa seção.

Real-Time Protection

As informações sobre o status atual do Real-Time Protection são exibidas nesse campo.

É possível ativar ou desativar o Real-Time Protection clicando no botão **ON/OFF**. Outras opções do Real-Time Protection podem ser acessadas clicando em **Real-Time Protection** na barra de navegação. Inicialmente você recebe informações sobre o último malware e arquivos infectados encontrados. Clique em **Configuração** para definir outras configurações.

- **Configuração**: Acesse a Configuração para definir as configurações dos componentes do Real-Time Protection.

As seguintes possibilidades estão disponíveis:

Ícone	Status	Opção	Descrição
	*Ativado*	**Desativar**	O serviço Real-Time Protection está ativo, ou seja, o sistema é monitorado continuamente quanto a vírus e programas indesejados. **Nota** É possível desabilitar o serviço Real-Time Protection. No entanto, observe que se o Real-Time Protection for desativado você não estará mais protegido contra vírus e programas indesejados. Todos os arquivos podem passar despercebidos pelo sistema e causar danos.

	*Desativado*	**Ativar**	O serviço Real-Time Protection está desativado, ou seja, o serviço está carregado, mas não está ativo. **Aviso** Não é realizada nenhuma varredura quanto a vírus e programas indesejados. Todos os arquivos podem passar despercebidos pelo sistema. Você não está protegido contra vírus e programas indesejados. **Nota** Para ficar protegido contra vírus e programas indesejados, clique no botão **LIGA/DESLIGA** ao lado do **Real-Time Protection** na área *Proteção do PC*.

	*Serviço interrompido*	**Iniciar serviço**	O serviço Real-Time Protection está interrompido. **Aviso** Não é realizada nenhuma varredura quanto a vírus e programas indesejados. Todos os arquivos podem passar despercebidos pelo sistema. Você não está protegido contra vírus e programas indesejados. **Nota** Para ficar protegido contra vírus e programas indesejados, clique no botão **LIGA/DESLIGA** ao lado do **Real-Time Protection** na área *Proteção do PC*. O estado atual deve ser exibido em verde, o que significa **Ativado**.

	Desconhecido	**Ajuda**	Esse status é exibido quando ocorre um erro desconhecido. Nesse caso, entre em contato com o nosso Suporte.

Última varredura

As informações sobre a última varredura do sistema executada são exibidas nesse campo. Quando uma varredura do sistema completa é executada, todos os discos rígidos no computador são verificados totalmente. São empregados todos os processos de varredura, com exceção da varredura da integridade dos arquivos do sistema: varredura padrão dos arquivos, varredura do registro e dos setores de inicialização, varredura dos rootkits etc.

Os seguintes detalhes são exibidos:

- Data da última varredura completa do sistema

As seguintes possibilidades estão disponíveis:

Varredura do sistema	Opção	Descrição
Não executado	**Verificar sistema**	Nenhuma verificação completa do sistema foi executada desde a instalação. **Aviso** O status do sistema é não verificado. Vírus ou programas indesejados talvez sejam encontrados em seu computador. **Nota** Para verificar o computador, clique no link **Verificar sistema**.
Data da última varredura do sistema, por exemplo, *18/09/2011*	**Verificar sistema**	Você executou uma varredura completa do sistema na data especificada. **Nota** Recomendamos que use o trabalho de varredura padrão *Varredura completa do sistema*. Use o Agendamento para ativar o trabalho **Varredura completa do sistema**.
Desconhecido	**Ajuda**	Esse status é exibido quando ocorre um erro desconhecido. Nesse caso, entre em contato com o nosso Suporte.

Última atualização

As informações sobre o status atual da última atualização realizada são exibidas aqui.

Os seguintes detalhes são exibidos:

- Data da última atualização
  - Clique no botão **Abrir configuração** para definir outras configurações de atualização automática.

As seguintes possibilidades estão disponíveis:

Ícone	Status	Opção	Descrição
	*Data da última atualização, por exemplo, 18/07/2011*	**Iniciar atualização**	O programa foi atualizado nas últimas 24 horas. **Nota** Você pode atualizar o produto Avira para a versão mais recente com o botão **Iniciar atualização**.
	*Data da última atualização, por exemplo, 18/07/2011*	**Iniciar atualização**	Já se passaram 24 horas desde a atualização, mas você ainda está no ciclo de lembretes de atualização escolhido. Isso depende das definições da configuração. **Nota** Você pode atualizar o produto Avira para a versão mais recente com o botão **Iniciar atualização**.

	Não executado	**Iniciar atualização**	Desde a instalação, nenhuma atualização foi realizada -ou- O ciclo de lembretes de atualização foi excedido (consulte Configuração) e nenhuma atualização foi realizada -ou- O arquivo de definição de vírus é mais antigo que o ciclo de lembretes de atualização selecionado (consulte Configuração). **Nota** Você pode atualizar o produto Avira para a versão mais recente com o botão **Iniciar atualização**.
		Não disponível	Se a licença tiver expirado, nenhuma atualização pode ser realizada.

Seu produto está ativado

As informações sobre o status atual da sua licença são exibidas nesse campo.

As seguintes possibilidades estão disponíveis:

Versão completa

Ícone	Status	Opção	Significado
	*Data de validade da licença atual para uma versão completa, por exemplo 31/10/2011*	**Renovar**	Você tem uma licença válida do produto Avira. Você pode acessar a loja on-line da Avira com o botão **Renovar**. Ali você pode adaptar sua licença atual às suas necessidades e atualizar para o Avira Premium.
	*Data de validade da licença atual para uma versão completa, por exemplo 31/10/2011*	**Renovar**	Você tem uma licença válida do produto Avira. No entanto, o período de licenciamento é igual ou inferior a trinta dias. Use o botão **Renovar** para acessar a loja on-line da Avira. Na loja, você pode estender a licença atual.

	*A licença expirou, por exemplo, em 31/08/2011*	**Comprar**	A sua licença do produto Avira expirou. Use o botão **Comprar** para acessar a loja on-line da Avira. Na loja, você pode comprar uma licença válida. **Aviso** Se a sua licença tiver expirado, não poderá mais fazer atualizações. As funções de proteção do programa são desativadas e não podem mais ser ativadas.

Licença de avaliação

Ícone	Status	Opção	Significado
	*Data de validade da licença de avaliação, por exemplo, 31/10/2011*	**Comprar**	Você tem uma licença de avaliação que permite testar a linha completa de funções do produto Avira durante um tempo determinado. Use o botão **Comprar** para acessar a loja on-line da Avira. Na loja, você pode comprar uma licença válida.
	*Data de validade da licença de avaliação, por exemplo, 31/10/2011*	**Renovar**	Você tem uma licença de avaliação. No entanto, o período de licenciamento é igual ou inferior a trinta dias. Use o botão **Renovar** para acessar a loja on-line da Avira. Na loja, você pode comprar uma licença válida.

	*A licença de avaliação expirou em: 31/10/2011*	**Comprar**	A sua licença do produto Avira expirou. Use o botão **Comprar** para acessar a loja on-line da Avira. Na loja, você pode comprar uma licença válida. **Aviso** Se a sua licença tiver expirado, não poderá mais fazer atualizações. As funções de proteção do programa são desativadas e não podem mais ser ativadas.

Proteção na Internet

As informações sobre o status atual do serviço que protegem o computador contra vírus e malwares da Internet são exibidos nessa seção.

- **FireWall**: O serviço monitora os canais de comunicação de entrada e saída do computador.
- **Web Protection**: O serviço verifica os dados que são transmitidos e carregados no navegador enquanto você navega na Internet (monitoramento das portas 80, 8080, 3128).
- **Mail Protection**: O serviço verifica e-mails e anexos em busca de vírus e malware.
- **Modo de apresentação**: se configurado como automático, o produto Avira alterna automaticamente para o Modo de apresentação para todo aplicativo que executar em tela cheia.

Outras opções para esses processos podem ser acessadas em um menu contextual clicando no ícone de configuração ao lado do botão **LIGA/DESLIGA**.

- **Configurar**: acesse Configuração para definir as configurações do componente do processo.

As seguintes possibilidades estão disponíveis: *Serviços*

Ícone	Status	Status do processo	Opção	Significado
	*OK*	*Ativado*	**Desativar**	Todos os serviços para Proteção na Internet estão ativos. **Nota** É possível desativar um serviço clicando no botão **LIGA/DESLIGA** . No entanto, você não estará mais totalmente protegido contra vírus e malwares assim que o serviço for desativado.
	*Restrito*	*Desativado*	**Ativar**	Um serviço está desativado, ou seja, o serviço foi iniciado, mas não está ativo. **Aviso** O seu sistema de computador não está sendo totalmente monitorado. Vírus e programas indesejados talvez acessem seu computador. **Nota** Para ativar o serviço, clique no botão **LIGA/DESLIGA**.

	Aviso	*Serviço interrompido*	**Iniciar serviço**	Um serviço foi interrompido **Aviso** O seu sistema de computador não está sendo totalmente monitorado. Vírus e programas indesejados talvez acessem seu computador. **Nota** Clique no botão **LIGA/DESLIGA** para iniciar o serviço e o seu sistema de computador passar a ser monitorado. O serviço é iniciado e ativado.
		Desconhecido	**Ajuda**	Esse status é exibido quando ocorre um erro desconhecido. Nesse caso, entre em contato com o nosso Suporte.

7.3.2 Modo Apresentação

Se um aplicativo foi executado em modo de tela cheia no sistema de computador, as notificações de desktop podem ser suspensas intencionalmente como janelas pop-up e mensagens no produto ativando o modo Apresentação. Todas as regras de aplicativo e adaptador configuradas no Avira FireWall se aplicam, mas nenhuma janela pop-up aparece com notificação de evento de rede.

O Modo de Apresentação pode ser ativado ou mantido em modo automático clicando no botão **ON/OFF**. Por padrão, o Modo de Apresentação está definido para **automático** e é exibido em cor verde. A configuração padrão define o recurso para automático, de modo que toda vez que for executado um aplicativo que precisar do modo de tela cheia, o produto Avira alterna automaticamente para o Modo de Apresentação.

- Clique no botão à esquerda do botão **DESLIGAR** para ativar o Modo Apresentação.
  - ↪ O Modo Apresentação é ativado e exibido em cor amarela.

Nota
É recomendável trocar a configuração padrão **DESLIGAR** pelo seu modo automático de reconhecimento de tela cheia apenas temporariamente, porque não serão recebidos avisos e notificações de desktop visíveis com relação a eventos de rede e ameaças possíveis.

7.3.3 Scanner

A seção **Scanner** permite configurar e iniciar facilmente uma varredura do sistema. Perfis predefinidos permitem uma varredura do sistema com opções padrão já adaptadas. Da mesma maneira é possível adaptar a varredura do sistema quanto a vírus e programas indesejados para os seus requisitos pessoais com ajuda de seleção ou criando perfis definidos pelo usuário. A ação desejada pode ser selecionada pelo ícone na barra de ferramentas, pelo atalho ou pelo menu contextual. Iniciar uma varredura através do item Iniciar a varredura com o perfil selecionado.

A exibição e a manipulação dos perfis editáveis são semelhantes às do Windows Explorer. Cada pasta do diretório principal corresponde a um perfil. Pastas ou arquivos a serem verificados são selecionados ou podem ser selecionados com uma marca de varredura na frente da pasta ou do arquivo a ser verificado.

- Para alterar diretórios, clique duas vezes no diretório desejado.
- Para alterar as unidades, clique duas vezes na letra da unidade desejada.
- Para selecionar pastas e unidades, pode clicar na caixa na frente do ícone da pasta ou unidade ou selecionar via o menu contextual.
- Você pode navegar pela estrutura de menus com a ajuda da barra de rolagem e das setas de rolagem.

Perfis predefinidos

Os perfis de varredura predefinidos estão disponíveis se necessários.

Nota
Esses perfis são somente leitura e não podem ser alterados ou excluídos. Para adaptar um perfil a suas necessidades, selecione para uma varredura individual a pasta Seleção manual ou Criar novo perfil para criar um perfil definido pelo usuário, que pode ser salvo.

Nota
As opções de varredura para os perfis predefinidos podem ser definidas em Configuração > Scanner > Varredura > Arquivos. É possível adaptar essas configurações a suas necessidades.

Unidades locais

Todas as unidades locais do sistema são verificadas quanto a vírus ou programas indesejados.

Discos rígidos locais

Todos os discos rígidos locais do sistema são verificados quanto a vírus ou programas indesejados.

Unidades removíveis

Todas as unidades removíveis disponíveis do sistema são verificadas quanto a vírus ou programas indesejados.

Diretório do sistema Windows

O diretório do sistema Windows do sistema é verificado quanto a vírus ou programas indesejados.

Varredura completa do sistema

Todos os discos rígidos locais do computador são verificados quanto a vírus ou programas indesejados. Durante a varredura, são usados todos os processos de varredura, com exceção da verificação de integridade dos arquivos do sistema: varredura padrão dos arquivos, varredura do registro e dos setores de inicialização, varredura dos rootkits, etc. (consulte Scanner > Visão geral). Os processos de varredura são realizados independentemente da definição do scanner na configuração em Scanner > Varredura: outras configurações.

Varredura rápida do sistema

As pastas mais importantes do sistema (diretórios *Windows*, *Programs*, *Documents and Settings\Local User*, *Documents and Settings\All Users*) são verificadas quanto a vírus e programas indesejados.

Meus documentos

O local padrão de "*Meus documentos*" do usuário conectado é verificado quanto a vírus e programas indesejados.

Nota
No Windows, "*Meus documentos*" é um diretório no perfil do usuário que é usado como o local padrão para documentos que precisam ser salvos. A configuração padrão do diretório é *C:\Documents and Settings\[nome do usuário]\My Documents*.

Processos ativos

Todos os processos atuais são verificados quanto a vírus ou programas indesejados.

Verificar rootkits e malware ativo

O computador não é verificado quanto a rootkits e programa de malware ativos (em execução). Todos os processos em execução são verificados.

Nota
No modo interativo existem várias maneiras de reagir a uma detecção. No modo automático a detecção é registrada no arquivo de relatório.

Nota
A varredura de rootkit não está disponível para o Windows XP de 64 bits !

7.3.4 Seleção manual

Selecione esta pasta para adaptar a varredura às suas necessidades individuais. Marque os diretórios e arquivos que deverão ser verificados. Se o seu produto Avira for gerenciado pelo Avira Management Console, você pode usar o campo **Seleção manual** na caixa de diálogo **Comandos** para verificar diversos diretórios, separados por '?' (por exemplo: `c:\temp?d:\test`).

Nota
O perfil **Seleção manual** é usado para verificar dados sem criar um novo perfil primeiro.

Perfis definidos pelo usuário

Um novo perfil pode ser criado através da barra de ferramentas, do atalho ou do menu contextual.

Novos perfis podem ser salvos com o nome desejado e, além da varredura controlada manualmente, são úteis para criar varreduras programadas com a ajuda do Agendamento.

Barra de ferramentas e atalhos

Ícone	Atalho	Descrição
	**F3**	**Iniciar varredura com o perfil selecionado** O perfil selecionado é verificado quanto a vírus ou programas indesejados.
	**F6**	**Iniciar varredura com o ícone selecionado como Administrador** O perfil selecionado é verificado com direitos administrativos
	**Ins**	**Criar novo perfil** Um novo perfil é criado.
	**F2**	**Renomear perfil selecionado** Um novo nome do perfil selecionado é salvo.
	**F4**	**Criar link na área de trabalho para o perfil selecionado** Um link para o perfil selecionado é criado na área de trabalho.
	**Del**	**Excluir perfil selecionado** O perfil selecionado é excluído de forma irrecuperável.

Menu contextual

O menu contextual desta seção pode ser obtida selecionando um perfil necessário com o mouse e mantendo o botão direito do mouse pressionado.

Iniciar varredura

O perfil selecionado é verificado quanto a vírus ou programas indesejados.

Iniciar varredura (admin)

(Essa função só está disponível no Windows Vista. É necessário ter direitos de administrador para executar essa ação.)

O perfil selecionado é verificado quanto a vírus ou programas indesejados.

Criar novo perfil

Um novo perfil é criado. Selecione os diretórios e arquivos que devem ser verificados.

Renomear perfil

Fornece ao perfil selecionado o nome escolhido por você.

> **Nota**
> Essa entrada não poderá ser selecionada no menu contextual se um perfil predefinido for selecionado.

Excluir perfil

O perfil selecionado é excluído de forma irrecuperável.

> **Nota**
> Essa entrada não poderá ser selecionada no menu contextual se um perfil predefinido for selecionado.

Filtro de arquivo

Padrão:

Significa que os arquivos são verificados de acordo com a configuração no grupo de Arquivos da Configuração. Você pode adaptar essa configuração aos seus requisitos na Configuração. Configuração pode ser acessada por meio do botão ou do link Configuração.

Varredura de todos os arquivos:

Todos os arquivos são verificados independentemente da definição na configuração.

Definido pelo usuário:

uma caixa de diálogo é aberta na qual são exibidas todas as extensões que são verificadas. As entradas padrão são definidas para as extensões. No entanto, entradas podem ser adicionadas ou excluídas.

> **Nota**
> Essa entrada só pode ser selecionada no menu contextual quando o mouse está sobre uma caixa de seleção.
> A opção não está disponível nos perfis predefinidos.

Selecionar

Com subdiretórios:

Tudo é verificado no nó selecionado (marca de varredura preta).

Sem subdiretórios:

Somente os arquivos são verificados no nó selecionado (marca de varredura verde).

Somente subdiretórios:

Somente os subdiretórios são verificados no nó selecionado, não os arquivos que estão no nó (marca de varredura cinza, os subdiretórios têm uma marca de varredura preta).

Sem seleção:

a seleção é cancelada, o nó selecionado atualmente não é verificado (sem marca de varredura).

Nota
Essa entrada só pode ser selecionada no menu contextual quando o mouse está sobre uma caixa de seleção.
A opção não está disponível nos perfis predefinidos.

Criar link na área de trabalho

Cria um link para o perfil selecionado na área de trabalho.

Nota
Essa entrada não poderá ser selecionada no menu contextual se o perfil Seleção manual for selecionado, pois as configurações de Seleção manual não são salvas permanentemente.

7.3.5 Real-Time Protection

A seção **Real-Time Protection** exibe informações sobre arquivos verificados, assim como outros dados estatísticos que podem ser redefinidos a qualquer momento e permite acesso ao arquivo de relatório. Informações mais detalhadas sobre o último vírus ou programa indesejado detectado podem ser obtidas praticamente "com o clicar de um botão".

Nota
Se o serviço Real-Time Protection não for iniciado, o botão ao lado do módulo é exibido na cor amarela. Porém, o arquivo de relatório do Real-Time Protection pode ser exibido.

Barra de ferramentas

Ícone	Descrição
	**Exibir arquivo de relatório** O arquivo de relatório do Real-Time Protection é exibido.
	**Redefinir dados estatísticos** As informações estatísticas nesta seção são definidas como zero.

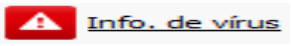
Informações exibidas

Último arquivo encontrado

Mostra o nome e o local do último arquivo encontrado pelo Real-Time Protection.

Ultimo vírus ou programa indesejado encontrado

Fornece o nome do último vírus ou programa indesejado encontrado.

Ícone/link	Descrição
	Clique no ícone ou link para exibir informações detalhadas sobre o vírus ou programa indesejado se houver uma conexão com a Internet.

Último arquivo verificado

Mostra o nome e o caminho do último arquivo verificado pelo Real-Time Protection.

Estatística

Número de arquivos

Mostra o número de arquivos verificados até o momento.

Número de detecções

Mostra o número de vírus e programas indesejados encontrados até o momento.

Número de arquivos suspeitos

Exibe o número de arquivos registrados pela heurística.

Número de arquivos excluídos

Mostra o número de arquivos excluídos até o momento.

Número de arquivos reparados

Mostra o número de arquivos reparados até o momento.

Número de arquivos movidos

Mostra o número de arquivos movidos até o momento.

Número de arquivos renomeados

Mostra o número de arquivos renomeados até o momento.

7.3.6 FireWall

Avira FireWall (Avira Professional Security)

A taxa de transferência de dados atual é exibida na seção FireWall. A seção FireWall permite configurar as definições básicas do Avira FireWall: o **nível de segurança** necessário pode ser configurado por meio de um controle deslizante. Para configurar um nível de segurança definido pelo usuário, você deve alternar para **Configuração**.

Barra de ferramentas

Ícone	Descrição
	**Redefinir estatísticas** As informações estatísticas nesta seção são definidas como zero.

Nível de segurança

Um dos seguintes níveis de segurança pode ser selecionado:

> **Nota**
> o nível de segurança pode ser alterado simplesmente arrastando o controle deslizante ao longo da escala de segurança. O nível de segurança selecionado é aplicado imediatamente após a seleção. Para obter informações mais detalhadas consulte a configuração do FireWall: Configuração > FireWall > Avira FireWall > Regras do adaptador.

Baixo

Flooding e varredura de porta são detectadas.

Meio

Os pacotes TCP e UDP suspeitos são descartados.

Flooding e varredura de porta são evitadas.

(Configurar como nível padrão.)

Alto

O computador não está visível na rede.

Novas conexões externas não são permitidas.

Flooding e varredura de porta são evitadas.

Personalizar

Regras definidas pelo usuário.

Bloquear todos

Todas as conexões de rede existente serão fechadas.

Transferir

As informações sobre a quantidade total e atual de dados enviados (*Upload*) e recebidos *(Download) são* exibidas nesta caixa. O valor máximo é exibido no canto superior esquerdo do gráfico.

A cor vermelha representa os pacotes de entrada e a cor verde os pacotes de saída. A área onde os dois estados se sobrepõem é cinza.

Firewall do Windows (Windows 7 ou superior)

Avira gerencia o Firewall do Windows a partir do Centro de Controle e Configuração.

A seção do FireWall permite verificar o estado do Firewall do Windows e restaurar as configurações recomendadas clicando no botão **Corrigir problema**.

7.3.7 Web Protection

A seção **Web Protection** mostra informações sobre URLs verificadas, além de outros dados estatísticos que podem ser redefinidos a qualquer momento e e permitem acesso ao arquivo de relatório. Informações mais detalhadas sobre o último vírus ou programa indesejado detectado podem ser obtidas praticamente "com o pressionamento de um botão".

Barra de ferramentas

Ícone	Descrição
	**Mostrar arquivo de relatório** O arquivo de relatório do Web Protection é exibido.
	**Redefinir dados estatísticos** As informações estatísticas nesta seção são definidas como zero.

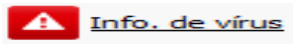
Informações exibidas

Último URL relatado

Exibe o último URL detectado pelo Web Protection.

Último vírus ou programa indesejado detectado

Fornece o nome do último vírus ou programa indesejado encontrado.

Ícone/link	Descrição
	Clique no ícone ou link para exibir informações detalhadas sobre o vírus ou programa indesejado se houver uma conexão com a Internet.

Último URL verificado

Mostra o nome e o caminho do último URL verificado pelo Web Protection.

Estatística

Número de URLs

Mostra o número de URLs verificados até o momento.

Número de detecções

Mostra o número de vírus e programas indesejados encontrados até o momento.

Número de URLs bloqueados

Mostra o número de URLs bloqueados anteriormente.

Número de URLs ignorados

Mostra o número de URLs ignorados anteriormente.

7.3.8 Mail Protection

A seção **Mail Protection** mostra todos os emails verificados pelo Mail Protection, suas propriedades e outros dados estatísticos.

Nota
Se o serviço Mail Protection não for iniciado, o botão ao lado do módulo é exibido na cor amarela. Porém, o arquivo de relatório do Mail Protection pode ser exibido. Se o módulo não estiver disponível no produto Avira, as caixas dessa seção estarão esmaecidas e não poderão ser selecionadas.

Nota
A eliminação de endereços de email individuais da verificação de malwares obviamente se aplica somente aos emails de entrada. Para desativar a verificação dos emails de saída, desative a verificação na configuração em Mail Protection > Verificar.

Barra de ferramentas

Ícone	Descrição
	**Exibir arquivo de relatório** O arquivo de relatório do Mail Protection é exibido.
	**Exibir propriedades do email selecionado** Abre uma caixa de diálogo com mais informações sobre o email selecionado.
	**Não verificar endereço de email em busca de malware** O endereço de email selecionado não será mais verificado em busca de vírus e programas indesejados no futuro. Essa configuração pode ser desfeita novamente em Mail Protection > Geral > Exceções.
	**Excluir o(s) email(s) selecionado(s)** O email selecionado é excluído do cache. No entanto, o email permanece no programa de email.

	Redefinir dados estatísticos As informações estatísticas nesta seção são definidas como zero.

Emails verificados

Essa área mostra os emails verificados pelo Mail Protection.

Ícone	Descrição
	Nenhum vírus ou programa indesejado foi encontrado.
	Um vírus ou programa indesejado foi encontrado.

Tipo

Mostra o protocolo usado para enviar ou receber o email:

- POP3: email recebido via POP3
- IMAP: email recebido via IMAP
- SMTP: email enviado via SMTP

De/para

Mostra o endereço do remetente do email.

Assunto

Mostra o assunto do email recebido.

Data/Hora

Mostra quando o email foi verificado em busca de spam.

> **Nota**
> Mais informações podem ser obtidas sobre um email clicando duas vezes no email relevante.

Estatística

Ação de email

Mostra a ação realizada quando o Mail Protection encontra um vírus ou programa indesejado em um email. No modo interativo nenhuma exibição está disponível aqui, pois você pode selecionar qual procedimento deve ser seguido em caso de detecção.

Nota
Você pode adaptar essa configuração às suas necessidades na Configuração. Configuração pode ser acessada por meio do botão ou do link **Configuração**.

Anexos afetados

Mostra a ação realizada quando Mail Protection encontra um vírus ou programa indesejado em um anexo afetado. No modo interativo nenhuma exibição está disponível aqui, pois você pode selecionar qual procedimento deve ser seguido em caso de detecção.

Nota
Você pode adaptar essa configuração às suas necessidades na Configuração. Configuração pode ser acessada por meio do botão ou do link **Configuração**.

Número de emails

Mostra o número de emails verificados pelo Mail Protection.

Última detecção

Fornece o nome do último vírus ou programa indesejado encontrado.

Número de detecções

Mostra o número de vírus e programas indesejados detectados e registrados anteriormente.

Emails suspeitos

Mostra o número de emails registrados pela heurística.

Número de emails de entrada

Mostra o número de emails recebidos.

Número de emails enviados

Mostra o número de emails enviados.

7.3.9 Quarentena

O **Gerenciador de quarentena** gerencia os objetos afetados (arquivos e e-mails). O produto Avira pode mover os objetos afetados para o diretório de quarentena em um formato especial. Não podem ser executados ou abertos.

Nota
Para mover objetos para o Gerenciador de quarentena, selecione a opção relevante para a quarentena em **Configuração** em **Scanner** e **Real-Time Protection** e **Mail Protection** - **Varredura > Ação na detecção** se estiver trabalhando em **modo automático**.
Como alternativa, pode selecionar a opção de quarentena relevante no **modo interativo**.

Barra de ferramentas, atalhos e menu contextual

Ícone	Atalho	Descrição
	**F2**	**Verificar novamente o(s) objeto(s)** Um objeto selecionado é verificado novamente em busca de vírus e programas indesejados. As configurações da varredura sob demanda são usadas para isso.
	**Retornar**	**Propriedades** Abre uma caixa de diálogo com informações mais detalhadas sobre o objeto selecionado. **Nota** Informações detalhadas podem ser obtidas também clicando duas vezes em um objeto.

  (Windows Vista)	**F3**	**Restaurar objeto(s)** Um objeto selecionado é restaurado. Em seguida, o objeto é colocado no seu local original. **Nota** Essa opção não está disponível para objetos do tipo e-mail. **Aviso** Danos graves no sistema devido a vírus e programas indesejados! Se arquivos forem restaurados: certifique-se de que somente arquivos que puderam ser limpos em outra varredura sejam restaurados. **Nota** No Windows Vista é necessário ter direitos de administrador para restaurar objetos.
	**F6**	**Restaurar objeto(s) para...** Um objeto selecionado pode ser restaurado em um local escolhido por você. Se essa opção for selecionada, a caixa de diálogo "Salvar como" será exibida; nessa caixa é possível selecionar o local do armazenamento. **Aviso** Danos graves no sistema devido a vírus e programas indesejados! Se arquivos forem restaurados: certifique-se de que somente arquivos que puderam ser limpos em outra varredura sejam restaurados.

	**Ins**	**Adicionar arquivo para quarentena** Se um arquivo for considerado suspeito, pode ser adicionado manualmente ao Gerenciador de quarentena com essa opção. Se um arquivo for considerado suspeito, pode ser adicionado ao Gerenciador de quarentena Avira com a opção Enviar objeto para investigação.
	**F4**	**Enviar objeto(s)** O objeto é carregado em um servidor da Web do Avira Malware Research Center para ser investigado pelo Avira Malware Research Center. Quando você clica no botão **Enviar objeto**, uma caixa de diálogo é aberta com um formulário para inserir seus dados de contato. Insira todos os dados necessários. Selecione um tipo: **Arquivo Suspeito** ou **Falso-Positivo** . Clique em **OK** para enviar o arquivo suspeito. **Observação** O tamanho dos arquivos carregados é limitado a 20 MB descompactados ou 8 MB compactados. **Nota** Você pode carregar vários arquivos ao mesmo tempo selecionando todos os arquivos que deseja enviar e, em seguida, clicando no botão **Enviar Objeto**.
	**Del**	**Excluir objeto(s)** Um objeto selecionado é excluído do Gerenciador de quarentena. O objeto não pode ser restaurado.
		**Copiar objeto(s) para** O objeto em quarentena realçado 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.

	**F7**	**Exportar todas as propriedades** As propriedades do objeto em quarentena realçado são exportadas em um arquivo de texto.
	**F10**	**Abrir diretório de quarentena** Abre o diretório INFECTADO.

Nota
Você tem a opção de executar ações em vários objetos realçados.
Para realçar vários objetos (objetos nas colunas), mantenha pressionada a tecla ctrl ou a tecla shift enquanto seleciona os objetos no gerenciador de quarentena. Pressione **Ctrl + A** para selecionar todos os objetos exibidos.
Quando a ação **Exibir propriedades** é executada, não é possível selecionar vários objetos.

Tabela

Status

Um objeto colocado em quarentena pode ter diferentes status:

Ícone	Descrição
	Nenhum vírus ou programa indesejado foi encontrado, o objeto está "limpo".
	Um vírus ou programa indesejado foi encontrado.
	Se um arquivo suspeito tiver sido adicionado ao Gerenciador de quarentena com a opção Adicionar arquivo, ele terá esse ícone de aviso.

Tipo

Designação	Descrição
E-mail	O objeto detectado é um e-mail.
Arquivo	O objeto detectado é um arquivo.

Detecção

Mostra o nome do malware encontrado.
Os resultados heurísticos são identificados com a abreviação HEUR/.

Origem

Mostra o caminho em que o objeto foi encontrado.

Data/Hora

Mostra a data e hora da detecção.

Informações detalhadas

Nome do arquivo

Caminho completo e nome do arquivo do objeto.

Objeto em quarentena

Nome do arquivo do objeto em quarentena.

Restaurado

SIM/ NÃO

SIM: o objeto selecionado foi restaurado.

NÃO:o objeto selecionado não foi restaurado.

Carregado para Avira

SIM/ NÃO

SIM: o objeto já foi carregado para um servidor da web do Avira Malware Research Center

para ser investigado pelo Avira Malware Research Center.

SIM: o objeto já foi carregado para um servidor da web do Avira Malware Research Center

para ser investigado pelo Avira Malware Research Center.

Sistema operacional

Windows XP: O malware foi identificado por um produto Avira de desktop.

Mecanismo de varredura

Número de versão do mecanismo de varredura

Arquivo de definição de vírus

Número de versão do arquivo de definição de vírus

Detecção

Nome do malware detectado.

Data/Hora

Data e hora da detecção

7.3.10 Agendamento

O **Agendamento** dá a opção de criar trabalhos de atualização e verificação programados e adaptar ou excluir trabalhos existentes.

Por padrão, o seguinte trabalho é criado após a instalação:

- Verificar trabalho **Verificação rápida do sistema** (ativado por padrão): Uma verificação rápida do sistema semanalmente é executada automaticamente. Durante a verificação rápida do sistema, somente pastas e arquivos importantes do computador são verificados quanto a vírus ou programas indesejados. . O trabalho **Verificação rápida do sistema** pode ser modificado, mas é recomendável criar outros trabalhos de verificação que reflitam melhor suas necessidades.

Barra de ferramentas, atalhos e menu contextual

Ícone	Atalho	Descrição
	**Ins**	**Inserir novo trabalho** Cria um novo trabalho. Um assistente o conduz pelas configurações necessárias.
	**Voltar**	**Propriedades** Abre uma caixa de diálogo com mais informações sobre o trabalho selecionado.
	**F2**	**Editar trabalho** Abre o assistente para criar e alterar um trabalho.
	**Del**	**Excluir trabalho** Exclui os trabalhos selecionados da lista.

		**Exibir arquivo de relatório** O arquivo de relatório do Agendamento é exibido.
	**F3**	**Iniciar trabalho** Inicia um trabalho marcado na lista.
	F4	**Interromper trabalho** Interrompe um trabalho iniciado e marcado.

Tabela

Tipo de trabalho

Ícone	Descrição
	O trabalho é um trabalho de atualização.
	O trabalho é um trabalho de verificação.

Nome

Nome do trabalho.

Ação

Indica se o trabalho é uma **verificação** ou uma **atualização**.

Frequência

Indica com que frequência e quando o trabalho é iniciado.

Modo de exibição

Os seguintes modos de exibição estão disponíveis:

Invisível: o trabalho é realizado em segundo plano e não é visível. Isso se aplica aos trabalhos de verificação e de atualização.

Minimizar: a janela do trabalho exibe somente uma barra de andamento.

Maximizar: a janela do trabalho fica completamente visível.

Ativado

O trabalho é ativado quando você ativa a caixa de seleção.

Nota
Se a frequência do trabalho tiver sido definida como Imediato, o trabalho será iniciado assim que for ativado. Isso possibilita reiniciar o trabalho, se necessário.

Status

Exibe o status do trabalho:

Pronto: o trabalho está pronto para execução.

Em execução: o trabalho foi iniciado e está sendo executado.

Criar trabalhos com o Agendamento

o assistente de planejamento oferece suporte no planejamento, na configuração e na criação

- uma verificação programada de vírus e programas indesejados
- uma atualização programada via Internet ou Intranet

Para os dois tipos de trabalho é necessário inserir

- o nome e a descrição do trabalho
- quando o trabalho deve ser iniciado
- com que frequência o trabalho deverá ser realizado
- o modo de exibição do trabalho

Frequência do trabalho

Frequência do trabalho	Descrição
Imediatamente	O trabalho é iniciado imediatamente após o término do assistente de planejamento.
Diariamente	O trabalho é iniciado todos os dias em uma determinada hora, por exemplo, 22:00.

Semanalmente	O trabalho é iniciado semanalmente em um determinado dia ou em vários dias da semana em uma determinada hora, por exemplo, terça-feira e sexta-feira às 16:26.
Intervalo	O trabalho é realizado em intervalos específicos, por exemplo, a cada 24 horas.
Única	O trabalho é realizado uma única vez em um horário definido, por exemplo, no dia 10.04.04 às 10:04.
Logon	O trabalho é realizado em cada logon de um usuário do Windows.

Hora inicial do trabalho

Você pode definir um dia da semana, data, hora ou intervalo para o horário de início do trabalho. Essa opção não será exibida se você tiver inserido **Imediatamente** como o horário de início.

Dependendo do tipo de trabalho, existem diversas opções adicionais

Também iniciar trabalho ao conectar à Internet (discada)

Além da frequência definida, o trabalho é realizado quando uma conexão com a Internet é configurada.
Essa opção pode ser selecionada com um trabalho de atualização que deve ser realizado diariamente, semanalmente ou em outros intervalos.

Repetir o trabalho se o tempo já tiver expirado

São realizados trabalhos passados que não puderam ser realizados no horário determinado, por exemplo, porque o computador estava desligado.
Essa opção pode ser selecionada tanto com um trabalho de atualização quanto com um trabalho de verificação que deve ser realizado diariamente, semanalmente, em intervalos ou uma única vez.

Desligar o computador se o trabalho tiver sido concluído

O computador é encerrado quando o trabalho é concluído. Os trabalhos de verificação podem ser exibidos minimizados e maximizados.

Nota
Com um trabalho de verificação é possível selecionar perfis predefinidos eperfis definidos pelo usuário na caixa de diálogo **Seleção do perfil**. O perfil Seleção manual é sempre realizado com a seleção atual.

7.3.11 Relatórios

A seção **Relatórios** permite acessar os resultados das ações executadas pelo programa.

Barra de ferramentas, atalhos e menu contextual

Ícone	Atalho	Descrição
	Voltar	**Exibir relatório** Abre uma janela na qual é exibido o resultado da ação selecionada. Por exemplo, o resultado de uma verificação.
	F3	**Exibir arquivo de relatório** Exibe o arquivo do relatório selecionado.
	F4	**Imprimir o arquivo de relatório** Abre a caixa de diálogo de impressão do Windows para imprimir o arquivo de relatório.
	Del	**Excluir relatório(s)** Exclui o relatório selecionado e o arquivo de relatório relevante.

Tabela

Status

Ícone	Descrição
	Verificar ação: concluído com êxito sem detectar vírus.
	Verificar ação: vírus detectado ou falha de conclusão.

	**Atualização da ação**: concluído com êxito.
	**Atualização da ação**: não concluído com êxito.

- **Ação**

  Mostra a ação executada.
- **Resultado**

  Mostra o resultado da ação.
- **Data/Hora**

  Mostra a data e a hora em que o relatório foi criado.

Conteúdo de um relatório de uma verificação

- *Data da verificação:*

  Data da verificação.
- *Hora inicial da verificação:*

  Hora inicial da verificação em hh:mm.
- *Tempo de verificação necessário:*

  A duração da verificação em formato mm:ss.
- *Status da verificação:*

  Mostra se a verificação foi concluída.
- *Última detecção:*

  Nome do último vírus ou programa indesejado encontrado.
- *Diretórios verificados:*

  Número total de diretórios verificados.
- *Arquivos verificados:*

  Número total de arquivos verificados.
- *Arquivos verificados:*

  Número de arquivos verificados.
- *Objetos ocultos:*

  Número total de objetos ocultos detectados
- *Detecções:*

  Número total de vírus e programas indesejados detectados.
- *Suspeito:*

  Número de arquivos suspeitos.
- *Avisos:*

Número de alertas sobre vírus detectados.

- *Informações:*

  Número de itens informativos emitidos, por exemplo, mais informações que podem surgir durante uma verificação.

- *Reparados:*

  Número total de arquivos reparados

- *Quarentena:*

  Número total de arquivos colocados em quarentena.

- *Renomeados:*

  Número total de arquivos renomeados.

- *Excluídos:*

  Número total de arquivos excluídos.

- *Apagados:*

  Número total de arquivos substituídos.

> **Nota**
> Os rootkits têm a capacidade de ocultar processos e objetos como entradas do registro ou arquivos. No entanto, nem todo objeto oculto é necessariamente prova da existência de um rootkit. Objetos ocultos também podem ser objetos inofensivos. Se uma verificação detectar objetos ocultos mas não emitir um alerta de detecção de vírus, o relatório deverá ser usado para determinar qual é o objeto de referência e obter mais informações sobre o objeto detectado.

7.3.12 Eventos

Eventos que foram gerados por vários componentes do programa serão exibidos em **Eventos**.

Os eventos são armazenados em um banco de dados. Você pode limitar o tamanho do banco de dados de eventos ou desativar a restrição de tamanho do banco de dados (consulte). Somente os eventos dos últimos 30 dias são salvos na configuração padrão. A exibição do evento é atualizada automaticamente quando a seção **Eventos** é selecionada.

> **Nota**
> A exibição não é atualizada automaticamente quando a seção for selecionada se houver mais de 20.000 eventos armazenados no banco de dados de eventos. Nesse caso, pressione **F5** para atualizar o visualizador de eventos.

Barra de ferramentas, atalhos e menu contextual

Ícone	Atalho	Descrição
	**Retornar**	**Mostrar evento selecionado** Abre uma janela na qual é exibido o resultado da ação selecionada. Por exemplo, o resultado de uma varredura.
	**F3**	**Exportar evento(s) selecionado(s)** Exporta eventos selecionados.
	**Del**	**Excluir evento(s) selecionado(s)** Exclui o evento selecionado.

Nota
Você tem a opção de executar ações em vários eventos selecionados. Para selecionar diversos eventos, mantenha pressionada a tecla **Ctrl** ou a tecla **Shift** (seleciona eventos consecutivos) à medida que seleciona os eventos desejados. Para selecionar todos os eventos exibidos, pressione **Ctrl + A**.
No caso da ação **Mostra evento selecionado**, não é possível executar a ação em várias seleções de objetos.

Módulos

Os eventos dos módulos a seguir (aqui em ordem alfabética) podem ser exibidos pelo visualizador de eventos:

Nome do módulo
FireWall
Serviço de ajuda
Mail Protection
Real-Time Protection

Agendamento
Scanner
Atualizador
Web Protection

Marcando a caixa **Tudo** você pode exibir os eventos de todos os módulos disponíveis. Para exibir somente os eventos de um módulo específico, marque a caixa ao lado do módulo necessário.

Filtro

A classificação de eventos a seguir pode ser exibida pelo visualizador de eventos.

Ícone	Descrição
	Informações
	Aviso
	Erro
	Detecção

Marcando a caixa **Filtrar**  , você pode exibir todos os eventos. Para exibir somente determinados eventos, marque a caixa ao lado do evento desejado.

Tabela

A lista de eventos contém as seguintes informações:

- **Ícone**

  O ícone da classificação do evento.
- **Tipo**

  Uma classificação da gravidade do evento: *Informaçãon*, *Aviso*, *Erro*, *Detecção*.
- **Módulo**

  O módulo que registrou o evento. Por exemplo, o módulo do Real-Time Protection que fez uma detecção.

- **Ação**

  Descrição do evento do respectivo módulo.

- **Data/Hora**

  A data e a hora local em que o evento ocorreu.

7.3.13 Atualizar

Atualiza a visualização da seção aberta.

7.4 Extras

7.4.1 Varredura de registros de inicialização

Você também pode verificar os setores de inicialização das unidades da estação de trabalho com uma verificação do sistema. É recomendável, por exemplo, quando uma verificação do sistema detectar um vírus e você deseja assegurar que os setores de inicialização não estão afetados.

É possível selecionar mais de um setor de inicialização mantendo a tecla Shift pressionada e selecionando as unidades necessárias com o mouse.

Nota
os setores de inicialização podem ser verificados automaticamente com uma verificação do sistema (consulte Varrer registros de inicialização selecionados).

Nota
No Windows Vista, é necessário ter direitos de administrador para verificar os setores de inicialização.

7.4.2 Lista de detecções

Esta função faz uma lista dos nomes dos vírus e programas indesejados reconhecidos pelo produto Avira. Existe uma função integrada conveniente de pesquisa de nomes.

Pesquisar na lista de detecções

insira uma palavra ou sequência de caracteres de pesquisa na caixa *Pesquisar:* .

Pesquisar sequência de caracteres dentro de um nome

Você pode inserir uma sequência consecutiva de letras ou caracteres aqui no teclado e o marcador se moverá até o primeiro ponto na lista de nomes que inclui essa

sequência – até mesmo no meio de um nome (por exemplo: "raxa" localiza "Abraxas").

Pesquisar a partir do primeiro caractere de um nome

Você pode inserir a primeira letra e os caracteres seguintes aqui no teclado e o marcador percorre a lista de nomes em ordem alfabética (por exemplo: "Ra" localiza "Rabbit").

Se o nome ou a sequência de caracteres procurado estiver disponível, a posição encontrada é marcada na lista.

Pesquisar para frente

Inicia a pesquisa para frente em ordem alfabética.

Pesquisar para trás

Inicia a pesquisa para trás em ordem alfabética.

Primeira correspondência

Percorre a lista até a primeira entrada encontrada.

Entradas da lista de detecções

Essa opção exibe uma lista de nomes de vírus ou programas indesejados que podem ser reconhecidos. A maioria das entradas dessa lista também pode ser removida com o produto Avira. Elas são listadas em ordem alfabética (primeiro caracteres especiais e números e, em seguida, as letras). Use a barra de rolagem para percorrer a lista para cima ou para baixo.

7.4.3 Download do CD de resgate

O comando de menu **Baixar CD de resgate** inicia o download do pacote Avira Rescue CD. O pacote contém um sistema dinâmico inicializável para computadores e um scanner antivírus da Avira com o arquivo de definição de vírus e o mecanismo de pesquisa mais atualizados. Você pode usar o Avira Rescue CD para iniciar e operar seu computador a partir do CD ou DVD se o sistema operacional estiver danificado, para resgatar dados ou executar uma verificação em busca de vírus e malwares.

Assim que o pacote Avira Rescue CD termina de ser baixado, uma caixa de diálogo é exibida na qual é possível selecionar uma unidade de CD/DVD para gravar o CD de resgate. Você também pode salvar o pacote Avira Rescue CD e gravar o CD posteriormente.

Nota
É necessário ter uma conexão ativa com a Internet para baixar o pacote Avira rescue CD. Para gravar o CD de resgate é necessário uma unidade de CD/DVD e um CD ou DVD gravável.

7.4.4 Configuração

O item de menu **Configuração** no menu **Extras** abre a Configuração.

7.5 Atualização

7.5.1 Iniciar atualização...

O item de menu **Iniciar atualização** no menu **Atualizar** inicia uma atualização imediata. O arquivo de definição de vírus e o mecanismo de varredura são atualizados.

7.5.2 Atualização manual...

O item de menu **Atualização manual...** no menu **Atualizar** abre uma caixa de diálogo para selecionar e carregar um pacote de atualização do VDF/mecanismo de pesquisa. O pacote de atualização pode ser baixado do site do fabricante e contém o arquivo de definição de vírus e o mecanismo de pesquisa atuais:
http://www.avira.com/pt-br/

> **Observação**
> No Windows Vista, você precisa ter direitos de administrador para efetuar uma atualização manual.

7.6 Ajuda

7.6.1 Tópicos

O item de menu **Tópicos** no menu **Ajuda** abre a lista de sumário da ajuda on-line.

7.6.2 Ajude-me

Quando houver uma conexão de Internet ativa, o item **Ajude-me** no menu **Ajuda** abre a página Suporte relevante do produto no site da Avira. Ali você pode ler respostas a perguntas frequentes, consultar a base de conhecimentos e entrar em contato com o Suporte Avira.Ali você pode ler respostas a perguntas frequentes, consultar a base de conhecimentos e entrar em contato com o Suporte Avira.

7.6.3 Fazer download do manual

Quando houver uma conexão de Internet ativa, o comando de menu **Fazer download do manual** no menu **Ajuda** abre a página de download do produto Avira. Ali você encontrará o link para download da versão atual do manual do produto Avira.

7.6.4 Carregar arquivo de licença

O item de menu **Carregar arquivo de licença** no menu **Ajuda** abre um diálogo para carregar o arquivo de licença *.KEY*.

> **Observação**
> No Windows Vista, você precisa ter direitos de administrador para carregar o arquivo de licença.

7.6.5 Enviar feedback

Quando houver uma conexão ativa com a Internet, o comando de menu **Enviar feedback** no menu **Ajuda** abre uma página de feedback para produtos Avira. Ali você encontrará um formulário de avaliação do produto que pode enviar para a Avira com suas avaliações da qualidade do produto e outras sugestões.

7.6.6 Sobre Avira Professional Security

- **Geral**

  Endereços e informações do produto Avira.
- **Informações da versão**

  Informações da versão dos arquivos no pacote do produto Avira.
- **Informações da licença**

  Dados da licença da licença atual e links para a loja on-line (comprar ou estender uma licença).

> **Nota**
> Os dados da licença podem ser salvos no cache. Clique com o botão direito na área *Dados da licença*. Um menu contextual é aberto. No menu contextual, clique no comando de menu **Copiar para área de transferência**. Seus dados de licença são salvos na área de transferência e podem ser adicionados a emails, formulários ou documentos através do comando **Adicionar** do Windows.

8. Configuração

8.1 Configuração

- Visão geral das opções de configuração
- Perfis de configuração
- Botões

Visão geral das opções de configuração

As seguintes opções de configuração estão disponíveis:

- **Scanner**: configuração de uma varredura do sistema (sob demanda)
  - Opções de varredura
  - Resolução de na detecções
  - Mais ações
  - Opções de varredura do arquivo
  - Exceções de varredura do sistema
  - Heurística de varredura do sistema
  - Configuração da função de registro
- **Real-Time Protection**: configuração de uma varredura em tempo real (durante o acesso)
  - Opções de varredura
  - Resolução de na detecções
  - Mais ações
  - Exceções de varredura durante o acesso
  - Heurística de varredura durante o acesso
  - Configuração da função de registro
- **Atualização**: Configuração das configurações de atualização, faça o download através do Servidor Web ou servidor de arquivos, configuração de atualizações de produtos
  - Fazer download através do servidor de arquivos
  - Fazer download através do servidor Web
  - Configurações de proxy
- **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 regra automática, parar o Firewall do Windows, notificações
- Configurações de pop-up (alertas para acesso de rede por parte dos aplicativos)

- **Web Protection**: Configuração da Web Protection
  - Opções de varredura, ativação e desativação da Web Protection
  - Resolução de na detecções
  - Acesso bloqueado: Tipos de arquivo e tipos MIME indesejados, filtro da Web para URLs indesejados (malware, phishing etc.)
  - Exceções de varredura da Web Protection: URLs, tipos de arquivo, tipos MIME
  - Heurística de Web Protection
  - Configuração da função de registro
- **Mail Protection**: Configuração da Mail Protection
  - Opções de varredura: ativar o monitoramento das contas POP3, das contas IMAP, dos e-mails enviados (SMTP)
  - Ações na detecção
  - Mais ações
  - Heurística de varredura da Mail Protection
  - Função AntiBot: servidores SMTP permitidos, remetentes de e-mail permitidos
  - Exceções de varredura da Mail Protection
  - Configuração do cache, limpar cache
  - Configuração de um rodapé nos e-mails enviados
  - Configuração da função de registro
- **Geral**:
  - Configuração de e-mail usando SMTP
  - Categorias de ameaça para o Scanner e o Real-Time Protection
  - Filtro de aplicativos: bloquear ou permitir aplicativos
  - Proteção avançada: Opções para ativar os recursos do ProActiv e do Protection Cloud.
  - Proteção com senha para acesso ao Centro de controle e à Configuração
  - Segurança: bloquear função autostart, exibição completa do status de varredura do sistema, proteção do produto, proteger arquivo hosts do Windows
  - WMI: Ativar o suporte a WMI
  - Configuração do registro de eventos
  - Configuração das funções de registro
  - Configuração dos diretórios usados
  - Alertas:
    Configuração de alertas de rede para componente(s):
    Scanner
    Real-Time Protection
    Configuração de alertas de e-mail para componente(s):
    Scanner

Real-Time Protection
Updater

- Configuração de alertas acústicos emitidos quando malwares são detectados

Perfis de configuração

Para gerenciar os perfis de configuração, clique no ícone da bandeja do lado direito da configuração padrão (consulte Ícone da bandeja).
Depois de clicar ali, uma série de opções será exibida e você poderá salvar as opções de configuração dos perfis de grupos: primeiro adicione uma nova configuração e digite os valores necessários na nova configuração, ou seja, defina as regras pelas quais esses perfis serão aplicados.

É possível escolher entre uma mudança manual da configuração ou uma automática. Para definir a mudança como automática, será necessário definir as regras a serem aplicadas.
As opções que são dadas são: escolher uma regra padrão que será aplicada cada vez que um gateway não atribuído for usado, ou definir um endereço IP ou endereço MAC (ou um endereço IP e uma máscara de rede) para definir o gateway padrão. Estes perfis de configuração serão aplicados toda vez que o gateway definido for usado.

Se nenhuma regra de comutação foi definida, você poderá alternar para uma configuração manualmente no menu contextual. É possível gerenciar os perfis de configuração utilizando o menu da opção configuração:

Menu contextual

Atalho	Menu contextual/descrição
Ins	**Criar nova configuração** Cria uma nova configuração com os valores padrão para as diversas opções de configuração.
F2	**Renomear configuração** Edita o nome da configuração.

Del	**Excluir configuração** Exclui a configuração realçada: primeiro, uma caixa de diálogo é aberta na qual é possível cancelar ou confirmar a configuração selecionada.
F4	**Copiar configuração** Copia a configuração realçada.

F6	**Redefinir configuração** Redefina as opções da configuração realçada aos valores padrão.
	Regras: Mostra as diferentes opções para definir regras para os perfis de configuração: **Nenhum** Não há nenhuma regra válida para alternar para a configuração realçada. A alternância para a configuração relevante deve ser executada manualmente. **Regra padrão** A configuração selecionada é usada como configuração padrão. Uma alternância automática para a configuração selecionada ocorre quando um gateway é usado e não é atribuído a nenhuma outra configuração. **Gateway padrão** Um endereço IP ou MAC do gateway padrão pode ser especificado como a regra de alternância para a configuração realçada. Uma alternância automática para a configuração selecionada ocorre quando o gateway padrão especificado é usado. **Endereço IP** Um endereço IP com a máscara de rede de um adaptador de rede pode ser especificado como a regra de alternância para a configuração realçada. Uma alternância automática para a configuração selecionada ocorre quando o endereço IP especificado é usado.

Nota
Você pode salvar até oito configurações.

Nota
Se uma regra aplicável não for encontrada ao alternar o gateway, a última configuração encontrada permanecerá ativa.

Botões

Botão	Descrição
Valores padrão	Todas as opções da configuração são restauradas aos valores padrão. Todas as correções e entradas personalizadas são perdidas quando as configurações padrão são restauradas.
OK	Todas as configurações feitas são salvas. A configuração é fechada. O Controle de Conta de Usuário vai pedir a você permissão para aplicar as alterações em sistemas operacionais a partir do Windows Vista.
Cancelar	A configuração é fechada sem salvar as definições.
Aplicar	Todas as configurações feitas são salvas. O Controle de Conta de Usuário vai pedir a você permissão para aplicar as alterações em sistemas operacionais a partir do Windows Vista.

8.2 Scanner

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

8.2.1 Varredura

É possível definir o comportamento da rotina de varredura por demanda. Se você selecionar alguns diretórios a serem verificados sob demanda, dependendo da configuração, o Scanner verificará:

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

Arquivos

O Scanner pode usar um filtro para varredura de 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. O filtro não é usado.

> **Nota**
> 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. Isso significa que o programa Avira decide se os arquivos são verificados ou não com base em seu conteúdo. Esse procedimento é um pouco mais lento do que Usar lista de extensão de arquivo, porém é mais seguro visto que não é apenas a extensão que é verificada. Essa opção é ativada como configuração padrão e é recomendada.

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

Usar lista de extensão de arquivo

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

> **Nota**
> Se essa opção for ativada e todas as entradas tiverem sido excluídas da lista com as extensões, aparecerá a mensagem "*Sem extensões*" 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 que são verificadas no modo "**Usar lista de extensões de arquivos"**. Entradas padrão são definidas para as extensões, mas as entradas podem ser adicionadas ou excluídas.

> **Nota**
> Observe que a lista padrão pode variar de acordo com a versão.

Configurações adicionais

Varrer registros de inicialização selecionados

Se essa opção for ativada, o Scanner verificará somente os setores de inicialização das unidades selecionadas para a varredura do sistema. Essa opção é ativada como a configuração padrão.

Varrer registros mestres de inicialização

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

Ignorar arquivos off-line

Se essa opção for ativada, a varredura direta ignorará os arquivos off-line por completo durante uma varredura. 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 a configuração padrão.

Varredura da integridade dos arquivos de sistema

Quando essa opção está ativada, os arquivos mais importantes do sistema Windows são submetidos a uma varredura particularmente segura das alterações realizadas por malwares durante cada varredura 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.

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

Nota
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 varredura do Scanner. Por razões de desempenho, a varredura utilizada é realizada somente no nível padrão.

Nota
Essa opção está disponível somente em sistemas com vários processadores. Se o seu programa Avira for gerenciado com AMC, a opção sempre será exibida e pode ser ativada: Se o sistema gerenciado não tiver mais de um processador, a opção Scanner não será utilizada.

Seguir links simbólicos

Se essa opção for ativada, o Scanner realizará uma varredura que segue todos os links simbólicos no perfil de varredura ou diretório selecionado e verifica os arquivos vinculados em busca de vírus e malwares.

Nota
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.

Procurar rootkits antes da varredura

Se essa opção for ativado e uma varredura for iniciada, o Scanner verificará o diretório do sistema Windows em busca de rootkits ativos em um atalho conhecido. Esse processo não verifica seu computador em busca de rootkits ativos de modo tão abrangente quanto o perfil de varredura "**Varredura de rootkits**", mas sua execução é significativamente mais rápida. Essa opção altera somente as configurações de perfis criados por você.

Nota
A varredura de rootkit não está disponível para o Windows XP de 64 bits

Fazer a varredura do registro

Se essa opção for ativada, o registro será verificado quanto a referências de malware. Essa opção altera somente as configurações de perfis criados por você.

Ignorar arquivos e caminhos nas unidades de rede

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

Processo da varredura

Permitir interrupção da varredura

Se essa opção for ativada, a varredura 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 varredura não é permitido! Essa opção é ativada como a configuração padrão.

Prioridade scanner

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

Baixo

O Scanner terá apenas o tempo de processador alocado pelo sistema operacional se nenhum outro processo exigir o tempo de computação, isto é, contanto que apenas o Scanner esteja em execução, a velocidade será máxima. Em suma, trabalhar com outros programas é ideal: o computador responderá mais rapidamente se outros programas exigirem o tempo de computação enquanto o Scanner continua em execução em segundo plano.

Normal

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

Alto

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

Resolução de na detecções

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

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 infectados ou cancelar o Scanner.

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

Ações permitidas

Nesta caixa de ações podem ser especificadas, que podem ser selecionadas no modo individual ou de notificação especialista para serem exibidas no caso de uma detecção de vírus.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 aos arquivos (por exemplo, com clique duplo) não será 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.

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

Nota
Se você tiver selecionado **Excluir** ou **Substituir e excluir** como ação padrão e desejar definir o modo de notificação para combinado, observe o seguinte: No caso de acessos heurísticos, os arquivos afetados não são excluídos, mas movidos para a 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 realizada quando o System Scanner encontra um vírus ou programa indesejado. Se a opção "" for selecionada mas o arquivo afetado não puder ser reparado, a ação selecionada em "" será realizada.

Nota
A opção só poderá ser selecionada se a configuração tiver sido selecionada em .

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 .

Nota
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 aos arquivos (por exemplo, com clique duplo) não será 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 for ativada, o arquivo é 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 " so poderá ser selecionada se a configuração tiver sido selecionada em ". 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 aos arquivos (por exemplo, com clique duplo) não será 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 . Esses 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 é 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 (limpá-lo). Não é possível restaurá-lo.

> **Nota**
> Se você tiver selecionado **Excluir** ou **Substituir e excluir** como ação primária ou secundária, observe 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.

> **Nota**
> 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 do sistema. Os eventos podem ser chamados no visualizador de eventos do Windows. A opção é desativada como configuração padrão.

Arquivos

Ao verificar os arquivos, o System Scanner utiliza uma verificação recursiva: Arquivamentos em arquivamentos também são descompactados e verificados quanto a vírus e programas indesejados. Os arquivos são verificados, descompactados e verificados novamente.

Varrer arquivos compactados

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

Todos os tipos de arquivo

Se essa opção for ativada, todos os tipos de arquivo da lista de arquivos compactados 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: e um arquivo *.zip tiver a extensão *.xyz, o System Scanner também descompactará e verificará esse arquivo. Essa opção é ativada como a configuração padrão.

Nota
Somente os tipos de arquivo marcados na lista são suportados.

Limitar profundidade da recursão

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

Nota
Para encontrar um vírus ou programa indesejado em um arquivo, o 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 recursividade máxima, a opção Profundidade máxima de 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 é 20, que é recomendado.

Valores padrão

O botão restaura os valores predefinidos para verificar os arquivos compactados.

Arquivos

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 do arquivo devem ser ignorados do Scanner

A lista dessa janela contém arquivos e caminhos que não devem ser incluídos pelo Scanner na varredura 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 varredura normal. Recomendamos que você sempre verifique esses arquivos quanto à presença de vírus ou programas indesejados antes que eles sejam incluídos nessa lista!

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

Aviso
Esses arquivos não são incluídos no processo de varredura!

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

Caixa de entrada

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

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

Adicionar

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

Excluir

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

Nota
Se você estiver gerenciando o programa Avira em AMC, você pode usar variáveis nos detalhes do caminho para exceções de arquivo. Você pode encontrar uma lista de variáveis que podem ser usadas em Real-Time Protection e Exceções do Scanner.

Heurística

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

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 seu produto Avira contém uma heurística de vírus de macros muito poderosa. Se essa opção for ativada, todas as macros no documento relevante serão excluídas em caso de reparo. Por outro lado, os arquivos suspeitos são apenas relatados, ou seja, você recebe um alerta. Essa opção é ativada como configuração padrão e é recomendada.

Detecção e análise heurística avançada (AheAD)

Ativar AHeAD

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

Nível de detecção baixo

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

Nível de detecção médio

Essa opção combina um nível de detecção forte com baixo risco de alertas falsos. Média será a configuração padrão se você tiver selecionado o uso dessa heurística.

Nível de detecção alto

Se esta opção for ativada, serão detectados significativamente mais malwares desconhecidos, mas há também a possibilidade de serem falso-positivos.

8.2.2 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.

Nota
Para ser capaz de definir as ações que o System Scanner realizou, quando vírus ou programas indesejados foram detectados, você deve ativar o arquivo de relatório na configuração .

Relatório

Desativado

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

Padrão

Padrão:quando essa opção é ativada, o System Scanner registra os nomes dos arquivos relacionados e seu caminho. 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. O relatório também contém um sufixo "(cloud)" para identificar as detecções do Protection Cloud.

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.

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

8.3 Real-Time Protection

A seção **Real-Time Protection** da configuração é responsável pela configuração da varredura durante o acesso.

8.3.1 Varredura

Em geral, você quer monitorar seu sistema constantemente. Para este fim, use o Real-Time Protection (= Scanner de acesso). Com ele, você pode executar a varredura de todos os arquivos que são copiados ou abertos no computador imediatamente em busca de vírus e programas indesejados.

Arquivos

O Real-Time 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.

> **Nota**
> 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 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 extensão de arquivo**, porém é mais seguro visto que não é apenas a extensão que é verificada.

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

Usar lista de extensão de arquivo

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

Nota
Se essa opção for ativada e todas as entradas tiverem sido excluídas da lista com as extensões, aparecerá a mensagem "Sem extensões" 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 que são verificadas no modo "**Usar lista de extensões de arquivos"**. Entradas padrão são definidas para as extensões, mas as entradas podem ser adicionadas ou excluídas.

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

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.

Nota
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. Elas não estarão mais protegidas contra vírus ou programas indesejados!

Nota
Quando os arquivos são executados em unidades de rede, eles são verificados pelo Real-Time 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 **Monitoriar unidades de rede** esteja desativada. Motivo: esses arquivos são acessados com os direitos “Executar arquivo”. Se desejar excluir esses arquivos ou, ou até mesmo os arquivos executados nas unidades de rede, da varredura feita pelo Real-Tim Protection, insira os arquivos na lista de objetos de arquivo a serem excluídos (consulte: Real-Time Protection > Varredura > Exceções).

Ativar armazenamento em cache

Se essa opção for ativada, os arquivos monitorados nas unidades de rede serão disponibilizados no cache do Real-Time 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

Varrer arquivos compactados

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

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

Profundidade máxima de recursão

Ao verificar os arquivos, o Real-Time Protection utiliza uma varredura recursiva: Arquivos em arquivos também são descompactados e verificados quanto a vírus e programas indesejados. É possível definir a profundidade de recursão. O valor padrão e recomendado para a profundidade recursiva é 1: todos os arquivos que estão diretamente localizados no arquivo principal são verificados.

Número máximo de arquivos

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

Resolução de na detecções

Você pode definir as ações a serem realizadas pelo Real-Time Protection quando um vírus ou programa indesejado for detectado.

Interativo

Se esta opção for ativada, é exibida uma notificação na área de trabalho quando o Real-Time Protection 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 a 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

O Real-Time Protection repara o arquivo infectado se possível.

Renomear

O Real-Time Protection renomeia o arquivo. Portanto, o acesso direto aos arquivos (por exemplo, com clique duplo) não será mais possível. O arquivo pode ser reparado posteriormente e renomeado de novo.

Quarentena

O Real-Time Protection move o arquivo para Quarentina. 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** (veja abaixo).

Ignorar

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

Substituir e excluir

O Real-Time Protection substitui o arquivo por um padrão antes de excluí-lo. Não é possível restaurá-lo.

Aviso
Se o Real-Time Protection estiver configurado para **Verificar durante a escrita**, o arquivo afetado não é 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**".

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

Clique aqui para obter mais informações.

Automático

Se esta opção for ativada, não aparecerá nenhuma caixa de diálogo em caso de vírus. O Real-Time Protection reage de acordo com as configurações pré-definidas nesta seção como ação primária e secundária.

Copiar arquivo para quarentena antes da ação

Se essa opção for ativada, o Real-Time Protection cria uma cópia de backup antes de realizar a ação primária ou secundária solicitada. A cópia de backup é salva na quarentena. Ela poderá ser restaurada através do Gerenciador de quarentena se tiver valor informativo. Você também pode enviar a cópia de backup para o Centro de pesquisa de malware da Avira. Dependendo do arquivo, outras opções de seleção estão 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 realizada quando o Real-Time Protection localiza um vírus ou programa indesejado. Se a opção "**Reparar**" for selecionada mas o arquivo afetado não puder ser reparado, a ação selecionada em "**Ação secundária**" será realizada.

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

Reparar

Se essa opção for ativada, o Real-Time Protection repara os arquivos afetados automaticamente. Se o Real-Time Protection não puder reparar um arquivo afetado, ele realiza a ação selecionada em **Ação secundária**.

Nota
Um reparo automático é recomendado, mas significa que o Real-Time Protection modifica arquivos na estação de trabalho.

Renomear

Se essa opção for ativada, o Real-Time Protection renomeia o arquivo. Portanto, o acesso direto aos arquivos (por exemplo, com clique duplo) não será mais possível. Os arquivos podem ser reparados posteriormente e voltar a ter seus nomes originais.

Quarentena

Se essa opção for ativada, o Real-Time Protection move o arquivo para 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 é 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 Real-Time Protection substitui o arquivo por um padrão e o exclui. Não é possível restaurá-lo.

Negar acesso

Se essa opção for ativada, o Real-Time Protection insere a detecção no arquivo de relatório somente se a função de registro estiver ativada. Além disso, o Real-Time Protection grava uma entrada no Registro de eventos se essa opção for ativada.

Aviso
Se o Real-Time Protection estiver configurado para **Verificar durante a escrita**, o arquivo afetado não é gravado.

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 Real-Time Protection renomeia o arquivo. Portanto, o acesso direto aos arquivos (por exemplo, com clique duplo) não será mais possível. Os arquivos podem ser reparados posteriormente e voltar a ter seus nomes originais.

Quarentena

Se essa opção for ativada, o Real-Time Protection move o arquivo para 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 é 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 Real-Time Protection substitui o arquivo por um padrão e o exclui. Não é possível restaurá-lo.

Negar acesso

Se essa opção for ativada, o arquivo afetado não é gravado; o Real-Time Protection insere a detecção no arquivo de relatório somente se a função de registro estiver ativada. Além disso, o Real-Time Protection grava uma entrada no Registro de eventos se essa opção for ativada.

Nota
Se você tiver selecionado **Excluir** ou **Substituir e excluir** como ação primária ou secundária, observe: 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 é ativada, uma entrada é adicionada ao registro de eventos do Windows para cada detecção. Os eventos podem ser chamados no visualizador de eventos do Windows. Essa opção é ativada como a configuração padrão.

Exceções

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

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

Processos a serem omitidos pelo Real-Time Protection

Todos os acessos de processos dessa lista são excluídos do monitoramento pelo Real-Time 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 do processo especificados deverão 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, símbolos Unicode são aceitos. Portanto, você pode inserir o processo ou nomes de diretórios que contenham símbolos especiais.

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

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

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

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

Para evitar o processo de exclusão globalmente do monitoramento pelo Real-Time Protection, as especificações que compreendem exclusivamente os seguintes

caracteres são inválidas: * (asterisco), ? (ponto de interrogação), / (barra), \ (barra invertida), . (ponto), : (dois pontos).

Você tem a opção de excluir processos do monitoramento pelo Real-Time Protection sem detalhes completos do caminho. Por exemplo: `application.exe`

Porém, isso só se aplica a processos em que os arquivos executáveis estão localizados em unidades de disco rígido.

Detalhes completos do caminho em que os arquivos executáveis estão localizados em unidades conectadas, por exemplo, unidades de rede. Observe as informações gerais sobre a notação de Exceções em unidades de rede conectadas.

Não especifique quaisquer exceções para processos em que os arquivos executáveis estão localizados em unidades dinâmicas. Unidades dinâmicas são utilizadas para discos removíveis, como CDs, DVDs ou pen drives.

Aviso
Todos os acessos de arquivo feitos pelos processos registrados na lista são excluídos da varredura quanto a vírus e programas indesejados!

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 de arquivo a serem omitidos pelo Real-Time Protection

Todos os acessos a objetos dessa lista são excluídos do monitoramento pelo Real-Time Protection.

Caixa de entrada

Nessa caixa, é possível inserir o nome do objeto de arquivo que não é incluído na varredura 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 pode usar os curingas* (qualquer número de caracteres) e ? (um único caractere): Extensões de arquivo individuais também podem ser excluídas (inclusive curingas):

```
C:\Directory\*.mdb
*.mdb
*.md?
*.xls*
C:\Directory\*.log
```

Nomes de diretório devem terminar com uma barra invertida \ .

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

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

```
Por exemplo, C:\Arquivos de programas\Application\Nome.log
```

Podem existir no máximo 64 exceções sem um caminho completo. 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 do Real-Time 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 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\applic*.exe\`
Essa entrada não é válida e não é tratada como uma exceção!

Observe o seguinte com relação às **exceções em unidades de rede conectadas**: se você usar a letra da unidade de rede conectada, os arquivos e as pastas especificados NÃO são excluídos da varredura do Real-Time Protection. Se o caminho UNC na lista de exceções for diferente do caminho UNC usado para conectar 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 varredura do Real-Time Protection. Localize o caminho UNC relevante no arquivo de relatório do Real-Time Protection:
`\\<Nome do computador>\<Ativar>\` - OU - `\\<endereço IP>\<Ativar>\`

Você pode localizar o caminho que o Real-Time Protection utiliza para verificar os arquivos infectados no arquivo de relatório do Real-Time Protection. Indique exatamente o mesmo caminho na lista de exceções. Proceda da seguinte maneira: configure a função de protocolo do Real-Time Protection para **Completar** na configuração em Real-Time Protection > Relatório. Agora acesse os arquivos, as pastas, as unidades montadas ou as unidades de rede conectadas com o Real-Time Protection ativado. Agora você pode ler o caminho a ser usado no arquivo de relatório do Real-Time Protection. O arquivo de relatório pode ser acessado no Centro de controle em Proteção local > Real-Time Protection.

Se você estiver gerenciando o produto Avira em AMC, você pode usar variáveis nos detalhes do caminho para exceções de processo e de arquivo. Uma lista de variáveis que podem ser usadas pode encontrada em Variáveis: Real-Time Protection e Exceções da varredura.

Exemplos de processos a serem excluídos:

- `application.exe`
  O processo *application.exe* é excluído da varredura do Real-Time Protection, independentemente da unidade de disco rígido em que está localizado e em qual diretório se encontra.
- `C:\Program Files1\Application.exe`
  O processo do arquivo *application.exe*, que está localizado no caminho *C:\Program Files1* é excluído da varredura do Real-Time Protection.
- `C:\Program Files1\*.exe`
  Todos os processos dos arquivos executáveis localizados no caminho *C:\Program Files1* são excluídos da varredura do Real-Time Protection.

Exemplos de arquivos a serem excluídos:

- `*.mdb`
  Todos os arquivos com a extensão '*mdb*' são excluídos da varredura do Real-Time Protection.

- `*.xls*`
  Todos os arquivos com extensão de arquivo que começa com '*xls*' são excluídos da varredura do Real-Time Protection, por exemplo, arquivos com as extensões *.xls* e *.xlsx*.
- `C:\Directory\*.log`
  Todos os arquivos de registro com a extensão '*log*' localizados no caminho *C:\Directory* são excluídos da varredura do Real-Time Protection.
- `\\Computer name\Shared1\`
  Todos os arquivos são excluídos da varredura do Real-Time Protection acessada por uma conexão '*\\Computer name1\Shared1*'. Isso geralmente é uma unidade de rede conectada que acessa outro computador com uma pasta compartilhada através do nome do computador '*Computer name1*' e do nome compartilhado '*Shared1*'.
- `\\1.0.0.0\Shared1\*.mdb`
  Todos os arquivos com a extensão '*mdb*' são excluídos da varredura do Real-Time Protection acessada por uma conexão '*\\1.0.0.0\Shared1*'. Isso geralmente é uma unidade de rede conectada que acessa outro computador com uma pasta compartilhada através do endereço IP '1.0.0.0' e do nome compartilhado '*Shared1*'.

Heurística

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

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 seu produto Avira contém uma heurística de vírus de macros muito poderosa. Se essa opção for ativada, todas as macros no documento relevante serão excluídas em caso de reparo. Por outro lado, os arquivos suspeitos são apenas relatados, ou seja, você recebe um alerta. Essa opção é ativada como configuração padrão e é recomendada.

Detecção e análise heurística avançada (AheAD)

Ativar AHeAD

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

Nível de detecção baixo

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

Nível de detecção médio

Essa opção combina um nível de detecção forte com baixo risco de alertas falsos. Média será a configuração padrão se você tiver selecionado o uso dessa heurística.

Nível de detecção alto

Se esta opção for ativada, serão detectados significativamente mais malwares desconhecidos, mas há também a possibilidade de serem falso-positivos.

8.3.2 Relatório

O Real-Time 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, o Real-Time 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, o Real-Time 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 a configuração padrão.

Estendido

Se essa opção for ativada, o Real-Time Protection registrará informações menos importantes no arquivo de relatório também.

Concluído

Se essa opção for ativada, o Real-Time 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 para 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 relatório

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 relatório

Se essa opção for ativada, a configuração da varredura durante o acesso será registrada no arquivo de relatório.

Nota
Se você não especificou nenhuma restrição no arquivo de relatório, será criado automaticamente um novo arquivo de relatório quando o mesmo atingir 100MB. É criado um backup do antigo arquivo de relatório. São salvos até três backups dos antigos arquivos de relatório. Os backups mais antigos são excluídos primeiro.

8.4 Variáveis: Real-Time Protection e Exceções do Scanner

Se o seu produto Avira for gerenciado com AMC, você poderá utilizar as variáveis para configurar as exceções para o Real-Time Protection e o Scanner. Ao salvar a configuração no sistema gerenciado, as variáveis são automaticamente substituídas por valores verdadeiros correspondentes ao sistema operacional e sua linguagem.

As seguintes variáveis podem ser utilizadas:

8.4.1 Variáveis para Windows XP 32 Bits (**Inglês)

Variável	Windows XP 32 Bits (**Inglês)
`%WINDIR%`	*C:\Windows*
`%SYSDIR%`	*C:\Windows\System32*

%ALLUSERSPROFILE%	*C:\Documents and Settings\All Users* **
%PROGRAMFILES%	*C:\Arquivos de programas* **
%PROGRAMFILES(x86)%	*C:\Arquivos de programas (x86)* **
%SYSTEMROOT%	*C:\Windows*
%INSTALLDIR%	*C:\Arquivos de programas\Avira\Antivir Desktop* **
%AVAPPDATA%	*C:\Documents and Settings\All Users\Avira\AntiVir Desktop* **

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

8.4.2 Variáveis para Windows 7 32 Bits/ 64 Bits (**Inglês)

Variável	Windows 7 32-Bit (**Inglês)	Windows 7 64-Bit (**Inglês)
%WINDIR%	*C:\Windows*	*C:\Windows*
%SYSDIR%	*C:\Windows\System32*	*C:\Windows\System32*
%ALLUSERSPROFILE%	*C:\ProgramData*	*C:\ProgramData*
%PROGRAMFILES%	*C:\Arquivos de programas* **	*C:\Arquivos de programas* **
%PROGRAMFILES(x86)%	*C:\Arquivos de programas (x86)* **	*C:\Arquivos de programas (x86)* **
%SYSTEMROOT%	*C:\Windows*	*C:\Windows*

%INSTALLDIR%	*C:\Arquivos de programas\Avira\Antivir Desktop* **	*C:\Arquivos de programas (x86)\Avira\Antivir Desktop* **
%AVAPPDATA%	*C:\ProgramData\Avira\AntiVir Desktop*	*C:\ProgramData\Avira\AntiVir Desktop*

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

8.5 Atualização

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.

> **Nota**
> Se você configurar o produto no Avira Management Console, as atualizações automáticas não estão disponíveis.

Atualização automática

Ativar

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

Todos os n dia(s) / 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 à Internet (discada)

Se essa opção for ativada, além do intervalo de atualização especificado, o trabalho de atualização é realizado toda vez que uma conexão com a Internet for estabelecida.

Repetir o trabalho se o tempo já tiver expirado

ISe essa opção for ativada, serão realizados os trabalhos de atualização antigos que não foram realizados na hora especificada, por exemplo, porque o computador estava desligado.

> É possível acessar outras configurações de atualização através de um servidor da web em: Configuração > Proteção do PC > Atualizar > 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 arquivos / 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 de proprietário na Internet.

Nota
É possível acessar outras configurações de atualização através de um servidor de arquivos em: Configuração > Proteção do PC > Atualizar > Servidor de arquivos.
Se essa opção for ativada, você poderá configurar o servidor de arquivos que está usando.

8.5.1 Servidor de arquivos

Se houver mais de uma estação de trabalho em uma rede, o produto Avira pode baixar uma atualização de um servidor de arquivos na intranet que, por sua vez obtem os arquivos de atualização de um servidor de download patenteado na Internet. Isso garante que o produto Avira fique atualizado em todas as estações de trabalho.

Nota
O título Configuração pode ser ativado somente se em Configuração > Proteção do PC > Atualizar a opção **via Servidor de Aquivos / Pastas compartilhadas** foi 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/*" necessários. O seguinte deve ser especificado: `arquivo://<endereço IP do servidor de arquivos>/release/update/`. O diretório "release" deve ser um diretório que pode ser acessado por todos os usuários.

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

Logon do servidor

Nome de logon

Insira um nome de usuário para conectar no servidor. Use uma conta do usuário com direitos de acesso às pastas compartilhadas usadas no servidor.

Senha de logon

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

> **Nota**
> Se nenhum dado for especificado na seção de logon do servidor, nenhuma autenticação será realizada ao acessar o servidor de arquivos. Nesse caso, o usuário deve ter direitos suficientes para o servidor de arquivos.

8.5.2 Servidor da web

Servidor da web

A atualização pode ser realizada diretamente através de um servidor da web na Internet ou na intranet.

Conexão do servidor da web

Usar conexão já existente (rede)

Essa configuração é exibida quando a conexão é usada por meio de uma rede.

Usar a conexão a seguir

Essa configuração é exibida se você definir sua conexão 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.Uma conexão discada pode ser estabelecida manualmente, por exemplo, através de uma entrada do catálogo de telefones do Windows.

Usuário

Insira o nome de usuário da conta selecionada.

Senha

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

> **Nota**
> Caso tenha esquecido o nome de usuário ou a senha de uma conta da Internet existente, entre em contato com seu provedor de serviços de Internet.

Nota
A discagem automática do atualizador através das chamadas ferramentas de discagem (por exemplo, SmartSurfer, Oleco etc.) não está disponível no momento.

Encerrar uma conexão discada que foi configurada para a atualização

Se essa opção for ativada, a conexão discada feita para a atualização é interrompida automaticamente mais uma vez assim que o download tiver sido concluído com êxito.

Nota
Essa opção está disponível somente no Windows XP. Nos sistemas operacionais mais novos a conexão discada aberta para a atualização é sempre finalizada assim que o download for realizado.

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://<hostname or IP>[:port]/update`. Se você não especificar uma porta, será usada a porta 80.

Servidor padrão

Insira o URL e o diretório de atualização dos servidores da web dos quais as atualizações serão transferidas por download. Várias entradas são separadas por vírgulas. O formato do endereço é: `http://<hostname ou IP>[:port]/update`. Se você não especificar uma porta, será usada a porta 80. Por padrão, os servidores da web da Avira acessíveis são especificados para atualização. No entanto, você pode usar seus próprios servidores da web na intranet corporativa. Se vários servidores da Web forem especificados, separe cada um com 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 é estabelecida 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. Configure as definições do sistema Windows para usar um servidor proxy em **Painel de controle > Opções da internet > Conexões > Configurações da LAN**. Também é possível acessar as opções da Internet no menu **Extras** no Internet Explorer.

Aviso
Se estiver sendo usado um servidor proxy que precisa de autêntica, insira todos os dados solicitados na opção **Usar este servidor proxy**. A opção **Usar configurações do sistema proxy** pode ser usada somente para servidores proxy sem autenticação.

Usar este servidor proxy

Se a conexão com o servidor da web for configurada através de um servidor proxy, você pode inserir as informações relevantes aqui.

Endereço

Insira o URL ou o endereço IP do servidor proxy que deseja usar para conectar com o servidor da web.

Porta

Insira o número da porta do servidor proxy que deseja usar para conectar com o servidor da web.

Nome de logon

Insira um nome de usuário para conectar no servidor proxy.

Senha de logon

Insira a senha relevante para fazer login no servidor proxy aqui. Por motivos de segurança, os caracteres reais digitados neste espaço são substituídos por curinga (*).

Exemplos:

Endereço: `proxy.domain.com` Porta: `8080`

Endereço: `192.168.1.100` Porta: `3128`

8.6 FireWall

8.6.1 Configurar o FireWall

Avira Professional Security permite configurar o Avira FireWall ou gerenciar o Firewall do Windows:

- Avira FireWall

- Avira FireWall em AMC
- Firewall do Windows

8.6.2 Avira FireWall

A seção **FireWall** em **Configuração > Proteção na Internet** é responsável pela configuração do Avira FireWall (em sistemas operacionais até Windows 7).

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 computador para os quais um driver foi instalado.

- Protocolo ICMP
- Varredura da porta TCP
- Varredura da porta UDP
- Regras 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 na Internet > FireWall** no Centro de controle ou definir suas próprias regras do adaptador. Se tiver definido suas próprias regras do adaptador, o *Nível de segurança* na seção FireWall do Centro de controle é definido para **Personalizado**.

> **Nota**
> A configuração padrão do *Nível de segurança* de 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 de informações em redes. O protocolo também é usado para mensagens de status com ping ou rastreador.
Com essa regra é possível definir os tipos de mensagem de entrada e saída que devem ser bloqueados, o comportamento em caso de flooding e a reação a pacotes ICMP fragmentados. Essa regra serve para evitar os assim chamados 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 flooding se o atraso entre pacotes for menor do que 50 ms.Assumir flooding se o atraso entre pacotes for menor do que **50** ms. **Rejeitar** pacotes ICMP fragmentados.
Meio	Mesma regra do nível Baixo.
Alto	Tipos de entrada bloqueados: **vários tipos** Tipos de entrada bloqueados: **vários tipos** Assumir flooding se o atraso entre pacotes for menor do que 50 ms.Assumir flooding 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.

Assumir flooding

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 um clique do mouse você tem a opção entre **Rejeitar** e **Não rejeitar** pacotes ICMP de entrada.

Varredura da porta TCP

Com essa regra é possível definir quando uma varredura da porta TCP é presumida pelo FireWall e o que deve ser feito nesse caso. Essa regra serve para evitar os assim chamados ataques de varredura da porta TCP que resultam na detecção de portas TCP abertas no 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 varredura da porta TCP

Configuração	Regras
Baixo	Assume a varredura 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.
Meio	Assume a varredura 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 que o 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 varredura da porta TCP seja assumida.

Janela de horário de varredura de porta

Com o mouse, clique neste link para exibir uma caixa de diálogo na qual é possível inserir o intervalo de tempo para um determinado número de verificações de porta para que uma varredura da porta TCP seja assumida.

Banco de dados de eventos

Com um clique do mouse no link você tem a opção entre **registrar** e **não registrar** o endereço IP do invasor.

Regra

Com um clique do mouse no link você tem a opção entre **adicionar** e **não adicionar** a regra para bloquear o ataque de varredura de porta TCP.

Varredura da porta UDP

Com essa regra é possível definir quando uma varredura da porta UDP é suposta pelo FireWall e o que deve ser feito nesse caso. Essa regra evita os assim chamados ataques de varredura da porta UDP, que resultam na detecção de portas UDP abertas no 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 varredura da porta UDP

Configuração	Regras
Baixo	Assume a varredura 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.
Meio	Assume a varredura 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 que o 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 varredura da porta UDP seja assumida.

Janela de horário de varredura de porta

Com o mouse, clique neste link para exibir uma caixa de diálogo na qual é possível inserir o intervalo de tempo para um determinado número de verificações de porta para que uma varredura da porta UDP seja assumida.

Banco de dados de eventos

Com um clique do mouse no link você tem a opção entre **registrar** e **não registrar** o endereço IP do invasor.

Regra

Com um clique do mouse no link você tem a opção entre **adicionar** e **não adicionar** a regra para bloquear o ataque de varredura de porta UDP.

Regras de entrada

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

> **Aviso**
> Quando um pacote é filtrado, as regras correspondentes são aplicadas sucessivamente, por isso 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 entrada é bloqueado pelo Avira FireWall.
Meio	**Permitir conexões TCP estabelecidas em 135** **Permitir** pacotes TCP do endereço **0.0.0.0** com máscara **0.0.0.0** se porta local estiver em **{135}** e 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 **<vazios>** com máscara **<vazia>** no deslocamento **0**. **Negar pacotes TCP em 135** **Negar** pacotes TCP do endereço **0.0.0.0** com máscara **0.0.0.0** se porta local estiver em **{135}** e 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 **<vazios>** com máscara **<vazia>** no deslocamento **0**. **Monitor de tráfego saudável de TCP** **Permitir** pacotes TCP do endereço **0.0.0.0** com máscara **0.0.0.0** se a porta local estiver em **{0-65535}** e a porta remota em **{0-65535}**. Aplicar para **início da conexão e aos pacotes de conexão existentes**. **Não registrar** quando o pacote corresponder à regra. Avançado: selecionar pacotes que possuem os seguintes bytes **<vazios>** com máscara **<vazia>** no deslocamento **0**. **Descartar tráfego TCP** **Negar** pacotes TCP do endereço **0.0.0.0** com máscara **0.0.0.0** se a porta local estiver em **{0-65535}** e a porta remota em **{0-65535}**. Aplicar a **todos os pacotes**. **Não registrar** quando o pacote corresponder à regra. Avançado: selecionar pacotes que possuem os seguintes bytes **<vazios>** com máscara **<vazia>** no deslocamento **0**.
Alto	**Monitorar tráfego TCP restabelecido** **Permitir** pacotes TCP do endereço **0.0.0.0** com máscara **0.0.0.0** se a porta local estiver em **{0-65535}** e a porta remota em **{0-65535}**. Aplicar aos **pacotes de conexões existentes**. **Não registrar** quando o pacote corresponder à regra. Avançado: selecionar pacotes que possuem os seguintes bytes **<vazios>** com máscara **<vazia>** no deslocamento **0**.

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 no link com o mouse, uma caixa de diálogo é exibida na qual é possível inserir o endereço IPv4 ou IPv6 necessário.

Máscara IP

Ao clicar no link com o mouse, uma caixa de diálogo é exibida na qual é possível inserir a máscara IPv4 ou IPv6 necessária.

Portas locais

Com o mouse, clique neste link para exibir uma caixa de diálogo na qual é possível definir o(s) número(s) 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(s) número(s) 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 pacotes de conexão existentes**" ou somente a "**pacotes de conexões existentes**" ou a "**todos os pacotes**".

Banco de dados de eventos

Ao clicar no link com o mouse você pode escolher entre "**Registrar**" e "**não registrar**" no banco de dados de eventos se o pacote atender 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 de dados UDP

Configuração	Regras
Baixo	-
Meio	**Monitor de tráfego aceito de UDP** **Permitir** pacotes UDP do endereço **0.0.0.0** com máscara **0.0.0.0** se a porta local estiver em **{0- 66535}** e a porta remota 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 **<vazios>** com máscara **<vazia>** no deslocamento **0**. **Descartar tráfego UDP** **Negar** pacotes UDP do endereço **0.0.0.0** com máscara **0.0.0.0** se a porta local estiver em **{0-65535}** e a porta remota em **{0-65535}**. Aplicar regra a **todas as portas** para **todos os fluxos**. **Não registrar** quando o pacote corresponder à regra. Avançado: selecionar pacotes que possuem os seguintes bytes **<vazios>** com máscara **<vazia>** no deslocamento **0**.
Alto	**Monitorar tráfego TCP restabelecido** **Permitir** pacotes TCP do endereço 0.0.0.0 com máscara 0.0.0.0 se a porta local estiver em {0-65535} e a porta remota em {0-65535}. 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 **<vazios>** com máscara **<vazia>** no deslocamento **0**.

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 no link com o mouse, uma caixa de diálogo é exibida na qual é possível inserir o endereço IPv4 ou IPv6 necessário.

Máscara IP

Ao clicar no link com o mouse, uma caixa de diálogo é exibida na qual é possível inserir a máscara IPv4 ou IPv6 necessária.

Portas locais

Com o mouse, clique neste link para exibir uma caixa de diálogo na qual é possível definir o(s) número(s) 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(s) número(s) 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

Com o mouse, clique neste link para aplicar esta regra a todos os fluxos ou somente a fluxos de saída.

Banco de dados de eventos

Ao clicar no link com o mouse você pode escolher entre "**Registrar**" e "**não registrar**" no banco de dados de eventos se o pacote atender 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	-
Meio	**Não descarte ICMP baseado em endereço IP** **Permitir** pacotes ICMP do endereço **0.0.0.0** com máscara **0.0.0.0**. **Não registrar** quando o pacote corresponder à regra. Avançado: descartar pacotes que possuem os seguintes bytes **<vazios>** com máscara **<vazia>** no deslocamento **0**.
Alto	Mesma regra que o nível Médio.

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 no link com o mouse, uma caixa de diálogo é exibida na qual é possível inserir o endereço IPv4 necessário.

Máscara IP

Ao clicar no link com o mouse, uma caixa de diálogo é exibida na qual é possível inserir a máscara IPv4 necessária.

Banco de dados de eventos

Ao clicar no link com o mouse você pode escolher entre "**Registrar**" e "**não registrar**" no banco de dados de eventos se o pacote atender 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 pacotes IP

Configuração	Regras
Baixo	-
Meio	-
Alto	**Negar todos os pacotes IP** **Negar pacotes IPv4** do endereço **0.0.0.0** com 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 aceita ou rejeita pacotes IP com definição especial.

IPv4/IPv6

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

Endereço IP

Ao clicar no link com o mouse, uma caixa de diálogo é exibida na qual é possível inserir o endereço IPv4 ou IPv6 necessário.

Máscara IP

Ao clicar no link com o mouse, uma caixa de diálogo é exibida na qual é possível inserir a máscara IPv4 ou IPv6 necessária.

Banco de dados de eventos

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

Regras de saída

As regras de saída são definidas para controlar o tráfego de dados 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, por isso 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, ou seja, aumenta a prioridade da regra.
Regra abaixo	Move a regra selecionada uma linha para baixo, ou seja, diminui a prioridade da regra.
Renomear regra	Permite dar outro nome à regra selecionada.

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

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

Adicionar nova regra

Nessa janela, é possível selecionar novas regras de entrada e de saída. A regra selecionada é incluída com as informações padrão na janela **Regras do adaptador** e

pode ser definida em mais detalhes nesse local. Além das regras de entrada e de saída, existem mais regras disponíveis.

Regras possíveis

Permitir rede ponto a ponto

Permite conexões ponto a ponto: comunicações TCP de entrada na porta 4662 e comunicações UDP de entrada na porta 4672

Porta TCP

Com o mouse, clique no link para exibir uma caixa de diálogo na qual é possível inserir a porta TCP permitida.

Porta UDP

Com o mouse, clique no link para exibir uma caixa de diálogo na qual é possível inserir a porta UDP permitida.

Permitir conexões VMWARE

Permite comunicação entre sistemas VMWare

Bloquear IP

Bloqueia todo o tráfego de um endereço IP especificado

Versão do Internet Protocol

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

Endereço IP

Ao clicar no link com o mouse, uma caixa de diálogo é exibida na qual é possível inserir o endereço IP necessário.

Bloquear sub-rede

Bloqueia todo o tráfego de um endereço IP e uma máscara de sub-rede específicos

Versão do Internet Protocol

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

Endereço IP

Ao clicar no link com o mouse, uma caixa de diálogo é exibida na qual é possível inserir o endereço IP necessário.

Máscara de sub-rede

Ao clicar no link com o mouse, uma caixa de diálogo é exibida na qual é possível inserir a máscara de sub-rede necessária.

Permitir IP

Permite todo o tráfego de um endereço IP especificado

Versão do Internet Protocol

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

Endereço IP

Ao clicar no link com o mouse, uma caixa de diálogo é exibida na qual é possível inserir o endereço IP necessário.

Permitir sub-rede

Permite todo o tráfego de um endereço IP e uma máscara de sub-rede específicos

Versão do Internet Protocol

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

Endereço IP

Ao clicar no link com o mouse, uma caixa de diálogo é exibida na qual é possível inserir o endereço IP necessário.

Máscara de sub-rede

Ao clicar no link com o mouse, uma caixa de diálogo é exibida na qual é possível inserir a máscara de sub-rede necessária.

Permitir servidor da web

Permite comunicação de um servidor da web na porta 80: comunicação TCP de entrada na porta 80

Porta

Com o mouse, clique no link para exibir uma caixa de diálogo na qual é possível inserir a porta usada pelo servidor da web.

Permitir conexões VPN

Permite conexões VPN (Virtual Private Network) com um IP especificado: tráfego de dados UDP de entrada nas portas x, tráfego de dados TCP de entrada nas portas x, tráfego de dados IP de entrada com os protocolos ESP(50), GRE(47)

Versão do Internet Protocol

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

Endereço IP

Ao clicar no link com o mouse, uma caixa de diálogo é exibida na qual é possível inserir o endereço IP necessário.

Permitir conexão de Área de trabalho remota

Permite conexões de "Área de trabalho remota" (Protocolo de área de trabalho remota) na porta 3389

Porta

Com o mouse, clique no link para exibir uma caixa de diálogo na qual é possível inserir a porta a ser usada para a conexão de área de trabalho remota permitida.

Permitir conexão VNC

Permite conexões VNC (Virtual Network Computing, Computação de rede virtual) na porta 5900

Porta

Com o mouse, clique no link para exibir uma caixa de diálogo na qual é possível inserir a porta a ser usada para a conexão de área de trabalho remota permitida.

Permitir compartilhamento de arquivos e impressoras.

permite acesso a aprovações de arquivo e impressora: tráfego de dados TCP de entrada nas portas 137, 139 e tráfego de dados UDP de entrada na porta 445 de um endereço IP específico.

Possíveis regras de entrada

- **Regra IP de entrada**
- **Regras ICMP de entrada**
- **Regras UDP de entrada**
- **Regras TCP de entrada**
- **Regra de protocolo IP de entrada**

Possíveis regras de saída

- **Regra IP de saída**
- **Regras ICMP de saída**
- **Regras UDP de saída**
- **Regras TCP de saída**
- **Regra de protocolo IP de saída**

Nota
A sintaxe das possíveis regras de entrada e de saída é idêntica à das regras predefinidas dos protocolos relevantes, descritas em FireWall > Regras do adaptador.

Botões

Botão	Descrição
OK	A regra realçada é incluída como uma nova regra do adaptador.
Cancelar	A janela é fechada sem a adição de uma nova regra.

Regras de aplicativo

Regras de aplicativo para o usuário

Esta lista contém todos os usuários do sistema. Se estiver conectado como administrador, você pode selecionar o usuário ao qual deseja aplicar as regras. Se você não for usuário com privilégios, 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 da 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 pode criar as regras do aplicativo com base nos filtros de pacote da mesma maneira como criou as regras do adaptador.

- Acesse **Configuração > Proteção na Internet > FireWall > Configurações** e ative a opção **Configurações avançadas** em *Regras de aplicativo*.
- Salve a configuração clicando em **Aplicar** ou **OK**.
  - ↪ Na seção **Configuração > Proteção na Internet > FireWall > Regras de aplicativo** uma coluna adicional com o título **Filtragem** é exibida na lista de regras de aplicativo, com a entrada **Básica** de cada aplicativo.

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 da rede. Se você escolher **Básica** na coluna **Filtragem**, pode clicar no link para escolher outro tipo de ação. Os valores são **Perguntar**, **Permitir** ou **Negar**. Se você escolher **Avançada** na coluna **Filtragem**, o tipo de ação **Regras** é exibido. O link **Regras** abre a janela **Regras de aplicativo avançadas**, na qual é possível inserir regras específicas para o aplicativo.
Filtragem	Mostra o tipo de filtragem. Você pode selecionar outro tipo de filtragem clicando no link. **Básica**: no caso de filtragem simples, a ação especificada é executada em todas as atividades de rede realizadas pelo aplicativo de software. **Avançada**: com esse tipo de filtragem, as regras que foram adicionadas à configuração estendida são aplicadas.

- Para criar regras específicas para um aplicativo, selecione a entrada **Avançada** em **Filtragem**.
  - ↪ A entrada **Regras** é exibida na coluna **Ação**.
- Clique em **Regras** para abrir a janela e criar regras específicas para o aplicativo.

Regras de aplicativo especificadas na configuração avançada

Usando as regras de aplicativo especificadas, você pode permitir ou negar tráfego de dados especificados do 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 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 código com a fachada de outro programa. Desse modo, o acesso à Internet na frente do Avira 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 de aplicativo desejar para cada aplicativo. As regras de aplicativo são executadas na sequência mostrada (mais informações podem ser encontradas em Regras de aplicativo avançadas).

Nota
Se você alternar de filtragem **Avançada** para **Básica** de uma regra de aplicativo, as regras de aplicativo já existentes na configuração avançada são simplesmente desativadas, não excluídas de forma irrecuperável. Se selecionar filtragem **Avançada** novamente, as regras de aplicativos avançadas existentes serão reativadas e exibidas na janela de configuração **Regras de aplicativo**.

Detalhes do aplicativo

Nesta caixa é possível ver detalhes do aplicativo selecionado na caixa de lista 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. Ali é possível selecionar o aplicativo necessário para criar uma nova regra.
Remover regra	Remove a regra de aplicativo selecionada.
Mostrar detalhes	A janela "**Mostrar detalhes"** exibe os detalhes dos aplicativos selecionados na caixa de lista de aplicativos.
Recarregar	Recarrega a lista de aplicativos e, ao mesmo tempo, descarta as alterações que acabaram de ser feitas.

Regras de aplicativo avançadas

A janela **Regras de aplicativo avançadas** permite criar regras específicas para o tráfego de dados dos aplicativos e para escuta nas portas. Uma nova regra pode ser criada com o botão **Adicionar regra**. Além disso, é possível especificar melhor as regras na parte inferior da janela. Você pode criar quantas regras desejar para um aplicativo. As regras são executadas na ordem exibida. Os botões **Para cima** e **Para baixo** podem ser usados para alterar a sequência das regras.

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

Detalhes do aplicativo

As informações sobre o aplicativo selecionado são exibidas na área *Detalhes do aplicativo*.

- *Nome* - Nome do aplicativo.
- *Caminho* - Caminho até o arquivo executável do aplicativo.

Opções de regra

Negar/permitir injeção de código

Ao clicar no link com o mouse, você pode decidir se permitirá ou negará a injeção de código para o aplicativo selecionado.

Tipo de regra: tráfego/ escuta

Ao clicar no link com o mouse você pode decidir se deseja criar uma regra para monitorar o tráfego ou escutar em portas.

Negar/ permitir ação

Ao clicar no link com o mouse você pode decidir qual ação é executada com a regra.

Porta

Com o mouse, clique no link para exibir uma caixa de diálogo na qual é possível inserir a porta local à qual a regra de escuta se aplica. Também pode inserir várias portas ou áreas de portas.

Saída, entrada, todos os pacotes

Com o mouse, clique neste link para decidir se a regra de tráfego deverá monitorar somente pacotes de saída ou somente pacotes de entrada.

Pacotes IP/ pacotes TCP/ pacotes UDP

Ao clicar no link com o mouse você pode decidir qual protocolo monitora a regra de tráfego.

Opções de pacotes IP:

Endereço IP

Ao clicar no link com o mouse é exibida uma caixa de diálogo na qual pode ser inserido o endereço IP solicitado.

Máscara IP

Ao clicar no link com o mouse é exibida uma caixa de diálogo na qual pode ser inserida a máscara IP solicitada.

Pacotes TCP / Opções de pacotes UDP:

Endereço IP local

Ao clicar no link com o mouse é exibida uma caixa de diálogo na qual é possível inserir o endereço IP local.

Máscara IP local

Ao clicar no link com o mouse é exibida uma caixa de diálogo na qual pode ser inserida a máscara IP local solicitada.

Endereço IP remoto

Ao clicar no link com o mouse é exibida uma caixa de diálogo na qual pode ser inserido o endereço IP remoto solicitado.

Máscara IP remota

Ao clicar no link com o mouse é exibida uma caixa de diálogo na qual pode ser inserida a máscara IP remota solicitada.

Porta local

Com o mouse, clique no link para exibir uma caixa de diálogo na qual é possível definir as portas locais ou até mesmo intervalos de porta completos.

Porta remota

Com o mouse, clique no link para exibir uma caixa de diálogo na qual é possível definir uma ou mais portas remotas solicitadas ou até mesmo intervalos de porta completos.

Arquivo de relatório

Ao clicar no link com o mouse você tem a opção "**acessar**" e "**não acessar**" o arquivo de relatório do programa quando uma regra for atendida.

Botões

Botão	Descrição
Adicionar regra	Uma nova regra de aplicativo é criada.
Remover regra	A regra de aplicativo selecionada é excluída.
Regra acima	A regra selecionada é movida uma linha para cima, ou seja, a prioridade da regra é aumentada.
Regra abaixo	A regra de aplicativo selecionada é movida uma linha para baixo, ou seja, a prioridade da regra é diminuída.
Renomear regra	A regra selecionada é editada, de modo que é possível inserir um novo nome de regra.
Aplicar	As alterações feitas são aceitas e aplicadas imediatamente pelo Avira FireWall.

OK	As alterações feitas são aplicadas. A janela para configurar as regras de aplicativo é fechada.
Cancelar	A janela para configurar as regras de aplicativo é fechada sem aplicar as alterações feitas.

Fornecedores confiáveis

Uma lista de fabricantes de software confiáveis é exibida em **Fornecedores confiáveis**.

Você pode adicionar ou remover fabricantes da lista usando a opção **Sempre confiar neste fornecedor** na janela pop-up **Evento de rede**. Para permitir o acesso à rede dos aplicativos que são assinados pelos fornecedores listados por padrão, ative a opção **Permitir automaticamente aplicativos criados pelos fornecedores confiáveis**.

Fornecedores confiáveis para usuário

Esta lista contém todos os usuários do sistema. Se você estiver conectado como administrador, poderá selecionar o usuário cuja lista de fornecedores confiáveis deseja visualizar ou atualizar. Se você não for usuário com privilégios, poderá ver somente o usuário conectado no momento.

Permitir automaticamente aplicativos 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.

Nota
Se você remover fornecedores da lista e, em seguida, selecionar **Aplicar** os

fornecedores serão removidos permanentemente da lista. A alteração não pode ser desfeita com a opção **Recarregar**. No entanto, você pode usar a opção **Sempre confiar neste fornecedor** na janela pop-up **Evento de rede** para adicionar um fornecedor à lista de fornecedores confiáveis novamente.

Nota
O Avira FireWall prioriza as regras do aplicativo antes de fazer entradas na lista de fornecedores confiáveis: se você criou uma regra de aplicativo e o provedor de aplicativo estiver indicado na lista de fornecedores confiáveis, a regra do aplicativo será executada.

Configurações

Opções avançadas

Ligar FireWall

Se essa opção for ativada, o Avira Firewall é ativado e protege o computador dos riscos da Internet e de outras redes.

Interromper o Windows Firewall na inicialização

Se essa opção for ativada, o Windows Firewall é desativado quando o computador for reiniciado. Essa opção é ativada como a configuração padrão.

Tempo limite de regra automática

Bloquear para sempre

Se essa opção for ativada, uma regra que foi criada automaticamente, por exemplo, durante uma verificação de porta é retida.

Remover após n segundos

Se essa opção for ativada, uma regra que foi criada automaticamente, por exemplo, durante uma verificação de porta é removida novamente após o tempo definido. Essa opção é ativada como a configuração padrão. Na caixa você pode especificar o número de segundos após o que as regras devem ser removidas.

Notificações

As notificações definem os eventos nos quais deseja receber uma notificação de área de trabalho do Avira FireWall.

Verificação de porta

Se a opção for ativada, você recebe uma notificação de área de trabalho quando uma verificação de porta for detectada pelo Avira FireWall.

Inundação

Se a opção for ativada, você recebe uma notificação de área de trabalho quando um ataque de flooding for detectado pelo Avira FireWall.

Aplicativos bloqueados

Se a opção for ativada, você recebe uma notificação de área de trabalho se o Avira FireWall negar, ou seja, bloquear a atividade de rede de um aplicativo.

IP bloqueado

Se a opção for ativada, você recebe uma notificação de área de trabalho se o Avira Firewall negar, ou seja, 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 pode 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.

Configurações de pop-up

Inspecionar pilha de inicialização de processo

Se essa opção for ativada, a inspeção da pilha de processo permite um controle mais preciso. O FireWall presume que qualquer dos processos não confiáveis na pilha pode ser realmente o que acessa a rede através do seu processo filho. Assim, uma janela diferente e será aberta em cada processo não confiável na pilha de processo. Essa opção é desativada como a configuração padrão.

Permitir vários pop-ups por processo

Se essa opção for ativada, um pop-up será acionado toda vez que um aplicativo estabelecer conexão de rede. Se preferir, você pode ser notificado somente na primeira tentativa de conexão. Essa opção é desativada como a configuração padrão.

Lembrar ação para este aplicativo

Sempre ativado

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

Sempre desativado

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

Ativado para aplicativos assinados

Quando essa opção é ativada, a opção **Lembrar ação para este aplicativo** da caixa de diálogo **Evento de rede** é ativada automaticamente durante o acesso à rede pelos aplicativos assinados. os aplicativos assinados são distribuídos pelos assim chamados "fornecedores confiáveis" (consulte Fornecedores confiáveis).

Lembrar último estado usado

Quando essa opção é ativada, a opção "**Lembrar ação para este aplicativo**" da caixa de diálogo "**Evento de rede**" é ativada da mesma maneira que 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, ou seja, 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 é administrada da mesma maneira que 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.

8.6.3 Avira FireWall em AMC

O FireWall é configurado para atender os requisitos específicos de uma administração através do Avira Security Management Center. Existem opções e restrições estendidas para opções de configuração individuais:

- As configurações do FireWall aplicam-se a todos os usuários do computador cliente
- Regras do adaptador: os níveis de segurança para adaptadores individuais podem ser definidos usando menus contextuais
- Regras do 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 no Centro de controle são desativadas nos computadores cliente:

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

Configurações gerais

Opções avançadas

Ativar Firewall

Se essa opção for ativada, o Avira Firewall é ativado e protege o 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 a configuração padrão.

Modo de aprendizado

Se a opção for ativada, o modo de aprendizado do Avira FireWall é ativado.

Tempo limite de regra automática

Bloquear para sempre

Se essa opção for ativada, uma regra que foi criada automaticamente, por exemplo, durante uma verificação de porta é retida.

Remover após n segundos

Se essa opção for ativada, uma regra que foi criada automaticamente, por exemplo, durante uma verificação de porta é removida novamente após o tempo definido. Essa opção é ativada como a configuração padrão.

Regras genéricas do adaptador

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 contextual do adaptador (na janela **Regras genéricas do adaptador** clique com o botão direito em **Meu computador** ou **Padrão, Sem fio, Discada** etc.) o você pode especificar regras de 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.

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

- Protocolo ICMP
- Varredura da porta TCP
- Varredura 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 de informações em redes. O protocolo também é usado para mensagens de status com ping ou rastreador.
Com essa regra é possível definir os tipos de mensagem de entrada e saída que devem ser bloqueados, o comportamento em caso de flooding e a reação a pacotes ICMP fragmentados. Essa regra serve para evitar os assim chamados 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 flooding se o atraso entre pacotes for menor do que 50 ms.Assumir flooding se o atraso entre pacotes for menor do que **50** ms. **Rejeitar** pacotes ICMP fragmentados.
Meio	Mesma regra do nível Baixo.
Alto	Tipos de entrada bloqueados: **vários tipos** Tipos de entrada bloqueados: **vários tipos** Assumir flooding se o atraso entre pacotes for menor do que 50 ms.Assumir flooding 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 ICMPA.

Pacotes ICMP fragmentados

Com o mouse, clique no link para rejeitar ou não pacotes ICMP fragmentados.

Varredura da porta TCP

Com essa regra é possível definir quando uma varredura da porta TCP é presumida pelo FireWall e o que deve ser feito nesse caso. Essa regra serve para evitar os assim chamados ataques de varredura da porta TCP que resultam na detecção de portas TCP

abertas no 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 varredura da porta TCP

Configuração	Regras
Baixo	Assume a varredura 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.
Meio	Assume a varredura 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 que o 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 varredura da porta TCP seja assumida.

Janela de horário de varredura de porta

Com o mouse, clique neste link para exibir uma caixa de diálogo na qual é possível inserir o intervalo de tempo para um determinado número de verificações de porta para que uma varredura 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 varredura da porta TCP.

Varredura da porta UDP

Com essa regra é possível definir quando uma varredura da porta UDP é suposta pelo FireWall e o que deve ser feito nesse caso. Essa regra evita os assim chamados ataques de varredura da porta UDP, que resultam na detecção de portas UDP abertas no 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 varredura da porta UDP

Configuração	Regras
Baixo	Assume a varredura 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.
Meio	Assume a varredura 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 que o 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 varredura da porta UDP seja assumida.

Janela de horário de varredura de porta

Com o mouse, clique neste link para exibir uma caixa de diálogo na qual é possível inserir o intervalo de tempo para um determinado número de varreduras de porta para que uma varredura 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 varredura da porta UDP.

Regras de entrada

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

Aviso
Quando um pacote é filtrado, as regras correspondentes são aplicadas

sucessivamente, por isso 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 entrada é bloqueado pelo Avira FireWall.

Meio	• Permitir conexões TCP estabelecidas em 135 **Permitir** pacotes TCP do endereço **0.0.0.0** com máscara **0.0.0.0** se porta local estiver em **{135}** e porta remota estiver em **{0-65535}**. Aplicar aos **pacotes de conexões existentes**. **Não registrar** quando o pacote corresponder à regra. Avançado: descartar pacotes que tenham os seguintes bytes **<vazios>** com máscara **<vazia>** no deslocamento **0** • Negar pacotes TCP em 135 **Negar** pacotes TCP do endereço **0.0.0.0** com máscara **0.0.0.0** se portas locais estiverem em **{135}** e 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 **<vazios>** com máscara **<vazia>** no deslocamento **0**. • Monitor de tráfego saudável de TCP **Permitir** pacotes TCP do endereço **0.0.0.0** com máscara **0.0.0.0** se a porta local estiver em **{0-65535}** e a porta remota em **{0-65535}**. Aplicar para **início da conexão e aos pacotes de conexão existentes**. **Não registrar** quando o pacote corresponder à regra. Avançado: selecionar pacotes que possuem os seguintes bytes **<vazios>** com máscara **<vazia>** no deslocamento **0**. • Descartar tráfego TCP **Negar** pacotes TCP do endereço **0.0.0.0** com 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 pacotes que possuem os seguintes bytes **<vazios>** com máscara **<vazia>** no deslocamento **0**.

Alto	Monitorar tráfego TCP estabelecido **Permitir** pacotes TCP do endereço **0.0.0.0** com máscara **0.0.0.0** se a porta local estiver em **{0-65535}** e a porta remota em **{0-65535}**. Aplicar aos **pacotes de conexões existentes**. **Não registrar** quando o pacote corresponder à regra. Avançado: selecionar pacotes que possuem os seguintes bytes **<vazios>** com máscara **<vazia>** 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 no link com o mouse, uma caixa de diálogo é exibida na qual é possível inserir o endereço IPv4 ou IPv6 necessário.

Máscara IP

Ao clicar no link com o mouse, uma caixa de diálogo é exibida na qual é possível inserir a máscara IPv4 ou IPv6 necessária.

Portas locais

Com o mouse, clique neste link para exibir uma caixa de diálogo na qual é possível definir o(s) número(s) 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(s) número(s) 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 se o pacote estiver 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 de dados de tráfego de UDP

Configuração	Regras
Baixo	-
Meio	• Monitor de tráfego UDP aceito **Permitir** pacotes UDP do endereço **0.0.0.0** com 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 **<vazios>** com máscara **<vazia>** no deslocamento **0**. • Descartar tráfego UDP **Negar** pacotes UDP do endereço **0.0.0.0** com 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 pacotes que possuem os seguintes bytes **<vazios>** com máscara **<vazia>** no deslocamento **0**.

Alto	Monitorar tráfego UDP estabelecido **Permitir** pacotes UDP do endereço **0.0.0.0** com 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**. **Não registrar** quando o pacote corresponder à regra. Avançado: descartar pacotes que possuem os seguintes bytes **<vazios>** com máscara **<vazia>** no deslocamento **0**.

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 no link com o mouse, uma caixa de diálogo é exibida na qual é possível inserir o endereço IPv4 ou IPv6 necessário.

Máscara IP

Ao clicar no link com o mouse, uma caixa de diálogo é exibida na qual é possível inserir a máscara IPv4 ou IPv6 necessária.

Portas locais

Com o mouse, clique neste link para exibir uma caixa de diálogo na qual é possível definir o(s) número(s) 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(s) número(s) 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 se o pacote estiver 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 de dados de tráfego de ICMP

Configuração	Regras
Baixo	-
Meio	Não descartar ICMP baseado no endereço IP **Permitir** pacotes ICMP do endereço **0.0.0.0** com máscara **0.0.0.0**. **Não registrar** quando o pacote corresponder à regra. Avançado: descartar pacotes que possuem os seguintes bytes **<vazios>** com máscara **<vazia>** no deslocamento **0**.
Alto	Mesma regra que o nível Médio.

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 no link com o mouse, uma caixa de diálogo é exibida na qual é possível inserir o endereço IPv4 ou IPv6 necessário.

Máscara IP

Ao clicar no link com o mouse, uma caixa de diálogo é exibida na qual é possível inserir a máscara IPv4 ou IPv6 necessária.

Arquivo de relatório

Ao clicar no link com o mouse, você pode decidir se gravará ou não um arquivo de relatório se o pacote estiver 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 pacotes IP

Configuração	Regras
Baixo	-
Meio	-
Alto	Negar todos os pacotes IP **Negar** pacotes **IP** do endereço **0.0.0.0** com 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 aceita ou rejeita pacotes IP com definição especial.

Endereço IP

Ao clicar no link com o mouse, uma caixa de diálogo é exibida na qual é possível inserir o endereço IPv4 ou IPv6 necessário.

Máscara IP

Ao clicar no link com o mouse, uma caixa de diálogo é exibida na qual é possível inserir a máscara IPv4 ou IPv6 necessária.

Arquivo de relatório

Ao clicar no link com o mouse, você pode decidir se gravará ou não um arquivo de relatório se o pacote estiver em conformidade com a regra.

Regra de protocolo IP de entrada

Pacotes IP

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

Endereço IP

Ao clicar no link com o mouse, uma caixa de diálogo é exibida na qual é possível inserir o endereço IPv4 ou IPv6 necessário.

Máscara IP

Ao clicar no link com o mouse, uma caixa de diálogo é exibida na qual é possível inserir a máscara IPv4 ou IPv6 necessária.

Protocolo

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

Arquivo de relatório

Ao clicar no link com o mouse, você pode decidir se gravará ou não um arquivo de relatório se o pacote estiver em conformidade com a regra.

Regras de saída

As regras de saída são definidas para controlar o tráfego de dados de saída do Avira FireWall. Você pode definir uma regra de saída para um dos seguintes protocolos: IP, ICMP, UDP e TCP. Consulte Adicionar nova regra.

Aviso
Quando um pacote é filtrado, as regras correspondentes são aplicadas sucessivamente, por isso 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, ou seja, aumenta a prioridade da regra.
Regra abaixo	Move a regra selecionada uma linha para baixo, ou seja, diminui a prioridade da regra.
Renomear regra	Permite dar outro nome à regra selecionada.

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

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

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 contextual:

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

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 contextual.

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 for usada a opção "**Adicionar por caminho**" o aplicativo FireWall adicionado é identificado pelo caminho e nome de arquivo.
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 for usada a opção "**Adicionar por md5**" todos os aplicativos adicionados são identificados exclusivamente com a soma de verificação MD5. Isso permite ao FireWall identificar 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.

Fornecedores confiáveis

Uma lista de fabricantes de software confiáveis é exibida em **Fornecedores confiáveis**. Os aplicativos dos fabricantes de software indicados 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.

Nota
Se você remover fornecedores da lista e, em seguida, selecionar **Aplicar** os fornecedores serão removidos permanentemente da lista. A alteração não pode ser desfeita com a opção **Recarregar**.

Nota
O FireWall prioriza as regras do aplicativo antes de fazer entradas na lista de fornecedores confiáveis: se você criou uma regra de aplicativo e o provedor de aplicativo estiver indicado na lista de fornecedores confiáveis, a regra do aplicativo será executada.

Outras configurações

Notificações

As notificações definem os eventos nos quais deseja receber uma notificação de área de trabalho do FireWall.

Verificação de porta

Se a opção for ativada, você recebe uma notificação de área de trabalho quando uma verificação de porta for detectada pelo FireWall.

Inundação

Se a opção for ativada, você recebe uma notificação de área de trabalho quando um ataque de flooding for detectado pelo FireWall.

Aplicativos bloqueados

Se a opção for ativada, você recebe uma notificação de área de trabalho se o FireWall negar, ou seja, bloquear a atividade de rede de um aplicativo.

IP bloqueado

Se a opção for ativada, você recebe uma notificação de área de trabalho se o Firewall negar, ou seja, bloquear o tráfego de dados de um endereço IP.

Configurações de pop-up

Inspecionar pilha de inicialização de processo

Se essa opção for ativada, a inspeção da pilha de processo permitirá um controle mais preciso.O FireWall presume que qualquer dos processos não confiáveis da pilha pode ser o que realmente acessa a rede através do 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 a configuração padrão.

Permitir vários pop-ups por processo

Se essa opção for ativada, um pop-up será acionado toda vez que um aplicativo estabelecer conexão de rede. Se preferir, você pode ser notificado somente na primeira tentativa de conexão. Essa opção é desativada como a configuração padrão.

Configurações de exibição

Lembrar ação para este aplicativo

Sempre ativado

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

Sempre desativado

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

Ativado para aplicativos assinados

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

Lembrar último estado usado

Quando esta opção tiver sido ativada, a opção "**Lembrar ação para este aplicativo**" na caixa de diálogo "**Evento de rede**" é ativada da mesma forma que 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, ou seja, 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 é administrada da mesma maneira que 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.

8.6.4 Firewall do Windows

A seção **FireWall** em **Configuração > Proteção na Internet** é responsável pela configuração do Firewall do Windows, a partir do Windows 7.

Firewall do Windows

Ativar o Firewall do Windows gerenciado pelo Avira

Se esta opção estiver ativada, o Avira irá gerenciar o Firewall do Windows.

Perfis de rede

Perfis de rede

O Firewall do Windows bloqueia o acesso não autorizado a programas e aplicativos do seu computador com base em três perfis de localização de rede:

- Rede privada: para redes domésticas ou de escritório
- Rede pública: para redes de locais públicos
- Rede de domínio: para redes com um controlador de domínio

Você pode gerenciar esses perfis a partir da configuração do seu produto Avira em **Proteção na Internet > Firewall do Windows > Perfis de rede**.

Para obter mais informações sobre esses perfis de rede, visite o site oficial da Microsoft.

Atenção
O Firewall do Windows aplica as mesmas regras a todas as rede que pertencem ao mesmo local de rede, ou seja, se você permitir que um programa ou aplicativo seja executado, também será concedido acesso a esse programa ou aplicativo também em todas as redes que têm o mesmo perfil.

Rede privada

Configurações de rede privada

As configurações de rede privada gerenciam o acesso que outros computadores ou dispositivos na sua rede doméstica ou do escritório têm ao seu computador. Como padrão, essas configurações permitem que os usuários da rede privada vejam o seu computador e tenham acesso a ele.

Ativar

Se essa opção estiver ativada, o Firewall do Windows está ativado e em funcionamento através do produto Avira.

Bloquear todas as conexões de entrada

Se esta opção estiver ativada, o Firewall do Windows rejeitará todas as tentativas não solicitadas de conexão ao seu computador, inclusive conexões de entrada de aplicativos permitidos.

Notifique-me quando um novo aplicativo for bloqueado

Se esta opção estiver ativada, você receberá uma notificação sempre que o Firewall do Windows bloquear um novo programa ou aplicativo.

Desativar (não recomendada)

Se esta opção estiver ativada, o Firewall do Windows estará desativado. Essa opção não é recomendada, porque expõe o seu computador a riscos.

Rede pública

Configurações de rede pública

As configurações de rede pública gerenciam o acesso que outros computadores ou dispositivos em redes de locais públicos têm ao seu computador. Como padrão, essas configurações não permitem que os usuários da rede pública vejam o seu computador ou tenham acesso a ele.

Ativar

Se essa opção estiver ativada, o Firewall do Windows está ativado e funcionamento através do produto Avira.

Bloquear todas as conexões de entrada

Se esta opção estiver ativada, o Firewall do Windows rejeitará todas as tentativas não solicitadas de conexão ao seu computador, inclusive conexões de entrada de aplicativos permitidos.

Notifique-me quando um novo aplicativo for bloqueado

Se esta opção estiver ativada, você receberá uma notificação todas as vezes que o Firewall do Windows bloquear um novo programa ou aplicativo.

Desativar (não recomendada)

Se esta opção estiver ativada, o Firewall do Windows estará desativado. Essa opção não é recomendada porque expõe o seu computador a riscos.

Rede de domínio

Configurações de rede de domínio

As configurações de rede de domínio gerenciam o acesso que outros computadores ou dispositivos têm ao seu computador em uma rede que é autenticada através de um controlador de domínio. Como padrão, essas configurações permitem que usuários autenticados do domínio vejam e acessem o seu computador.

Ativar

Se essa opção estiver ativada, o Firewall do Windows está ativado e em funcionamento através do produto Avira.

Bloquear todas as conexões de entrada

Se esta opção estiver ativada, o Firewall do Windows rejeitará todas as tentativas não solicitadas de conexão ao seu computador, inclusive conexões de entrada de aplicativos permitidos.

Notifique-me quando um novo aplicativo for bloqueado

Se esta opção estiver ativada, você receberá uma notificação todas as vezes que o Firewall do Windows bloquear um novo programa ou aplicativo.

Desativar (não recomendada)

Se esta opção estiver ativada, o Firewall do Windows estará desativado. Essa opção não é recomendada porque expõe o seu computador a riscos.

Nota
Esta opção apenas está disponível se o seu computador estiver conectado a uma rede com um controlador de domínio.

Regras de aplicativo

Se você clicar no link sob **Firewall do Windows > Regras de aplicativo**, você será redirecionado ao menu **Aplicativos e recursos permitidos** da configuração do Firewall do Windows.

Configurações avançadas

Se você clicar no link sob **Firewall do Windows > Configurações avançadas**, você será redirecionado ao menu **Firewall do Windows com Segurança Avançada** da configuração do Firewall do Windows.

8.7 Web Protection

A seção **Proteção para a Web** em **Configuração > Proteção para a internet** é responsável pela configuração da Proteção para a Web.

8.7.1 Varredura

A Proteção para a Web protege você contra vírus ou malwares que atingem seu computador a partir de páginas da Web carregadas em seu navegador a partir da Internet. A opção **Verificar** pode ser usada para definir o comportamento do componente da Proteção para a Web.

Varredura

Ativar Proteção para a Web

Se essa opção for ativada, o recurso Proteção para a Web estará ativo.

Ativar suporte para IPv6

Se essa opção for ativada, a versão 6 do Internet Protocol será suportada pela Web Protection. Esta opção não está disponível para novas instalações ou instalações alteradas em Windows 8.

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.

Resolução de na detecções

Você pode definir as ações a serem realizadas pela Proteção para a Web quando um vírus ou programa indesejado for detectado.

Interativo

Se essa opção for ativada, uma caixa de diálogo aparecerá quando um vírus ou programa indesejado for detectado durante uma verificação sob demanda, na qual você poderá especificar o que deve ser feito com o arquivo afetado. Essa opção é ativada como a 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.Esta notificação foi criada especialmente para fazer download de sites com volumes maiores de dados: se estiver navegando com a Proteção para a Web, 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 a configuração padrão.

Ações permitidas

Nesta caixa podem ser especificadas ações, que 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 o navegador. Uma mensagem de erro para notificar que o acesso foi negado é exibida no navegador. A Proteção para a Web registrará a detecção no arquivo de relatório se a função de registro estiver ativada.

Mover para quarentena

No caso um vírus ou malware ser detectado, o site solicitado do servidor da web e/ou os dados e 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 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 esta opção for ativada, não aparecerá nenhuma caixa de diálogo em caso de vírus. A Proteção para a Web reage de acordo com as configurações pré-definidas nesta seção como ação primária e 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 realizada quando a Proteção para a Web encontra um vírus ou programa indesejado.

Negar acesso

O site solicitado do servidor da Web e/ou todos os dados ou arquivos transferidos não são enviados para seu navegador. Uma mensagem de erro para notificar que o acesso foi negado é exibida no navegador. A Proteção para a Web registrará a detecção no arquivo de relatório se a função de registro estiver ativada.

Mover para quarentena

Caso um vírus ou malware seja detectado, o site solicitado do servidor 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 Web e/ou os dados e arquivos que foram transferidos são encaminhados pela Proteção para a Web 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

Em **Solicitações bloqueadas** é possível especificar os tipos de arquivo e os tipos MIME (tipos de conteúdo para os dados transferidos) a serem bloqueados pela Proteção para a Web. O filtro da Web permite bloquear URLs conhecidos de phishing e malware.A Proteção para a Web impede a transferência de dados da Internet para seu computador. pecialista.

A Proteção para a Web bloqueia os seguintes tipos de arquivos / Os tipos MIME

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

Caixa de entrada

Nessa caixa, insira os nomes dos tipos MIME e dos tipos de arquivo que devem ser bloqueados pela Proteção para a Web. 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**.

Nota
No entanto, os arquivos que já estão armazenados em seu computador 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.

Nota
A lista de tipos de arquivo e MIME bloqueados será ignorada se os tipos forem inseridos na lista de tipos de arquivo e MIME excluídos em Proteção para a Web > Verificar > Exceções.

Nota
Nenhum caractere curinga (* para qualquer número de caracteres ou ?para um único caractere) pode ser usado ao inserir os tipos de arquivo e os tipos MIME.

Tipos MIME: exemplos para tipos de mídia:

- `text` = para arquivos de texto
- `image` = para arquivos gráficos
- `video` = para arquivos de vídeo
- `audio` = para arquivos de som
- `application` = para arquivos vinculados a um programa específico

Exemplos de tipos de arquivo e MIME excluídos

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

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 Proteção para a Web.

Nota
O filtro da Web é ignorado para as entradas na lista de URLs excluídos em Proteção para a Web > Verificar > Exceções.

Nota
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 Proteção para a Web. Os tipos MIME e os URLs especificados são ignorados pela Proteção para a Web, isto é, os dados não são verificados em busca de vírus e malwares quando são transferidos para seu computador.

Tipos MIME ignorados pela Proteção para a Web

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

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

Todos os tipos MIME (tipos de conteúdo para os dados transferidos) na lista são ignorados pela Proteção para a Web 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 Proteção para a Web 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**.

Nota
Nenhum caractere curinga (* para qualquer número de caracteres ou ?para um único caractere) pode ser usado ao inserir os tipos de arquivo e os tipos MIME.

Aviso
É feito o download de todos os tipos de arquivo e tipos de conteúdo na lista de exclusão no navegador da Internet sem nenhuma verificação das solicitações bloqueadas (Lista de tipos de arquivos e MIME a serem bloqueados na Proteção para a Web > Verificar > Solicitações bloqueadas) ou pela Proteção para a Web: Para todas as entradas na lista de exclusão, as entradas na lista de arquivo e tipos MIME a serem bloqueados são ignorados. Nenhuma verificação quanto a vírus e malwares 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 tipos de arquivo e MIME excluídos:

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

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 ignoradas pela Proteção da Web

Todos os URLs dessa lista são excluídos das verificações da Proteção para a Web.

Caixa de entrada

Nessa caixa, é possível inserir os URLs (endereços da Internet) a serem excluídos das verificações da Proteção para a Web, por exemplo, `www.domainname.com`. Você pode especificar as partes do URL, usando pontos principais ou seguir para indicar o nível de domínio: `.domainname.com` para todas as páginas e todos os subdomínios do domínio. Indique os sites com domínio de nível superior (`.com` ou `.net`) com um ponto a seguir: `domainname.`Se você indicar uma string sem um ponto no início ou no final, a string será interpretada como um domínio de nível superior, como `net`, para todos os domínios NET (`www.domain.net`).

Nota
Você também pode usar o caractere curinga * para qualquer número de caracteres ao especificar os URLs. Você também pode usar pontos principais ou a seguir em combinação com curingas para indicar o nível de domínio:
`.domainname.*`
`*.domainname.com`
`.*name*.com` (válido mas não recomendado)
Especificações sem pontos, como *`name`*, são interpretadas como parte de um domínio de nível superior e não são recomendadas.

Aviso
É feito o download de todos os sites na lista de URLs excluídos no navegador da Internet sem nenhuma verificação pelo filtro da Web ou pela Proteção para a Web: Para todas as entradas na lista de URLs excluídos, as entradas no filtro de web (consultar Proteção para a Web > Verificar > Solicitações bloqueadas) são ignoradas. Nenhuma verificação quanto a vírus e malwares é realizada. Desse modo, somente URLs confiáveis devem ser excluídos das verificações da Proteção para a Web.

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 Proteção para a Web: *www.avira.com/en/pages/index.php*, *www.avira.com/en/support/index.html*, *www.avira.com/en/download/index.html*, etc.

Os URLs com o domínio `www.avira.de` não são excluídos das verificações da Proteção para a Web.

- `avira.com` -OU- `*.avira.com`
  = Todos os URLs com o domínio de segundo nível e de nível superior `avira.com` são excluídos das verificações da Proteção para a Web: 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 Proteção para a Web: A especificação implica todos os domínios de nível superior ou subdomínios para `.avira`: *www.avira.com*, *www.avira.de*, *forum.avira.com*, etc.
- `.*domain*.*`
  Todos os URLs contendo um domínio de segundo nível com a string `domain` são excluídos das verificações da Proteção para a Web: *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 Proteção para a Web: *www.name1.net*, *www.name2.net*, etc.

Aviso
Insira o URLs que deseja excluir da verificação da Proteção para a Web o mais precisamente 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 Proteção para a Web 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 varredura.

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 seu produto Avira contém uma heurística de vírus de macros muito poderosa. Se essa opção for ativada, todas as macros no documento relevante serão excluídas em caso de reparo. Por outro lado, os arquivos suspeitos são apenas relatados, ou seja, você recebe um alerta. Essa opção é ativada como configuração padrão e é recomendada.

Detecção e análise heurística avançada (AheAD)

Ativar AHeAD

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

Nível de detecção baixo

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

Nível de detecção médio

Essa opção combina um nível de detecção forte com baixo risco de alertas falsos. Média será a configuração padrão se você tiver selecionado o uso dessa heurística.

Nível de detecção alto

Se esta opção for ativada, serão detectados significativamente mais malwares desconhecidos, mas há também a possibilidade de serem falso-positivos.

8.7.2 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 para n MB

Se essa opção for ativada, o arquivo de relatório poderá ser limitado a um determinado tamanho; possíveis valores: Os valores permitidos estão 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 tenha sido 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.

Nota
Se você não especificou nenhuma restrição no arquivo de relatório, entradas antigas serão automaticamente excluídas quando o arquivo de relatório atingir 100MB. As entradas serão excluídas até que o tamanho do arquivo de relatório atinja 80 MB.

8.8 Mail Protection

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

8.8.1 Varredura

Use a Mail Protection para executar varredura de e-mails de entrada em busca de vírus, malware . Os e-mails de saída podem ser verificados quanto a vírus e malware pela Mail Protection. Os e-mails de saída que são spams enviados de um bot desconhecido em seu computador podem ser bloqueados pelo para evitar spams.

Ativar Mail Protection

Se esta opção for ativada, o tráfego de e-mails será monitorado pelo Mail Protection. A Mail Protection é um servidor proxy que verifica o tráfego de dados entre o servidor

de e-mail que você usa e do programa de e-mail do cliente em seu computador: e-mails de entrada são verificados em busca de malware por padrão. Se esta opção for desativada, o serviço de Mail Protection ainda será iniciado, mas o monitoramento por Mail Protection será desativado.

Varredura de e-mails de entrada

Se essa opção for ativada, os e-mails 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 e-mail para receber .

Monitorar contas POP3

Se essa opção for ativada, as contas POP3 serão monitoradas nas portas especificadas.

Portas monitoradas

Nesse campo, você deve inserir a porta a ser usada como caixa de entrada pelo protocolo POP3. Várias portas são separadas por vírgulas.

Padrão

Esse botão redefine a porta especificada como a porta POP3 padrão.

Monitorar contas IMAP

Se essa opção for ativada, as contas IMAP serão monitoradas nas portas especificadas.

Portas monitoradas

Nesse campo, você deve inserir a porta a ser usada como caixa de entrada pelo protocolo IMAP. Várias portas são separadas por vírgulas.

Padrão

Esse botão redefine a porta especificada como a porta IMAP padrão.

Varredura de e-mails de saída (SMTP)

Se essa opção for ativada, os e-mails de saída serão verificados em busca de vírus e malware. Os e-mails que são spams enviados por bots desconhecidos são bloqueados.

Portas monitoradas

Nesse campo, você deve inserir a porta a ser usada como caixa de saída pelo protocolo SMTP. Várias portas são separadas por vírgulas.

Padrão

Esse botão redefine a porta especificada como a porta SMTP padrão.

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

Ativar suporte para IPv6

Se essa opção for ativada, a versão 6 do Internet Protocol será suportada pela Mail Protection. (Opção indisponível para novas instalações ou instalações alteradas em Windows 8.)

Resolução de na detecções

Essa seção de configuração contém mais configurações para as ações realizadas quando o Mail Protection encontra um vírus ou programa indesejado em um e-mail ou anexo.

> **Nota**
> Essas ações são realizadas quando um vírus é detectado tanto em e-mails de entrada quanto em e-mails de saída.

Interativo

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

Mostrar barra de andamento

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

Ações permitidas

Nesta caixa podem ser especificadas ações, que 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 e-mail que inclui todos os anexos é movido para a quarentena. Ele pode ser enviado por email posteriormente pelo Gerenciador de quarentena. O e-mail afetado é excluído. O corpo do texto e todos os anexos do e-mail são substituídos por um texto padrão.

Excluir e-mail

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

Excluir anexo

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

Mover anexo para a quarentena

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

Ignorar

Se essa opção for ativada, um e-mail 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. O Mail Protection reage de acordo com as configurações definidas nessa seção.

E-mails afetados

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

Excluir

Se essa opção for ativada, o e-mail afetado será excluído automaticamente caso um vírus ou programa indesejado seja encontrado. O corpo do e-mail é substituído pelo texto padrão fornecido abaixo. O mesmo se aplica a todos os anexos incluídos; eles também são substituídos por um texto padrão.

Ignorar

Se essa opção for ativada, o e-mail afetado será ignorado apesar da detecção de um vírus ou programa indesejado. No entanto, você pode decidir o que deve ser feito com o anexo afetado.

Mover para quarentena

Se essa opção for ativada, o e-mail completo, incluindo todos os anexos, será colocado na quarentena se um vírus ou programa indesejado for encontrado. Se necessário, ele poderá ser restaurado posteriormente. O e-mail afetado propriamente dito é excluído. O corpo do e-mail é substituído pelo texto padrão fornecido abaixo. O mesmo se aplica a todos os anexos incluídos; eles também são substituídos por um texto padrão.

Anexos afetados

A opção *Anexos afetados* só poderá ser selecionada se a configuração **Ignorar** tiver sido selecionada em "*E-mails 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.

Aviso
Se essa opção for selecionada, você não terá nenhuma proteção do Mail Protection contra vírus e programas indesejados. Selecione esse item somente se tiver certeza do que está fazendo. Desative a visualização no programa de e-mail. Nunca abra anexos clicando duas vezes neles.

Mover para quarentena

Se essa opção for ativada, o anexo afetado será colocado na quarentena e excluído (substituído por um texto padrão). Se necessário, o(s) anexo(s) afetado(s) poderá(rão) ser restaurado(s) posteriormente.

Mais ações

Essa seção de configuração contém mais configurações para as ações realizadas quando a Proteção de email encontra um vírus ou programa indesejado em um email ou anexo.

Nota
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 varredura.

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 seu produto Avira contém uma heurística de vírus de macros muito poderosa. Se essa opção for ativada, todas as macros no documento relevante serão excluídas em caso de reparo. Por outro lado, os arquivos suspeitos são apenas relatados, ou seja, você recebe um alerta. Essa opção é ativada como configuração padrão e é recomendada.

Detecção e análise heurística avançada (AheAD)

Ativar AHeAD

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

Nível de detecção baixo

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

Nível de detecção médio

Essa opção combina um nível de detecção forte com baixo risco de alertas falsos. Média será a configuração padrão se você tiver selecionado o uso dessa heurística.

Nível de detecção alto

Se esta opção for ativada, serão detectados significativamente mais malwares desconhecidos, mas há também a possibilidade de serem falso-positivos.

AntiBot

A função AntiBot da Proteção de email impede que o computador se torne parte de uma chamada bot-net e sendo usado para enviar emails de spam: Para enviar spam através de uma bot-net, um atacante normalmente infecta um número de computadores com um bot que se conecta a um servidor de IRC, abre um canal específico e aguarda o comando para enviar emails de spam. Para diferenciar emails de spam de um bot desconhecido de emails genuínos, a Proteção de email verifica se algum email de saída do servidor SMTP e do remetente do email está incluído nas listas de servidores e remetentes permitidos. Caso não esteja, os emails de saída serão bloqueados, isto é, o email não será enviado. O email bloqueado é exibido em uma caixa de diálogo.

Nota
A função AntiBot só poderá ser usada se a verificação de emails de saída da Proteção de email estiver ativada (consulte a opção **Verificar nos emails de saída** em Proteção de email > Verificar).

Servidores permitidos

Todos os servidores dessa lista são autorizados pela Proteção de email para enviar e-mails: emails enviados para esses servidores **não** são bloqueados pela Proteção de email. Se nenhum servidor estiver incluído na lista, o servidor SMTP usado para enviar os emails de saída não será verificado. Se a lista estiver preenchida, a Proteção de email bloqueará os emails enviados para qualquer servidor SMTP não incluído na lista.

Caixa de entrada

Insira o nome do host ou o endereço IP do servidor SMTP usado para enviar seus emails nessa caixa.

Nota
Você pode encontrar detalhes do servidor SMTP usado por seu programa de email para enviar mensagens em seu programa de email na data em que a conta de usuário foi criada.

Adicionar

Você pode usar esse botão para incluir os servidores especificados na caixa de entrada na lista de servidores permitidos.

Excluir

Esse botão exclui uma entrada destacada da lista da servidores permitidos. Esse botão estará desativado se nenhuma entrada for selecionada.

Limpar tudo

Esse botão exclui todas as entradas da lista de servidores permitidos.

Remetente(s) permitido(s)

Todos os remetentes dessa lista são autorizados pela Proteção de email para enviar e-mails: E-mails enviados deste endereço de email **não** são bloqueados pela Proteção de email. Se nenhum remetente estiver incluído na lista, o endereço de email usado para enviar os emails de saída não será verificado. Se a lista estiver preenchida, a Proteção de email bloqueará os emails dos remetentes não incluídos na lista.

Caixa de entrada

Insira o(s) endereço(s) de email dos remetentes nessa caixa.

Adicionar

Você pode usar esse botão para incluir os remetentes especificados na caixa de entrada na lista de remetentes permitidos.

Excluir

Esse botão exclui uma entrada destacada da lista de remetentes permitidos. Esse botão estará desativado se nenhuma entrada for selecionada.

Limpar tudo

Esse botão exclui todas as entradas da lista de remetentes permitidos.

8.8.2 Geral

Exceções

Exceções de varredura

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

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

Exceções de varredura

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 e-mail

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 Proteção de email contém dados sobre os emails verificados que são exibidos como dados estatísticos no Centro de controle em **Proteção de email**.

Número máximo de emails a serem armazenados no cache

Esse campo é usado para definir o número máximo de emails que são armazenados pela Proteção de email 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 e-mail que é exibido nos e-mails enviados.

Essa função requer a ativação da varredura feita pela Mail Protection dos e-mails de saída (consulte a opção **Varredura nos e-mails de saída (SMTP)** em **Configuração > Mail Protection > Varredura**). Você pode usar o rodapé definido pelo Avira Mail Protection para confirmar que o e-mail 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 de Avira Mail Protection.

Rodapé para e-mails a serem enviados

Anexar rodapé do Mail Protection

Se esta opção for ativada, o rodapé de Avira Mail Protection será exibido abaixo do texto da mensagem do e-mail enviado. O rodapé de Avira Mail Protection confirma que o e-mail enviado foi verificado quanto a vírus e programas indesejados pela Mail Protection do Avira e não se origina de um bot desconhecido. O rodapé de Avira Mail Protection contém o seguinte texto: "*Verificado com a Mail Protection do Avira [versão do produto] [iniciais e número da versão do mecanismo de busca] [iniciais e número da versão do arquivo de definição de vírus]*".

Anexe o seguinte rodapé

Se essa opção for ativada, o texto que você inseriu na caixa de entrada será exibido como rodapé nos e-mails enviados.

Caixa de entrada

Nessa caixa de entrada, você pode inserir um texto que é exibido como uma nota de rodapé em e-mails enviados.

8.8.3 Relatório

A Proteção de email 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 Proteção de email 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 Proteção de email 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 a configuração padrão.

Estendido

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

Concluído

Se essa opção for ativada, a Proteção de email registrará todas as informações no arquivo de relatório.

Limitar arquivo de relatório

Limitar tamanho para n MB

Se essa opção for ativada, o arquivo de relatório poderá ser limitado a um determinado tamanho; possíveis valores: Os valores permitidos estão 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 Proteção de email será registrada no arquivo de relatório.

Nota
Se você não especificou nenhuma restrição no arquivo de relatório, será criado automaticamente um novo arquivo de relatório quando o mesmo atingir 100MB. É criado um backup do antigo arquivo de relatório. São salvos até três backups

dos antigos arquivos de relatório. Os backups mais antigos são excluídos primeiro.

8.9 Geral

8.9.1 Categorias de ameaça

Seleção das categorias de ameaça estendidas

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

- Adware
- Adware/Spyware
- Aplicativos
- Clientes Backdoor
- Discador
- Arquivos com Extensão Dupla
- Software fraudulento
- Jogos
- Piadas
- Phishing
- Programas que violam o domínio privado
- Compactadores de tempo de execução incomuns

Ao clicar na caixa relevante o tipo selecionado é ativado (marca de seleção definida) ou desativado (sem marca de seleção).

Selecionar tudo

Se essa opção for ativada, todos os tipos são ativados.

Valores padrão

Esse botão restaura os valores padrão predefinidos.

Nota
Se um tipo for desativado, os arquivos reconhecidos como sendo do tipo de programa relevante não são mais indicados. Nenhuma entrada é feita no arquivo de relatório.

8.9.2 Proteção avançada

ProActiv

Ativar ProActiv

Se essa opção for ativada, os programas serão monitorados no sistema do seu computador e verificados quanto a ações típicas de malware. 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. 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.

O ProActiv protege contra ameaças novas e desconhecidas para as quais não há nenhuma definição de vírus ou heurística disponível. A tecnologia ProActiv está integrada no componente Real-Time Protection e observa e analisa as ações realizadas do programa. O comportamento do programa é verificado com relação aos padrões de ação típicos do malware: Tipo de ação e sequência de ação. Se um programa exibir um comportamento típico de malware, será considerado uma detecção de vírus : Você tem a opção de bloquear o programa ou ignorar a notificação e continuar a usar o programa. Você pode classificar o programa como confiável e adicioná-lo ao filtro de aplicativos para programas permitidos. Você tem a opção de adicionar o programa ao filtro de aplicativos para programas bloqueados usando o comando **Sempre bloquear**.

O componente ProActiv usa conjuntos de regras desenvolvidos pelo Centro de pesquisa de malware da Avira para identificar o comportamento suspeito. Os conjuntos de regras são fornecidos pelos bancos de dados da Avira. O ProActiv envia informações sobre os programas suspeitos para o banco de dados da Avira a fim de que sejam registrados. Durante a instalação do Avira, você tem a opção de desativa a transmissão de dados para os bancos de dados do Avira.

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

Protection Cloud

Ativar Protection Cloud

Os dados de todos os arquivos suspeitos são enviados para a Protection Cloud para inspeção dinâmica on-line. Os arquivos executáveis são identificados imediatamente como limpos, infectados ou desconhecidos.

A Protection Cloud serve como localização central para observar as tentativas de ataques cibernéticos em toda a nossa base de usuários. Os arquivos acessados pelo computador são comparados com os dados dos arquivos armazenados na nuvem. Como uma maior varredura é feita na nuvem, é necessária menos capacidade de processamento pelo aplicativo de antivírus.

Uma lista de locais que são destino frequente do malware é gerada quando o trabalho **Varredura rápida do sistema** é executado. A lista inclui processos em execução, programas que executam na inicialização e serviços. Os dados de cada arquivo são gerados e enviados para o Protection Cloud, que é, então, classificado como "limpo" ou "malware". Os arquivos de programa desconhecidos são enviados via upload para a Protection Cloud para serem analisados.

Confirmar manualmente ao enviar arquivos suspeitos para Avira

É possível ver uma lista dos arquivos suspeitos que devem ser enviados para a Protection Cloud escolher quais arquivos devem ser enviados.

Varredura de arquivos em tempo real

Se esta opção estiver habilitada, arquivos desconhecidos serão enviados para a Protection Cloud para análise assim que forem acessados.

Exibir progresso de envios para a Avira Protection Cloud

Uma janela mostrará as seguintes informações sobre os arquivos enviados, na forma de uma barra de progresso:

- local do arquivo

- nome do arquivo

- status (enviando/analisando)

- resultado (limpo/infectado)

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 de seu computador. Também é possível adicionar programas ao filtro de aplicativos bloqueados por meio de notificações do Real-Time 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 por meio da configuração ou notificando o componente ProActiv. Os aplicativos da lista são bloqueados pelo ProActiv e não podem ser executados no sistema de 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, devem ser especificados o caminho completo, o nome do arquivo e a extensão de arquivo. O caminho deve exibir a unidade onde 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 remover um aplicativo realçado da lista de aplicativos a serem bloqueados.

Aplicativos permitidos

A seção *Aplicativos a serem ignorados* relaciona os aplicativos excluídos do monitoramento pelo componente ProActiv: programas autorizados classificados como confiáveis e incluídos na lista por padrão; todos os aplicativos classificados como confiáveis e adicionados ao filtro do aplicativo: é possível adicionar aplicativos permitidos à lista em Configuração. Além disso, existe a possibilidade de adicionar aplicativos ao comportamento do programa suspeito por meio das notificações da Proteção em Tempo Real usando a opção **Programa confiável** na notificação da Proteção em Tempo Real.

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 por meio da configuração ou das notificações do Real-Time Protection. O componente ProActiv identifica aplicativos usando o caminho, o nome do arquivo e o conteúdo. Recomendamos verificar o conteúdo, pois códigos de malware podem ser adicionados a um programa por meio de alterações como atualizações. É possível determinar se deve ser executada uma verificação de conteúdo a partir do **Tipo** especificado: para o tipo "*Conteúdo*", os aplicativos especificados por caminho e nome de arquivo são verificados em relação às alterações do conteúdo do arquivo antes de serem excluídos da monitoração pelo componente ProActiv. Se o conteúdo

do arquivo tiver sido modificado, o aplicativo será monitorado novamente pelo componente ProActiv. Para o tipo "*Caminho*", o conteúdo não é verificado antes de o aplicativo ser excluído da monitoração pelo Real-Time Protection. Para alterar o tipo de exclusão, clique no tipo exibido.

Aviso
Somente use o tipo *Caminho* em casos excepcionais. O código malicioso pode ser adicionado a um aplicativo por meio de uma atualização. O aplicativo originalmente inofensivo agora é um malware.

Observação
Alguns aplicativos confiáveis, incluindo, por exemplo, todos os componentes do aplicativo do seu produto Avira, são excluídos, por padrão, do monitoramento pelo componente ProActiv, mesmo que não sejam incluídos na lista.

Caixa de entrada

Nesta caixa, é possível inserir o aplicativo a ser excluído do monitoramento pelo componente ProActiv. Para identificar o aplicativo, devem ser especificados o caminho completo, o nome do arquivo e a extensão de arquivo. O caminho deve exibir a unidade onde o aplicativo está localizado ou começar com uma variável de ambiente.

O botão abre uma janela na qual você pode 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 remover um aplicativo realçado da lista de aplicativos a serem excluídos.

8.9.3 Senha

Você pode proteger o produto Avira em diferentes áreas com uma senha. Se uma senha foi criada, ela será solicitada toda vez que desejar abrir a área protegida.

Senha

Digitar senha

Insira a senha solicitada aqui. Por motivos de segurança, os caracteres reais digitados neste espaço são substituídos por curinga (*). A senha pode ter no máximo 20

caracteres. Depois que a senha for criada, o programa nega 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 curinga (*).

Nota
A senha diferencia maiúsculas e minúsculas!

Áreas protegidas por senha

O produto Avira pode proteger áreas individuais com uma senha. Ao clicar na caixa relevante, a solicitação de senha pode 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 é necessária para iniciar o Centro de Controle.
Ativar / desativar o Real-Time Protection	Se essa opção for ativada, a senha predefinida será necessária para ativar ou desativar o Avira Real-Time Protection.
Ativar / Desativar o Mail Protection	Se essa opção for ativada, a senha predefinida será necessária para ativar/desativar o Mail Protection.
Ativar/desativar o FireWall	Se essa opção for ativada, a senha predefinida será necessária para ativar/desativar o FireWall.

Ativar / desativar o Web Protection	Se essa opção for ativada, a senha predefinida será necessária para ativar/desativar o Web Protection.
Quarentena	Se essa opção for ativada, todas as áreas possíveis 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 varredura 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 é necessária para exibir as propriedades de um objeto.
Excluir objetos afetados	Se essa opção for ativada, a senha predefinida é necessária para excluir um objeto.
Enviar e-mail para a Avira	Se essa opção for ativada, uma senha predefinida é 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 é necessária para copiar o objeto afetado.

Adicionar e modificar tarefas	Se essa opção for ativada, a senha predefinida é necessária para adicionar e modificar trabalhos no Agendamento.
Baixe o CD de resgate da Internet	Se essa opção for ativada, a senha predefinida é necessária para iniciar o download do CD de resgate da Avira.
Configuração	Se essa opção for ativada, a configuração do programa somente poderá ser feita depois que a senha predefinida for inserida.
Alternar a configuração manualmente	Se essa opção for ativada, a senha predefinida é necessária para desejar alternar manualmente para um perfil de configuração diferente.
Instalação / desinstalação	Se essa opção for ativada, a senha predefinida é necessária para a instalação ou desinstalação do programa.

8.9.4 Segurança

Execução automática

Bloquear função de execução automática

Se essa opção estiver ativada, a execução da função Execução automática do Windows é bloqueada em todas as unidades conectadas, incluindo pendrives, unidades de CD e DVD e unidades de rede. Com a função de execução automática do Windows, os arquivos em mídias de dados ou unidades de rede são lidos imediatamente no carregamento ou na 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 Execução automática é particularmente crítica para pendrives, pois os dados de um pendrive podem ser alterados a qualquer momento.

Excluir CDs e DVDs

Quando esta opção estiver ativada, a função Execução automática é permitida em unidades de CD e DVD.

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

Proteção do sistema

Proteger arquivos host do Windows contra alterações

Se essa opção for configurada para ativada, os arquivos hosts do Windows são protegidos contra gravação. A manipulação não é mais possível. Por exemplo, o malware não pode redirecioná-lo para sites indesejados. Essa opção é ativada como a configuração padrão.

Proteção do produto

Nota
As opções de proteção do produto não estão disponíveis se o Real-Time Protection não foi instalado usando a opção de instalação definida pelo usuário.

Proteger os processos de encerramento indesejado

Se essa opção for ativada, todos os processos do programa serão protegidos contra encerramento indesejado acionado por vírus e malwares ou contra encerramento “não controlado” acionado pelo usuário, por exemplo, através do Gerenciador de tarefas. Essa opção é ativada como a configuração padrão.

Proteção de processo avançada

Se essa opção for ativada, todos os processos do programa serão protegidos com opções avançadas contra encerramento indesejado. A proteção de processo 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.

Nota
A proteção por senha não está disponível para Windows XP 64 bits !

Aviso
Se a proteção do processo for ativada, poderão ocorrer problemas de interação com outros produtos de software. Nesses casos, desative a proteção do processo.

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 do programa (arquivos binários e de configuração) serão protegidos contra manipulação. A proteção contra manipulação impede o acesso de gravação, exclusão e, em alguns casos, de leitura às entradas do registro ou aos arquivos de programa por usuários ou programas externos. Para ativar essa opção, é necessário reiniciar o computador.

Aviso
Observe que se essa opção for desativa, o reparo de computadores infectado com tipos específicos de malware poderá falhar.

Nota
Quando essa opção estiver ativada, as alterações podem ser feitas somente na configuração, incluindo alterações nas solicitações de varredura ou atualização, por meio da interface do usuário.

Nota
A proteção de arquivos e entradas de registro não está disponível para Windows XP 64 bits !

8.9.5 WMI

Suporte para Instrumentação de gerenciamento do Windows

A Instrumentação de gerenciamento do Windows é uma técnica de administração básica do Windows que usa linguagens de script e programação para permitir o acesso de leitura e gravação, local e remoto, às configurações dos sistemas Windows. Seu produto Avira oferece suporte a WMI e fornece dados (informações de status, dados estatísticos, relatórios, solicitações planejadas etc.) bem como eventos e métodos (processos de início e término) por meio de uma interface. A WMI oferece a opção de baixar dados operacionais do programa e controlar o programa.Você pode solicitar um guia de referência completo da interface da WMI ao fabricante. 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.

8.9.6 Eventos

Limitar tamanho do banco de dados de eventos

Limitar o tamanho ao máximo de n entradas

Se essa opção for ativada, o número máximo de eventos indicados no banco de dados de eventos pode ser limitado a um tamanho determinado; valores possíveis:

100 a 10000 e entradas. Se o número de entradas inseridas foi excedido, as entradas mais antigas são 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; valores possíveis: 1 a 90 de dias. Essa opção é ativada como a 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.

8.9.7 Relatórios

Limitar relatórios

Limitar número para no máx. n partes

Quando essa opção é ativada, o número máximo de relatórios pode ser limitado a um valor específico. São permitidos valores entre 1 e 300. Se o número especificado for ultrapassado, o relatório mais antigo no momento é excluído.

Excluir todos os relatórios mais antigos que n dia(s)

Se essa opção for ativada, os relatórios são excluídos automaticamente depois de um número de dias específico. Os valores permitidos são: 1 a 90 dias. Essa opção é ativada como a configuração padrão, com um valor de 30 dias.

Sem limite

Se essa opção for ativada, o número de relatórios não é restringido.

8.9.8 Diretórios

Caminho temporário

Usar configurações padrão do sistema

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

Nota
Você pode ver onde o sistema salva os arquivos temporários - por exemplo, com o Windows XP - em: **Iniciar > Configurações > Painel de Controle > Sistema > Cartão de índice** "**Avançado**" Botão "**Variáveis ambientais**". As variáveis temporárias (`TEMP`, `TMP`) do usuário registrado atualmente e das

variáveis de sistema (`TEMP`, `TMP`) são mostradas aqui com seus valores relevantes.

Use o seguinte diretório

Se essa opção for ativada, o caminho exibido na caixa de entrada é usado.

Caixa de entrada

Nesta caixa de entrada, insira o caminho em que 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 absoluto até o diretório do 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.

8.9.9 Alertas acústicos

Quando um vírus ou malware é detectado pelo Scanner ou Real-Time 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.

Nota
O modo de ação do System Scanner é definido na configuração em System Scanner > Verificar > Ação na detecção. O modo de ação do Real-Time Protection é definido na configuração em Real-Time Protection > Verificar > Resolução de na detecções.

Nenhum aviso

Quando essa opção for ativada, nenhum alerta acústico será emitido quando um vírus for detectado pelo Scanner ou Real-Time Protection.

Usar os alto falantes do PC (apenas no modo interativo)

Se essa opção for ativada, há um alerta acústico com o sinal padrão quando um vírus for detectado pelo Scanner ou Real-Time 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, há um alerta acústico com o WAVE arquivo selecionado quando um vírus for detectado pelo Scanner ou Real-Time 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.

8.9.10 Alertas

Rede

Alertas configuráveis individualmente podem ser enviados do System Scanner ou do Real-Time Protection para qualquer estação de trabalho da rede.

Nota
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**.

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

Aviso
Essa funcionalidade **não é mais suportada** pelos 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.

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

Inserir

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

O botão abre uma janela na qual você pode selecionar, como alternativa, um computador diretamente no ambiente de computador.

Excluir

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

Alertas de rede do Real-Time Protection

Alertas de rede

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

Nota
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	Insere uma guia A linha atual é recuada vários caracteres à direita.
Ctrl + Enter	Insere 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 de arquivo do arquivo afetado
`%COMPUTER%`	Contém o nome do computador em que o Real-Time Protection está em execução
`%NAME%`	Contém o nome do usuário que acessou o arquivo afetado
`%ACTION%`	Contém a ação executada após a detecção do vírus
`%MACADDR%`	Contém o endereço MAC do computador em que o Real-Time Protection está em execução

Padrão

O botão restaura o texto padrão predefinido de um alerta.

Alertas de rede do Scanner

Ativar alertas de rede

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

> **Nota**
> 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	Insere uma guia A linha atual é recuada vários caracteres à direita
Ctrl + Enter	Insere 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 Scanner
`%COMPUTER%`	Contém o nome do computador em que o Scanner está em execução

Padrão

O botão restaura o texto padrão predefinido de um alerta.

E-mail

O produto Avira pode enviar alertas e mensagens via e-mail para um ou mais destinatários com determinados eventos. Isso é feito com o Protocolo de transferência de mensagem simples (SMTP).

As mensagens podem ser acionadas por vários eventos. Os seguintes componentes suportam o envio de e-mails:

- Alertas de e-mail do Real-Time Protection
- Alertas de e-mail do Scanner
- Alertas de e-mail do atualizador

> **Nota**
> Observe que não há suporte para ESMTP. Além disso, no momento transferências criptografadas via TLS (Transport Layer Security) ou SSL (Secure Sockets Layer) não são permitidas.

Mensagens de e-mail

Servidor SMTP

Insira o nome do host a ser usado aqui – seu endereço IP ou o nome do host direto. O nome do host pode ter no máximo 127 caracteres.

Por exemplo*:*

`192.168.1.100` ou `mail.samplecompany.com`.

Porta

Insira a porta a ser usada aqui.

Endereço do remetente

Nessa caixa de entrada, insira o endereço de e-mail do remetente. O endereço do remetente pode ter no máximo 127 caracteres.

Autenticação

Alguns servidores de e-mail esperam que um programa verifique o servidor (faça login) antes que o e-mail seja enviado. Alertas podem ser transmitidos com autenticação para um servidor SMTP via e-mail.

Autenticação do usuário

Se essa opção for ativada, um nome de usuário e uma senha podem ser inseridos nas caixas relevantes para logon (autenticação).

Nome de logon:
Insira seu nome de usuário aqui.

Senha:
Insira a senha relevante aqui. A senha é salva na forma criptografada. Por motivos de segurança, os caracteres reais digitados neste espaço são substituídos por curinga (*).

Enviar e-mail de teste

Ao clicar no botão, o programa tenta enviar um e-mail de teste para o endereço do remetente para verificar os dados inseridos.

Alertas de e-mail do Real-Time Protection

O Avira Real-Time Protection pode enviar alertas por e-mail para um ou mais destinatários para determinados eventos.

Alertas de e-mail

Se essa opção for ativada, o Avira Real-Time Protection envia mensagens de e-mail com as informações mais importantes quando ocorrer um evento determinado. Essa opção é desativada como a configuração padrão.

Mensagens de e-mail para os eventos a seguir

A varredura durante o acesso detectou um vírus ou programa indesejado

Se essa opção for ativada, você sempre receberá um e-mail com o nome do vírus ou programa indesejado e o arquivo afetado quando a varredura no acesso detectar um vírus ou programa indesejado.

Editar

O botão "**Editar**" abre a janela "**Modelo de e-mail**', na qual é possível configurar a notificação de um evento “Detecção durante o acesso”. Você tem a opção de inserir texto na linha de assunto e no corpo do e-mail. Variáveis podem ser usadas para esse propósito. (consulte Modelo de e-mail)

Ocorreu um erro crítico no Real-Time Protection

Se essa opção for ativada, você receberá um e-mail toda vez que um erro crítico interno for detectado.

Nota
nesse caso, informe ao nosso suporte técnico e inclua os dados fornecidos no e-mail. O arquivo especificado também deverá ser enviado para análise.

Editar

O botão "**Editar**" abre a janela "**Modelo de e-mail**" na qual é possível configurar a notificação de um evento "Erro crítico no Real-Time Protection". Você tem a opção de inserir texto na linha de assunto e no corpo do e-mail. Variáveis podem ser usadas para esse propósito. (consulte Modelo de e-mail)

Destinatário(s)

Insira o(s) endereço(s) de e-mail do(s) destinatário(s) nessa caixa. Os endereços individuais são separados por vírgulas. Todos os endereços juntos (ou seja, a sequência de caracteres) podem ter no máximo 260 caracteres.

Alertas de e-mail do Scanner

Para determinados eventos, a varredura sob demanda pode enviar alertas e mensagens por e-mail para um ou mais destinatários.

Alertas de e-mail

Se essa opção for ativada, o programa envia mensagens de e-mail com as informações mais importantes quando ocorrer um determinado evento. Essa opção é desativada como a configuração padrão.

Mensagens de e-mail para os eventos a seguir

A varredura por solicitação detectou um vírus ou programa indesejado

Se essa opção for ativada, você receberá um e-mail com o nome do vírus ou programa indesejado e o arquivo afetado toda vez que a varredura sob demanda detectar um vírus ou programa indesejado.

Editar

O botão**Editar** abre a janela "**Modelo de e-mail**" na qual é possível configurar a notificação para um evento de “Detecção durante a varredura”. Você tem a opção de inserir texto na linha de assunto e no corpo do e-mail. Variáveis podem ser usadas para esse propósito. (Consulte Modelo de e-mail)

Fim da varredura programada

Quando a opção estiver ativada, um e-mail é enviado quando um trabalho de varredura for realizado. O e-mail contém dados sobre o local e a duração do trabalho de varredura, as pastas e os arquivos verificados, bem como sobre os vírus encontrados e avisos.

Editar

O botão**Editar** abre a janela "**Modelo de e-mail**" na qual é possível configurar a notificação para um evento de “Fim da varredura”. Você tem a opção de inserir texto na linha de assunto e no corpo do e-mail. Variáveis podem ser usadas para esse propósito. (Consulte Modelo de e-mail)

Adicionar arquivo de relatório como anexo

Se essa opção for ativada, o arquivo de relatório atual do componente Scanner é adicionado ao e-mail como um anexo ao enviar notificações do Scanner.

Destinatário(s)

Insira o(s) endereço(s) de e-mail do(s) destinatário(s) nessa caixa. Os endereços individuais são separados por vírgulas. Todos os endereços juntos (ou seja, a sequência de caracteres) podem ter no máximo 260 caracteres.

Alertas de e-mail do atualizador

O componente Atualizador pode enviar notificações por e-mail para um ou mais destinatários para eventos específicos.

Alertas de e-mail

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

Mensagens de e-mail para os eventos a seguir

Nenhuma atualização é necessária. O programa está atualizado

Se essa opção for ativada, um e-mail será enviado se o Atualizador consiguir estabelecer uma conexão com o servidor de download, mas nenhum arquivo novo estiver disponível no servidor. Isso significa que o produto Avira está atualizado.

Editar

O botão "**Editar**" abre a janela "**Modelo de e-mail**" na qual é possível configurar a notificação para um evento “Nenhuma atualização necessária”. Você tem a opção de inserir texto na linha de assunto e no corpo do e-mail. Variáveis podem ser usadas para esse propósito. (consulte Modelo de e-mail)

Atualização da concluída com êxito. Novos arquivos foram instalados

Se essa opção for ativada, um e-mail é enviado para todas as atualizações executadas: essa pode ser uma atualização do produto, do arquivo de definição de vírus ou do mecanismo de varredura.

Editar

O botão**Editar** abre a janela "**Modelo de e-mail**" na qual é possível configurar a notificação para um evento “Atualização bem-sucedida - novos arquivos instalados”. Você tem a opção de inserir texto na linha de assunto e no corpo do e-mail. Variáveis podem ser usadas para esse propósito. (consulte Modelo de e-mail)

Atualização falhou

Se essa opção for ativada, um e-mail será enviado se houver uma falha de atualização devido a um erro.

Editar

O botão "**Editar**" abre a janela "**Modelo de e-mail**" na qual é possível configurar a notificação para um evento de “Falha de atualização”. Você tem a opção de inserir texto na linha de assunto e no corpo do e-mail. Variáveis podem ser usadas para esse propósito. (consulte Modelo de e-mail)

Adicionar arquivo de relatório como anexo

Se essa opção for ativada, o arquivo de relatório atual do componente Atualizador é adicionado a um e-mail como anexo ao enviar notificações do Atualizador.

Destinatário(s)

Insira o(s) endereço(s) de e-mail do(s) destinatário(s) nessa caixa. Os endereços individuais são separados por vírgulas. Todos os endereços juntos (ou seja, a sequência de caracteres) podem ter no máximo 260 caracteres.

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 aceitáveis globalmente

Variável	Valor
Variáveis do ambiente Windows	O componente de notificações de email suporta todas as variáveis do ambiente Windows.
%SYSTEM_IP%	Endereço IP do computador
%FQDN%	Nome de domínio totalmente qualificado
%TIMESTAMP%	Registro 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 varredura usado	Real-Time Protection Scanner
%VDFVER%	Versão do arquivo de definição de vírus usado	Real-Time Protection Scanner
%SOURCE%	Nome de arquivo totalmente qualificado	Real-Time Protection
%VIRUSNAME%	Nome do vírus ou programa indesejado	Real-Time Protection
%ACTION%	Ação executada após a detecção	Real-Time Protection
%MACADDR%	Endereço MAC da primeira placa de rede registrada	Real-Time Protection

%UPDFILESLIST%	Lista de arquivos atualizados	Atualizador
%UPDATETYPE%	Tipo de atualização: atualização do mecanismo de varredura e do arquivo de definição de vírus ou atualização do produto com atualização do mecanismo de varredura 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	Scanner
%FILECOUNT%	Número de arquivos verificados	Scanner
%MALWARECOUNT%	Número de vírus ou programas indesejados detectados	Scanner
%REPAIREDCOUNT%	Número de arquivos infectados reparados	Scanner
%RENAMEDCOUNT%	Número de arquivos infectados renomeados	Scanner
%DELETEDCOUNT%	Número de arquivos infectados excluídos	Scanner
%WIPECOUNT%	Número de arquivos infectados substituídos e excluídos	Scanner
%MOVEDCOUNT%	Número de arquivos infectados movidos para a quarentena	Scanner

%WARNINGCOUNT%	Número de avisos	Scanner
%ENDTYPE%	Status da varredura: terminada/concluída com êxito	Scanner
%START_TIME%	Hora do início da varredura: Hora do início da atualização	Scanner, Atualizador
%END_TIME%	Final da varredura Final da atualização	Scanner, Atualizador
%TIME_TAKEN%	Duração da varredura em minutos Duração da atualização em minutos	Scanner, Atualizador
%LOGFILEPATH%	Caminho e nome do arquivo de relatório	Scanner, Atualizador

Alertas acústicos

Quando um vírus ou malware é detectado pelo Scanner ou Real-Time 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.

Nota
O modo de ação do System Scanner é definido na configuração em System Scanner > Verificar > Ação na detecção. O modo de ação do Real-Time Protection é definido na configuração em Real-Time Protection > Verificar > Resolução de na detecções.

Nenhum aviso

Quando essa opção for ativada, nenhum alerta acústico será emitido quando um vírus for detectado pelo Scanner ou Real-Time Protection.

Usar os alto falantes do PC (apenas no modo interativo)

Se essa opção for ativada, há um alerta acústico com o sinal padrão quando um vírus for detectado pelo Scanner ou Real-Time 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, há um alerta acústico com o WAVE arquivo selecionado quando um vírus for detectado pelo Scanner ou Real-Time 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 de programa bem sucedidas ou não, como as atualizações. Em **Alertas** é possível ativar ou desativar as notificações de eventos específicos.

Com as notificações de área de trabalho, você pode desativar a notificação diretamente na tela deslizante. É possível reativar a notificação na janela de configuração **Alertas**.

Atualização

Alertar, se a última atualização ocorreu há mais de 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 é 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, uma mensagem de alerta é exibida se o arquivo de definição de vírus não estiver desatualizado. Com a ajuda da opção de alerta, você pode configurar o intervalo de tempo para um alerta se a última atualização tiver mais que n dia(s).

Avisos / Notas com as situações a seguir

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 computador através da rede telefônica ou ISDN. There is a danger that the connection may have been created by an

unknown and unwanted dialer and that the connection may be chargeable (consulte Vírus e mais > Categorias de Ameaça: Discador).

Arquivos foram atualizados com sucesso

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

Atualização falhou

Se essa opção for ativada, você receberá uma notificação de área de trabalho toda vez que uma atualização falhar: não pôde ser criada conexão com o servidor de download ou os arquivos de atualização não puderam ser instalados.

Nenhuma atualização é necessária

Se essa opção for ativada, você receberá uma notificação de área de trabalho toda vez que uma atualização for iniciada, mas a instalação dos arquivos não for necessária porque o programa está atualizado.

9. Ícone de Bandeja

O ícone de bandeja na bandeja do sistema da barra de tarefas exibe o status do serviço do Real-Time Protection e do FireWall .

Ícone	Descrição
	O Avira Real-Time Protection é ativado e o FireWall é ativado
	O Avira Real-Time Protection é desativado ou o FireWall é desativado

Entradas no menu contextual

- **Ativar Real-Time Protection**: Ativa ou desativa o Avira Real-Time Protection.
- **Ativar Mail Protection**: Ativa ou desativa o Avira Mail Protection.
- **Ativar Web Protection**: Ativa ou desativa o Avira Web Protection.
- **FireWall**:
  - **Ativar FireWall**: Ativa ou desativa o Avira FireWall
  - **Ativar Firewall do Windows**: Ativa ou desativa o Firewall do Windows (esta funcionalidade está disponível a partir do Windows 8).
  - **Bloquear todo o tráfego**: Ativado: Bloqueia todas as transferências de dados, exceto as transferências para o sistema do computador host (Host Local/IP 127.0.0.1).
- **Iniciar Avira Professional Security**: Abre o Centro de Controle.
- **Configurar Avira Professional Security**: 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 já foram definidas regras para comutação automática para uma configuração.
- **Ajuda**: abre a ajuda online.
- **Sobre o Avira Professional Security**: Abre uma caixa de diálogo com informações sobre seu produto Avira: Informações do produto, Informações da versão, Informações de licença.
- **Avira na Internet**: Abre o portal da Web da Avira na Internet. Para isso, é necessário ter uma conexão ativa com a Internet.

10. FireWall

Avira Professional Security permite gerenciar o tráfego de dados de entrada e de saída dependendo das configurações do computador:

- Avira FireWall

O Avira Professional Security inclui o Avira FireWall.

- Avira FireWall em AMC

Se for gerenciado com o Avira Management Console, o Avira Professional Security também inclui o Avira FireWall.

- Firewall do Windows

A partir do Windows 7, o Firewall do Windows é agora gerenciado com o produto Avira.

10.1 Avira FireWall

10.1.1 FireWall

O Avira FireWall monitora e regula o tráfego de dados de entrada e saída no sistema de seu computador e o protege contra diversos ataques e ameaças da Internet. Tráfego de dados de entrada e saída ou detecção de portas serão permitidos ou negados com base em diretrizes de segurança. 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 tenta pela primeira vez 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**. O salvamento das ações na janela Evento de Rede fornece a você um conjunto de regras para as atividades de rede dos aplicativos.

Observação
Para aplicativos de fornecedores confiáveis, o acesso à rede é permitido por

padrão, a menos que uma regra do adaptador proiba o acesso à rede. 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 de adaptador na Configuração. O nível de segurança do FireWall é definido automaticamente para o valor *Personalizado* se você adicionar ou alterar as regras de adaptador.
As regras do aplicativo permitem definir regras de monitoramento especificadas para aplicativos:
você pode usar regras de aplicativo simples para definir se todas as atividades de rede de um aplicativo de software devem ser negadas ou permitidas ou se elas devem ser manipuladas por meio da janela popup *Evento de Rede* .
Na configuração avançada da *Configuração de Regras do Aplicativo*, você pode definir diferentes filtros de pacote para um aplicativo, os quais são executados como regras do aplicativo específicas.

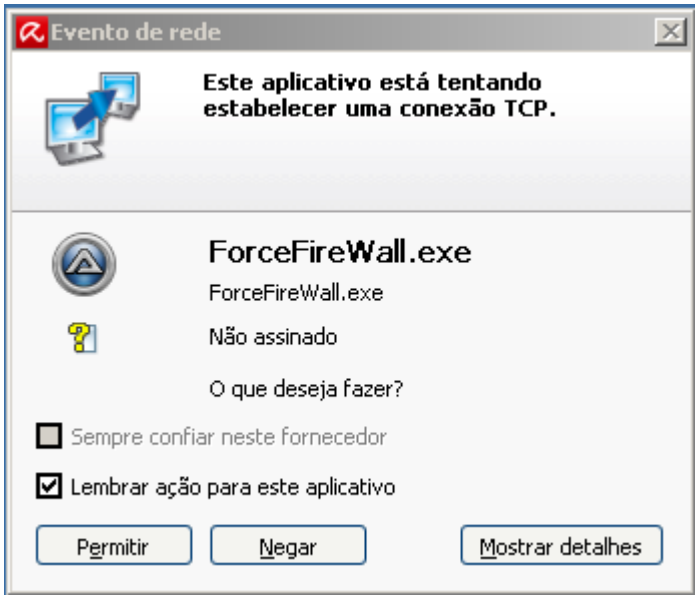
10.1.2 Evento de rede

Na janela Evento de Rede do componente Avira FireWall, você pode decidir se um aplicativo de software do acesso à rede pode ou não enviar dados ou realizar outras atividades de rede: Você pode permitir ou negar o tráfego de dados ou a detecção passiva de portas. Negar atividades de rede pode causar o cancelamento de uma conexão.

A janela Evento de Rede é aberta nos seguintes casos quando os aplicativos são acessados a partir da rede:

- Nenhuma regra de aplicativo foi criada ainda para o aplicativo. Isso acontece quando um aplicativo estabelece uma conexão com a rede pela primeira vez após a instalação do Avira Firewall. No entanto, aplicativos cujos fornecedores foram classificados como confiáveis e cujo acesso à rede foi permitido automaticamente são excluídos (consulte Capítulo Configuração > FireWall > Fornecedores Confiáveis).
- Uma regra de aplicativo simples com o tipo de ação **Perguntar** foi criada.
- As regras de aplicativo especificadas foram criadas para o aplicativo com base nos filtros de pacote na configuração estendida, no entanto, nenhuma regra foi detectada para o evento de rede que surgiu. Neste caso, você pode usar o botão *Estendido* para chamar as regras de aplicativo existentes e para adicionar o acesso à rede como uma nova regra.

Evento de rede



Informações exibidas

Nome do aplicativo.

Nome do aplicativo.

Nome do arquivo

Nome do arquivo executável.

Verificação e recomendação da assinatura

Resultado da ação de verificação e recomendação da assinatura.
Se o aplicativo for assinado com o certificado de um provedor confiável, é recomendado permitir o tráfego de dados.

Informações detalhadas

Endereço local

Endereço e porta de origem.

Endereço remoto

Endereço e porta de destino.

Usuário

Usuário registrado para quem o aplicativo é executado.

ID do processo

ID do processo do aplicativo.

Caminho

Caminho até o arquivo executável do aplicativo.

Empresa

Fornecedor do aplicativo (informações da versão).

Versão

Versão do aplicativo.

Assinado por

Fornecedor do aplicativo (assinatura).

Ações e botões

Sempre confiar neste fornecedor

Se essa opção for ativada, o fornecedor do software será adicionado à lista de fornecedores confiáveis durante a execução da solicitação de *Evento de Rede*. O botão Negar é desativado assim que essa opção é ativada.

> **Observação**
> Esta ação está disponível somente em aplicativos assinados.

Lembrar ação para este aplicativo

Se essa opção for ativada, a ação executada será salva como uma regra de aplicativo. A regra de aplicativo pode ser chamada na configuração em FireWall > Configurações de Popup.

Se a opção *Lembrar ação para este aplicativo* for ativada e existirem regras do aplicativo específicas com base nos filtros de pacote para o aplicativo, a janela de configuração avançada das regras de aplicativo será exibida quando você clicar nos botões **Permitir** ou **Negar**. O tráfego de dados ocorrido foi adicionado automaticamente ao início da lista como uma regra de aplicativo específica. Você pode alterar a posição das regras de aplicativo adicionadas ou remover as regras de aplicativo adicionadas na janela *FireWall > Regras de Aplicativo*.

Botões	Descrição
Avançado	A janela para configuração avançada das regras de aplicativo é aberta. **Observação** O botão está disponível somente se configurações estendidas são ativadas para regras de aplicativos (consulte Configuração > FireWall > Configurações).
Permitir	A atividade de rede relevante é permitida.
Negar	A atividade de rede relevante é negada.
Mostrar/Ocultar Detalhes	Informações detalhadas sobre o aplicativo são exibidas ou ocultadas.

10.2 Firewall do Windows

A partir do Windows 7, Avira Professional Security dá a opção de gerenciar diretamente o Firewall do Windows por meio do Centro de Controle e Configuração Avira. As seguintes opções estão disponíveis para o Firewall do Windows:

ativar o Firewall do Windows por meio do Centro de Controle

A opção *FireWall* em **Status > Proteção na Internet** permite ativar ou desativar o Firewall do Windows clicando no botão **ON/OFF**.

verificar o estado do Firewall do Windows por meio do Centro de Controle

É possível verificar o estado do Firewall do Windows na seção **PROTEÇÃO NA INTERNET > FireWall** e restaurar as configurações recomendadas clicando no botão **Corrigir problema**.

11. Atualizações

11.1 Atualizações

A eficiência do software antivírus depende do quão atualizado está o programa, especialmente o ficheiro de definição de vírus e o motor de pesquisa. Para executar atualizações regulares, o componente Atualizador é integrado no seu produto Avira. O Atualizador assegura que o seu produto Avira está sempre atualizado e é capaz de lidar com novos vírus que surgem diariamente. O Atualizador atualiza os seguintes componentes:

- Ficheiro de definição de vírus:

  O ficheiro de definição de vírus contém os padrões de vírus dos programas prejudiciais utilizados pelo seu produto Avira para verificar a presença de vírus e malwares e reparar objetos infectados.

- Motor de pesquisa:

  O motor de pesquisa contém os métodos utilizados pelo seu produto Avira para verificar a existência de vírus e malwares.

- Ficheiros 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 ficheiro de definição de vírus, o motor de pesquisa e o produto estão atualizados e, se necessário, implementa uma atualização. Depois da atualização do produto, talvez seja necessário reiniciar o sistema do computador. Se apenas o ficheiro de definição de vírus e o motor de pesquisa forem atualizados, o computador não precisará de ser reiniciado.

Quando uma atualização do produto requer um reinício, pode decidir continuar com a atualização ou ser lembrado mais tarde sobre esta. Se continuar a atualização do produto imediatamente, poderá escolher quando pretende que o reinício seja efetuado.

Se pretende ser lembrado sobre a atualização mais tarde, o ficheiro de definição de vírus e o motor de pesquisa serão atualizados de qualquer maneira mas a atualização do produto não será desempenhada.

Nota
A atualização do produto não será concluída até que seja efetuado um reinício.

Nota
Por motivos de segurança, o Atualizador verifica se o ficheiro *hosts* do Windows do seu computador foi alterado de modo a que, por exemplo, o URL de Atualização tenha sido manipulado por malware e esteja a desviar o

Atualizador para sites de transferências indesejados. Se o ficheiro hosts do Windows tiver sido manipulado, isso será mostrado no ficheiro de relatório do Atualizador.

Uma atualização é executada automaticamente no seguinte intervalo: 60 minutos. Pode editar ou desativar a atualização automática através da configuração (Configuração > Atualizar).

No Centro de Controlo, no **Agendamento**, pode criar trabalhos de atualização adicionais que são realizados pelo Atualizador nos intervalos especificados. Também pode iniciar uma atualização manualmente:

- no Centro de Controlo: no menu **Atualizar** e na secção **Estado**
- através do menu de contexto do ícone de bandeja

As atualizações podem ser obtidas na Internet através de um servidor da Web proprietário ou de um servidor da Web ou de ficheiros numa intranet, que transfere os ficheiros de atualização da Internet e os disponibiliza a outros computadores na rede. Isto é útil se desejar atualizar produtos Avira em mais de um computador numa rede. É possível utilizar um servidor de transferência numa intranet para garantir que os produtos Avira são atualizados nos computadores protegidos utilizando o mínimo de recursos. Para configurar um servidor de transferência funcional numa intranet, precisa de um servidor que seja compatível com a estrutura de atualização do seu produto Avira.

Nota
Pode utilizar o Avira Update Manager (servidor de ficheiros ou servidor da Web no Windows) como um servidor da Web ou um servidor de ficheiros na intranet. O Avira Update Manager espelha os servidores de transferência 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 utilizado, é utilizado o protocolo HTTP para a transferência. Ao utilizar um servidor de ficheiros, o acesso ao ficheiro de atualização é concedido pela rede. Pode configurar a ligação com o servidor da Web ou o servidor de ficheiros em Configuração > Atualizar. A configuração predefinida utiliza uma ligação com a Internet existente como a ligação com os servidores da Web da Avira.

11.2 Atualizador

A janela Atualizador é aberta no início de uma atualização.

Observação
Para atualizar trabalhos criados no Agendamento, é possível definir o modo de exibição para a janela de atualização: Você pode selecionar **Ocultar**, **Minimizar** ou **Maximizar**.

Observação
Se estiver usando um programa no modo de tela inteira (por exemplo,. jogos) e o modo de exibição do atualizador estiver configurado como maximizado ou minimizado, o atualizador comutará para a área de trabalho. Para evitar isto, inicie o atualizador com o modo de exibição configurado como Ocultar. Nesse modo, você não receberá mais notificações sobre atualizações na janela de atualização.

Status: Mostra o andamento do atualizador.

Tempo decorrido: O tempo que decorreu desde o início do download.

Tempo restante: Tempo até o fim do download.

Velocidade do download: A velocidade do download.

Transmitido: Bytes já baixados.

Restantes: Bytes que faltam baixar.

Botões e links

Botão / link	Descrição
	Esta página da ajuda on-line é aberta por meio deste botão ou link.
Reduzir	A janela de exibição do atualizador aparecerá em tamanho reduzido.
Ampliar	A janela de exibição do atualizador voltará ao tamanho original.
Anular	O procedimento de atualização será cancelado. O atualizador será fechado.
Fechar	O procedimento de atualização foi concluído. A janela de exibição será fechada.
Relatório	O arquivo de relatório da atualização é exibido.

12. Perguntas Frequentes, Dicas

Este capítulo contém informações importantes sobre solução de problemas e dicas adicionais sobre como usar seu produto Avira.

- consulte o Capítulo Ajuda no caso de um problema
- consulte o Capítulo Atalhos
- consulte o Capítulo Windows Security Center (Windows XP) ou Windows Action Center (no Windows 7)

12.1 Ajuda caso ocorra um problema

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

- A mensagem de erro *O arquivo de licença não pode ser aberto* é exibida.
- 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 relata o Avira Real-Time Protection e o Avira Mail Protection imediatamente após a ativação.
- O Avira Mail Protection não funciona.
- Não há nenhuma conexão de rede disponível em uma máquina virtual (por exemplo, VMWare, PC virtual...) se o Avira FireWall foi instalado na máquina do host e o nível de segurança do Avira FireWall está definido como *médio* ou *alto*.
- A conexão VPN (Virtual Private Network, Rede Privada Virtual) é bloqueada se o nível de segurança do Avira FireWall está definido como *médio* ou *alto*.
- Um e-mail enviado através de uma conexão TLS foi bloqueado pelo Mail Protection.
- O Webchat não está operacional: As mensagens de bate-papo não são exibidas; os dados estão sendo carregados no navegador.

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

Motivo: O arquivo está criptografado.

- Para ativar a licença não é necessário 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. Nenhuma conexão com o servidor da web na Internet pode, portanto, ser estabelecida.

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

Motivo: não é possível conectar com o servidor proxy.

- Verifique se o logon 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 sua configurações na Configuração em Proteção do PC > Atualizar.

Vírus e malwares não podem ser movidos nem excluídos.

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

- Atualize seu produto Avira.
- Se você usar o sistema operacional Windows XP, desative a Restauração do Sistema.
- Inicie o computador no Modo de Segurança.
- Inicie a Configuração de seu produto Avira .
- Selecione **Scanner > Varredura > Arquivos compactados > Todos os tipos de arquivamento** e confirme a janela com **OK**.
- Inicie uma varredura de todas as unidades locais.
- Inicie o computador no Modo Normal.
- Realize uma varredura no Modo Normal.
- Se nenhum outro vírus ou malware for encontrado, ative a Restauração do Sistema se estiver disponível e for posasível utilizá-la.

O status do ícone de bandeja está desativado.

Motivo: o Avira Real-Time Protection está desativado.

- No Centro de Controle, clique em **Status** e ative o **Real-Time Protection** na área *Proteção do PC*.

-OU-

- Abra o menu de contexto com um clique no botão direito do mouse no Ícone da bandeja. Clique em **Ativar o Real-Time Protection**.

Motivo: o Avira Real-Time Protection está bloqueado por um firewall.

- Defina uma aprovação geral para o Avira Real-Time Protection na configuração do firewall. O Avira Real-Time Protection funciona somente com o endereço 127.0.0.1 (host local). Uma conexão com a Internet não está estabelecida. O mesmo se aplica ao Avira Mail Protection.

Caso contrário:

- Verifique o tipo de partida do serviço Avira Real-Time 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 (no Windows XP o applet de serviços está localizado no subdiretório *Ferramentas Administrativas*). Localize a entrada *Avira Real-Time Protection*. `Automático` deve ser inserido como o tipo de inicialização e `Iniciado` como o status. Se necessário, inicie o serviço manualmente selecionando a linha relevante e o botão **Iniciar**. Se uma mensagem de erro for exibida, verifique a exibição do evento.

O computador fica extremamente lento quando faço backup dos dados.

Motivo: durante o procedimento de backup, o Avira Real-Time Protection verifica todos os arquivos que estão sendo usados pelo procedimento de backup.

- Selecione **Real-Time Protection > Varredura > Exceções** na Configuração e insira os nomes de processo do software de backup.

Meu firewall relata o Avira Real-Time Protection e o Avira Mail Protection imediatamente após a ativação.

Motivo: A comunicação com o Avira Real-Time Protection e o Avira Mail Protection ocorre através do protocolo da Internet TCP/IP. Um firewall monitora todas as conexões através desse protocolo.

- Defina uma aprovação geral para o Avira Real-Time Protection e o Avira Mail Protection. O Avira Real-Time Protection funciona somente com o endereço 127.0.0.1 (host local). Uma conexão com a Internet não está estabelecida. O mesmo se aplica ao Avira Mail Protection.

O Avira Mail Protection não funciona.

Verifique o funcionamento correto do Avira Mail Protection com a ajuda das listas de varredura a seguir se ocorrerem problemas com o Avira Mail Protection.

Lista de varredura

- Verifique se seu cliente de e-mail estabelece conexão com o servidor via Kerberos, APOP ou RPA. No momento, esses métodos de varredura não são suportados.
- Verifique se o seu cliente de e-mail se comunica com o servidor usando SSL (também conhecido como TSL – Transport Layer Security). O Avira Mail Protection não suporta SSL e, portanto, finaliza quaisquer conexões SSL criptografadas. Se desejar usar conexões SSL criptografadas sem protegê-las com o Mail Protection, você precisará usar uma porta que não seja monitorada pelo Mail Protection para a conexão. As portas monitoradas pelo Mail Protection podem ser configuradas na configuração em **Mail Protection > Varredura**.
- O serviço do Avira Mail Protection 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 (no Windows XP o applet de serviços está localizado no subdiretório *Ferramentas Administrativas*). Localize a entrada *Avira Mail Protection*. `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 isto não funcionar, poderá ser necessário desinstalar completamente o produto Avira via **Iniciar > Configurações > Painel de Controle > Adicionar ou Remover Programas**, reiniciar o computador e, em seguida, reinstalar seu produto Avira.

Geral

As conexões POP3 criptografadas via SSL (Secure Sockets Layer, também conhecido como TLS (Transport Layer Security)) não podem ser protegidas no momento e são ignoradas.

No momento, a varredura do servidor de e-mail só é permitida através de senhas. "Kerberos" e "RPA" não são suportados no momento.

Seu produto Avira não verifica e-mails 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 há nenhuma conexão de rede disponível em uma máquina virtual (por exemplo, VMWare, PC virtual...) se o Avira FireWall foi instalado na máquina do host e o nível de segurança do Avira FireWall está definido como *médio* ou *alto*.

Se o Avira FireWall estiver instalado em um computador no qual uma máquina virtual (por exemplo, VMWare, Virtual PC etc.) também está em execução, o Avira FireWall bloqueará todas as conexões de rede para a 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 permitirá as conexões de rede.

Motivo: A máquina virtual emula uma placa de rede por meio do software. Essa emulação encapsula os pacotes de dados do sistema convidado em pacotes especiais (pacotes UDP) e os encaminha por meio de um gateway externo de volta 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 para o Centro de Controle e selecione a seção *PROTEÇÃO NA INTERNET* **> FireWall**.
- Clique no botão **Configuração**.

  A caixa de diálogo *Configuração* é exibida. Você está na seção de configuração *Regras de aplicativo*.
- 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 permite 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) é bloqueada se o nível de segurança do Avira FireWall está definido como *médio* ou *alto*.

Motivo: por padrão, todos os pacotes que não atendem às regras predefinidas são descartados. Os pacotes enviados pelo software da VPN (também conhecidos como pacotes GRE) não se enquadram em nenhuma outra categoria e, portanto, é filtrado por essas regras.

Adicione a regra **Permitir conexões VPN** nas **Regras do adaptador** do Avira FireWall Configuration. Essa regra permite todos os pacotes relacionados a VPN.

Um e-mail enviado através de uma conexão TLS foi bloqueado pelo Mail Protection.

Motivo: Transport Layer Security (TLS: protocolo de criptografia para a transferência de dados na Internet) não é suportado pelo Mail Protection atualmente. As seguintes opções estão disponíveis para o envio de e-mail:

- Use uma porta diferente da porta 25, que é usada pelo SMTP. Isto ignorará o monitoramento pelo Mail Protection.
- Desative a conexão TSL criptografada e desative o suporte para TSL em seu cliente de e-mail.
- Desative (temporariamente) o monitoramento de e-mails enviados pelo Mail Protection na configuração em **Mail Protection > Varredura**.

O Webchat não está operacional: As mensagens de bate-papo não são exibidas; os dados estão sendo carregados no navegador.

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

Motivo: O Web Protection verifica os dados enviados completamente em busca de vírus e programas indesejados primeiro, antes que os dados sejam carregados no navegador da web. Durante uma transferência de dados com ‘transfer-encoding: chunked’, o Web Protection não consegue determinar o tamanho da mensagem nem o volume de dados.

- Insira a configuração da URL dos bate-papos da web como uma exceção (consulte Configuração: **Web Protection > Varredura > Exceções**).

12.2 Atalhos

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

A seguir há uma visão geral dos comandos do teclado disponíveis. Mais informações sobre a funcionalidade estão disponíveis no capítulo correspondente da ajuda.

12.2.1 Nas caixas de diálogo

Atalho	Descrição
Ctrl + Tab **Ctrl + Page down**	Navegação no Centro de Controle Ir para a próxima seção.
Ctrl + Shift + Tab **Ctrl + Page up**	Navegação no Centro de Controle Ir para seção anterior.

←↑→↓	Navegação nas seções de configuração Primeiro, use o mouse para definir o foco em uma seção de configuração. Alternar entre as opções de uma lista suspensa marcada ou entre várias opções de um grupo de opções.
Tab	Altera para a opção ou grupo de opções seguinte.
Shift + Tab	Alterar para a opção ou o grupo de opções anterior.
Espaço	Ativar ou desativar uma caixa de seleção, se a opção ativa for uma caixa de seleção.
Alt + letra sublinhada	Selecionar a opção ou iniciar o comando.
Alt + ↓ **F4**	Abrir a lista suspensa selecionada.
Esc	Fechar a lista suspensa selecionada. Cancelar o comando e fechar diálogo.
Enter	Inicia o comando para a opção ou o botão ativo.

12.2.2 Na ajuda

Atalho	Descrição
Alt + Espaço	Exibir menu do sistema.
Alt + Tab	Alternar entre a ajuda e as outras janelas abertas.
Alt + F4	Fechar a ajuda.
Shift + F10	Exibir o menu contextual da ajuda.

Ctrl + Tab	Ir para a próxima seção na janela de navegação.
Ctrl + Shift + Tab	Ir para a seção anterior na janela de navegação.
Page up	Mudar para o assunto, que é exibido acima no conteúdo, no índice ou na lista de resultados de pesquisa.
Page down	Mudar para o assunto, que é exibido abaixo no conteúdo atual, no índice ou na lista de resultados de pesquisa.
Page up **Page down**	Navegar por um assunto.

12.2.3 No Centro de controle

Geral

Atalho	Descrição
F1	Exibir ajuda
Alt + F4	Fechar o Centro de controle
F5	Atualizar
F8	Abrir 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	Verificar novamente o objeto
F3	Restaurar objeto
F4	Enviar objeto
F6	Restaurar objeto para...
Voltar	Propriedades
Ins	Adicionar arquivo

Del	Excluir objeto

Seção Agendamiento

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)

12.3 Central de Segurança do Windows

- Windows XP Service Pack 2 -

12.3.1 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.

12.3.2 A Central de Segurança do Windows e o produto da sua Avira

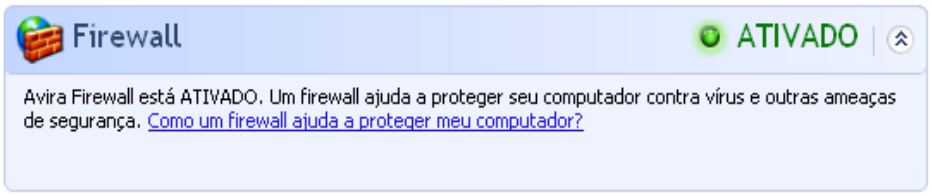
FireWall

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

- Firewall ATIVO / Firewall ativado
- Firewall INATIVO / Firewall desativado

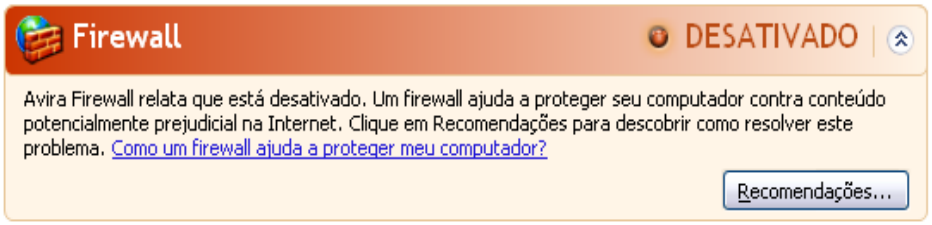
Firewall ATIVO / Firewall ativado

Após instalar o produto da sua Avira e desativar o firewall do Windows, você receberá a seguinte mensagem:



Firewall INATIVO / Firewall desativado

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



Observação
Você pode ativar ou desativar o FireWall de Avira através da guia de Status no Centro de Controle.

Advertência
Se você desativar o FireWall de Avira, usuários não autorizados podem obter acesso ao seu computador através de uma rede ou na Internet.

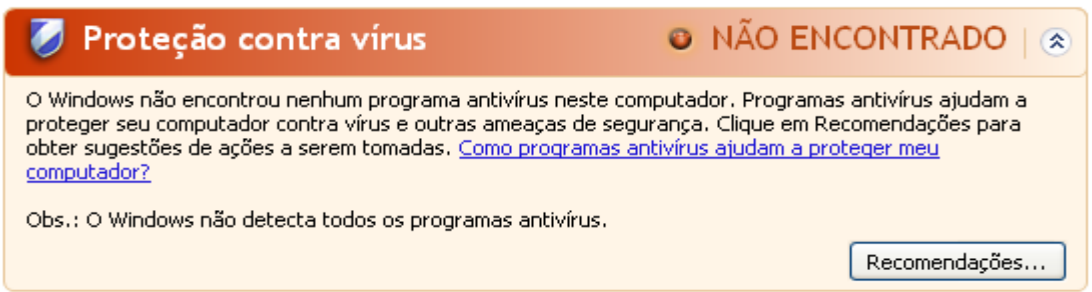
Software de proteção contra vírus/Proteção contra software malicioso

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

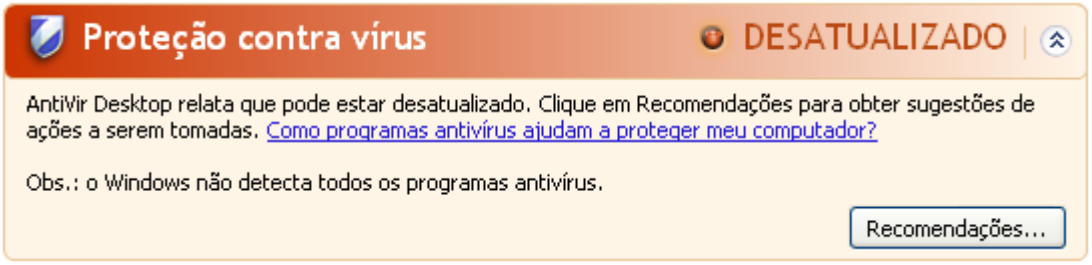
Essas informações aparecem quando a Central de segurança do Windows não encontra nenhum software antivírus em seu computador.



Observação
Instale seu produto Avira no seu computador para proteção contra vírus e outros programas indesejados!

Proteção contra vírus DESATUALIZADA

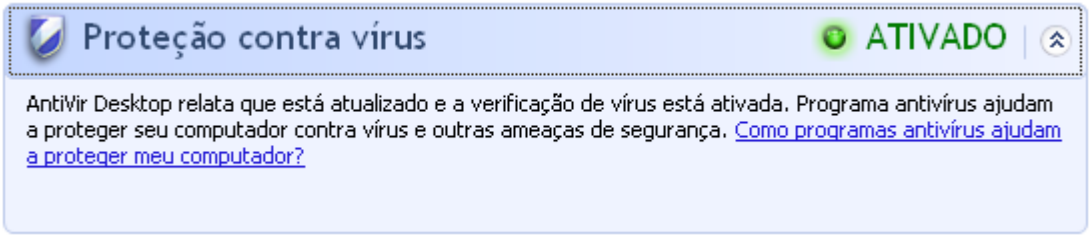
Se você já tiver instalado o Windows XP Service Pack 2 e então instalar o produto Avira, ou instalar o Windows XP Service Pack 2 em um sistema o qual o Avira já estiver instalado, você receberá a seguinte mensagem:



Observação
Para que o Centro de Segurança do Windows reconheça seu produto Avira como atualizado, deverá ser feita uma atualização após a instalação Atualize o sistema executando uma atualização.

Proteção contra vírus ATIVADA

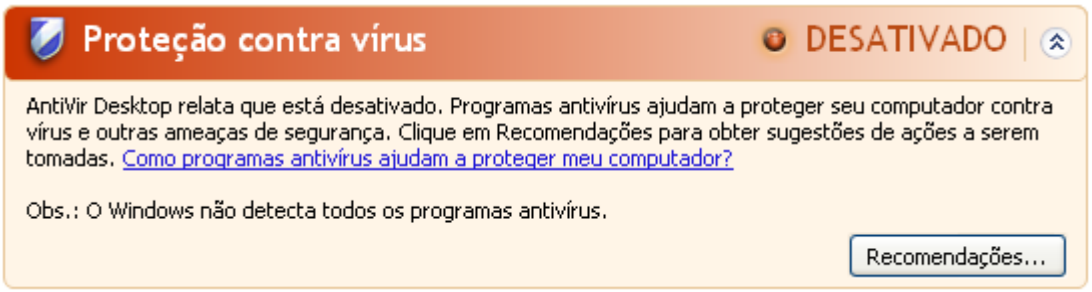
Após instalar seu produto Avira e efetuar a atualização subsequente, você receberá a seguinte mensagem:



O seu produto Avira agora está atualizado e o Avira Real-Time Protection está ativado.

Proteção contra vírus DESATIVADA

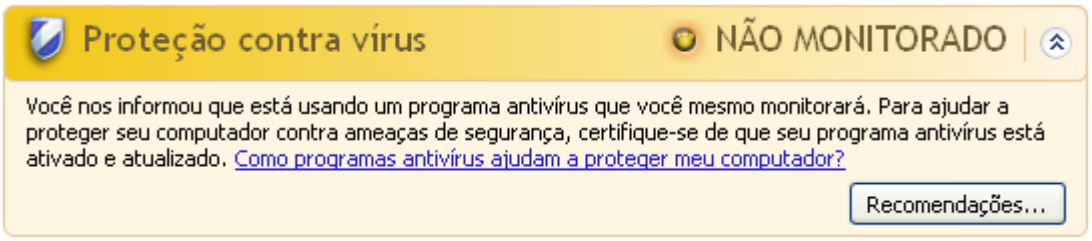
Você receberá a mensagem a seguir se desativar o Avira Real-Time Protection ou parar o serviço Real-Time Protection.



Observação
Você pode ativar ou desativar o Avira Real-Time Protection na seção de Status da **Central de Controle**. Você também pode verificar que o Avira Real-Time Protection está ativado 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
A Central de Segurança do Windows é suportada por seu produto Avira. Você pode ativar esta opção a qualquer momento por meio do botão **Recomendações**.

Observação
Mesmo se você tiver instalado o Windows XP Service Pack 2, ainda precisará de uma solução de proteção contra vírus. Embora o Windows 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!

12.4 Central de Ações do Windows

- Windows 7 e Windows 8 -

12.4.1 Geral

> **Nota:**
> A partir do Windows 7 a **Central de Segurança do Windows** foi renomeado para **Central de Ações do Windows**. Nesta seção você localizará o status de todas as opções de segurança.

A Central de Ações do Windows verifica o status do computador com relação a importantes aspectos de segurança. Pode ser acessada diretamente clicando na bandeirinha na barra de tarefas ou em **Painel de Controle > Central de Ações**.

Se algum problema for detectado em um desses pontos importantes (por exemplo, um programa antivírus desatualizado), a Central de Ações emitirá um alerta e fará recomendações sobre como proteger melhor seu computador. Isto significa que, se tudo funcionar corretamente, não serão exibidas mensagens. O status de segurança do computador pode ser observado no **Central de Ações do Windows**, no item **Segurança**. A **Central de Ações do Windows** também oferece a opção de gerenciar os programas instalados e escolher entre eles (por exemplo, *Ver programas antispyware instalados*).

Você pode até mesmo desativar as mensagens de aviso em **Alterar Configurações da Central de Ações** (por exemplo, *Desativar mensagens sobre o spyware e a proteção relacionada*).

12.4.2 A Central de Ações do Windows e seu produto Avira

Firewall de rede

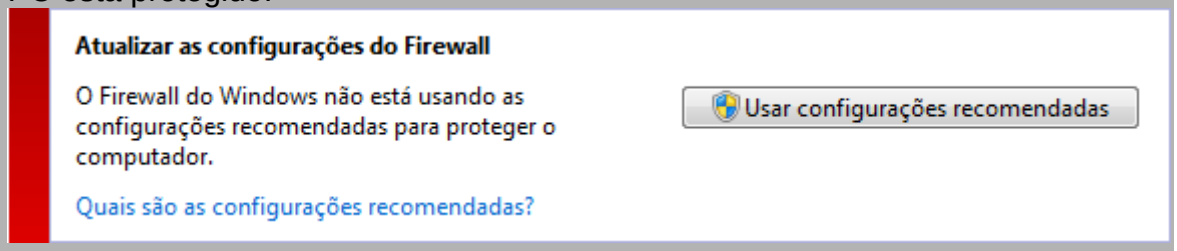
Você poderá receber as seguintes informações do **Central de Ações do Windows** com relação ao seu firewall:

- O Avira FireWall relata que está ligado
- O Firewall do Windows e o Avira FireWall relatam que estão desligados.
- Firewall do Windows está desativado ou configurado incorretamente

O Avira FireWall relata que está ligado

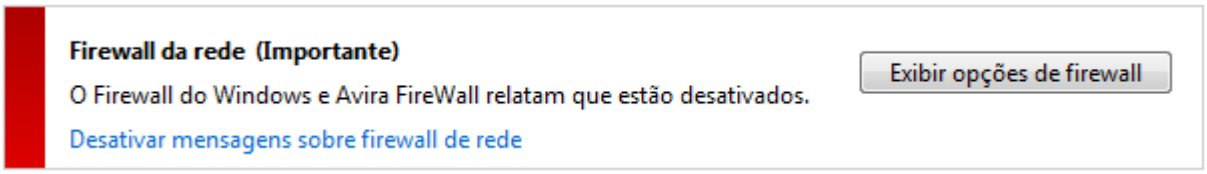
Após instalar o produto Avira e desativar o Firewall do Windows, você verá a seguinte mensagem em **Central de Ações > Segurança > Firewall de rede**: *O Avira FireWall relata que está ativado*. Isso significa que você escolheu o Avira FireWall como a sua solução de firewall. (Observe a diferença entre Firewall do Windows e Avira FireWall, com W maiúsculo).

Aviso
Na seleção **Painel de Controle > Firewall do Windows** o **único produtp referenciado é o Firewall do Windows e não o Avira FireWall**. Esse é o motivo pelo qual tudo será marcado em vermelho com a mensagem: *Atualizar suas configurações de Firewall* e ***Firewall do Windows não está usando as configurações recomendadas para proteger seu computador***. Não é necessário fazer nada, o produto Avira está funcionando perfeitamente e o seu PC está protegido.



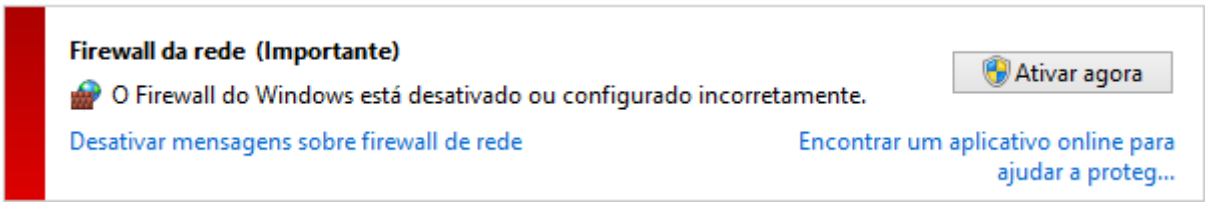
O Firewall do Windows e o Avira FireWall relatam que estão desligados

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



Aviso
Se você desativar o Avira FireWall, usuários não autorizados poderão ter acesso ao seu computador através de uma rede ou da Internet.

Firewall do Windows está desativado ou configurado incorretamente



Isto significa que nem o firewall do Windows nem o Avira estão ativados. Você pode receber esta mensagem em duas situações diferentes:

- **Avira FireWall**

  O Avira FireWall está configurado incorretamente ou não foi instalado corretamente. O Avira FireWall deve ser detectado imediatamente pela Central de Ações do Windows. Tente reinicializar o computador e, se isso não funcionar, instale novamente o Avira.

- **Firewall do Windows**

  A partir do Windows 7, Avira Professional Security dá a opção de gerenciar diretamente o Firewall do Windows a partir do Centro de Controle e Configuração Avira.

Proteção contra vírus

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

- O Avira Desktop relata que está atualizado e a verificação de vírus está ativada.
- O Avira Desktop relata que está ativado.
- O Avira Desktop relata que está desatualizado.
- O Windows não localizou software antivírus neste computador.
- O Avira Desktop expirou.

O Avira Desktop relata que está atualizado e a verificação de vírus está ativada

Após a instalação de seu produto Avira e uma atualização subsequente, você não receberá nenhuma mensagem da Central de Ações do Windows. Mas, se você acessar **Central de Ações > Segurança**, poderá ver: *O Avira Desktop relata que ele está atualizado e a verificação de vírus está ativada.* Isso significa que o produto Avira agora está atualizado e o Avira Real-Time Protection está ativado.

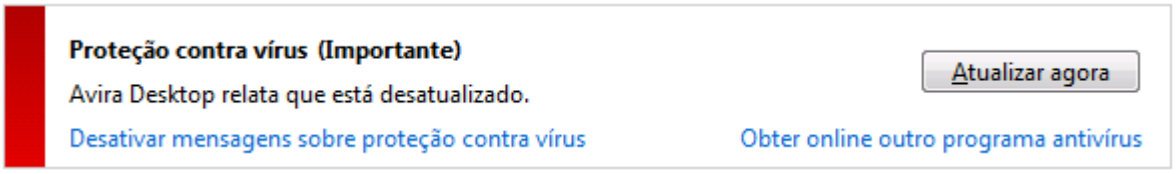
O Avira Desktop relata que está desativado

Você recebe a mensagem a seguir se desativar o Avira Real-Time Protection ou parar o serviço Real-Time Protection.

Nota
O Avira Real-Time Protection pode ser ativado ou desativado na seção **Status** do **Centro de Controle Avira**. Você também pode verificar que o Avira Real-Time Protection está ativado com o guarda-chuva vermelho aberto na barra de tarefas. Também é possível ativar o produto Avira clicando no botão *Ativar agora* na mensagem da Central de Ações do Windows. Você receberá uma notificação solicitando sua permissão para executar o Avira. Clique em *Sim, eu confio no Editor e desejo executar este programa* e o Real-Time Protection será ativado novamente.

O Avira Desktop relata que está desatualizado

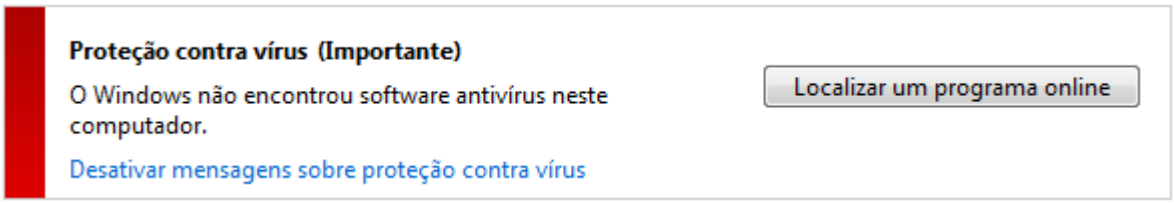
Se você acabou de instalar o Avira ou se por algum motivo o arquivo de definição de vírus, o mecanismo de varredura ou os arquivos de programa do produto Avira não foram atualizados automaticamente (por exemplo, se foi feita uma atualização de um sistema operacional Windows mais antigo, no qual o produto Avira já está instalado) você receberá a seguinte mensagem:



Observação
Para que a Central de Ações do Windows reconheça seu produto Avira como atualizado, uma atualização deverá ser executada após a instalação. Atualize seu Produto Avira executando uma atualização.

O Windows não localizou software antivírus neste computador

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



Nota
Observe que esta opção não aparece no Windows 8, pois o Windows Defender agora também é a função de proteção de vírus predefinida.

Observação
Instale o produto Avira em seu computador para protegê-lo contra vírus e outros programas indesejados!

O Avira Desktop expirou

Essas informações da Central de Ações do Windows aparecem quando a licença do produto Avira expirou.
Se você clicar no botão **Renovar a assinatura** será redirecionado para um site da Avira, onde poderá comprar uma nova licença.

Nota
Observe que essa opção está disponível somente para o Windows 8.

Spyware e proteção contra software indesejado

Você poderá receber as seguintes informações da Central de Ações do Windows com relação à sua proteção contra spyware:

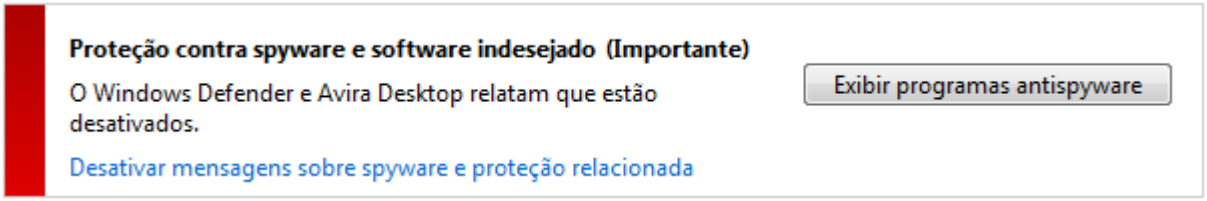
- O Avira Desktop relata que está ativado.
- O Windows Defender e o Avira Desktop relatam que estão desativados.
- O Avira Desktop relata que está desatualizado.
- O Windows Defender está desligado.
- O Windows Defender está desligado.

O Avira Desktop relata que está ativado

Após a instalação do produto Avira e uma atualização subsequente, você não receberá nenhuma mensagem da Central de Ações do Windows. Mas, se você acessar **Central de Ações > Segurança**, poderá ver: *O Avira Desktop relata que ele está ativado*. Isso significa que o produto Avira agora está atualizado e o Avira Real-Time Protection está ativado.

O Windows Defender e o Avira Desktop relatam que estão desativados

Você recebe a mensagem a seguir se desativar o Avira Real-Time Protection ou parar o serviço Real-Time Protection.

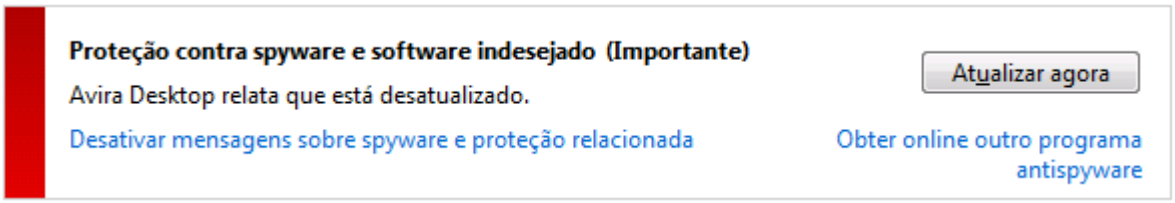


Nota
O Avira Real-Time Protection pode ser ativado ou desativado na seção **Status** do **Centro de Controle Avira**. Você também pode verificar que o Avira Real-Time Protection está ativado com o guarda-chuva vermelho aberto na barra de

tarefas. Também é possível ativar o produto Avira clicando no botão *Ativar agora* na mensagem da Central de Ações do Windows. Você receberá uma notificação solicitando sua permissão para executar o Avira. Clique em *Sim, eu confio no Editor e desejo executar este programa* e o Real-Time Protection será ativado novamente.

O Avira Desktop relata que está desatualizado

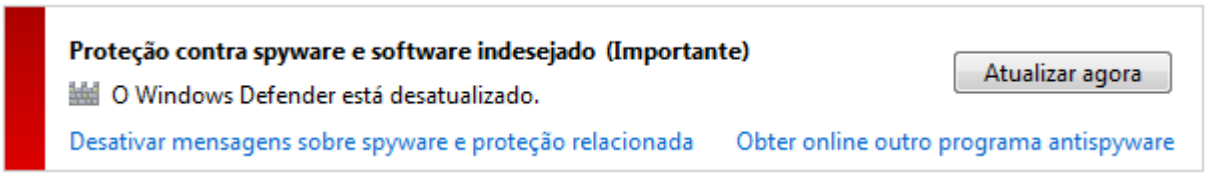
Se você acabou de instalar o Avira ou se por algum motivo o arquivo de definição de vírus, o mecanismo de varredura ou os arquivos de programa do produto Avira não foram atualizados automaticamente (por exemplo, se foi feita uma atualização de um sistema operacional Windows mais antigo, no qual o produto Avira já está instalado) você receberá a seguinte mensagem:



Observação
Para que a Central de Ações do Windows reconheça seu produto Avira como atualizado, uma atualização deverá ser executada após a instalação. Atualize seu Produto Avira executando uma atualização.

O Windows Defender está desatualizado

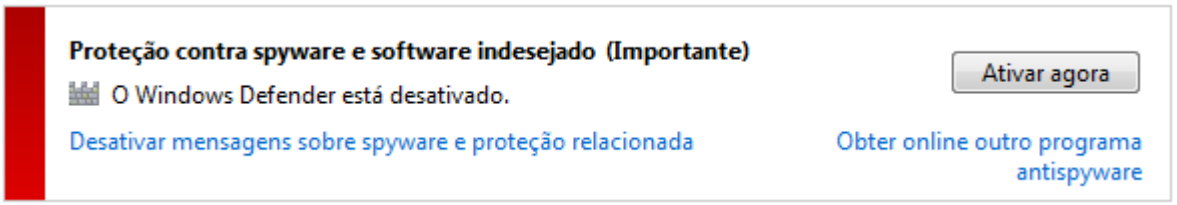
Você pode receber a mensagem a seguir se o Windows Defender estiver ativado. Se já tiver instalado o produto Avira, esta mensagem não deve ser exibida. Verifique se a instalação ocorreu corretamente.



Nota
O Windows Defender é a solução predefinida de proteção contra vírus e spyware do Windows.

O Windows Defender está desligado

Essas informações da Central de Ações do Windows aparecem quando a Central de Ações do Windows não encontrar nenhum outro software antivírus no computador além daquele que o sistema operacional integra por padrão: Windows Defender. Se você tiver algum software antivírus instalado anteriormente em seu computador, este aplicativo foi desativado. Se você já tiver instalado o produto Avira, esta mensagem não deverá ser exibida: O Avira deve ser detectado automaticamente. Verifique se a instalação ocorreu corretamente.



13. Vírus e mais

Avira Professional Security não somente detecta vírus e malware, como também protege de outras ameaças. Neste capítulo é possível obter uma visão geral dos diferentes tipos de malware e outras ameaças, descrevendo suas práticas, seus comportamentos e as surpresas desagradáveis que elas reservam para você.

Tópicos relacionados:

- Categorias de ameaça
- Vírus e outros malwares

13.1 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 detecta Adware. Se a opção **Adware** estiver ativada com um visto na configuração em Categorias de ameaça, você receberá um alerta correspondente se seu produto Avira detectar 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.

Seu produto Avira reconhece "Adware/Spyware". Se a opção **Adware/Spyware** estiver ativada com um visto na configuração em Categorias de ameaça, você receberá um alerta correspondente se seu produto Avira detectar adware ou spyware.

Aplicativos

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

Seu produto Avira reconhece "Aplicativo (APPL)". Se a opção **Aplicativo** estiver ativada com um visto na configuração em Categorias de ameaça, você receberá um alerta correspondente se seu produto Avira detectar tal comportamento.

Clientes backdoor

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

Seu produto Avira reconhece "Software de controle de backdoor". Se a opção **Software de controle de backdoor** estiver ativada com um visto na configuração em Categorias de ameaça, você receberá um alerta correspondente se seu produto Avira detectar tal 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 está 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 no 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 com a operadora de telefone para solicitar o bloqueio dessa faixa de números para que seja protegido imediatamente contra discadores indesejados (discadores 0190/0900).

Seu produto Avira pode detectar os discadores familiares por padrão.

Se a opção **Discadores** estiver ativada com um visto 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.

Seu produto Avira reconhece "Arquivos com extensão dupla". Se a opção **Arquivos com extensão dupla** estiver ativada com um visto na configuração em Categorias de ameaça, você receberá um alerta correspondente se seu produto Avira detetar tais arquivos.

Software fraudulento

Também conhecido como "scareware" ou "rogueware", ele é um software fraudulento que deseja que seu computador seja infectado por vírus ou malware. Este software se parece enganosamente com um software Antivírus profissional, mas seu objetivo é provocar incertezas ou assustar 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 detecta scareware. Se a opção **Software Fraudulento** estiver ativada com um visto na configuração Categorias de ameaça, você receberá um alerta correspondente se seu produto Avira detectar tais 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. Jogos por e-mail também se tornaram mais populares: inúmeras variações estão circulando, variando desde simples jogo de xadrez até "treinamentos de tropas" (incluindo combates de torpedo): Os movimentos correspondentes são enviados aos parceiros via programas de e-mail, os quais respondem.

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.

Seu produto Avira reconhece jogos de computador. Se a opção **Jogos** estiver ativada com um visto na configuração em Categorias de ameaça, você receberá um alerta correspondente se seu 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 Tróia. 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, seu produto Avira pode detectar programas de piada e eliminá-los como programas indesejados se necessário. Se a opção **Piadas** estiver ativada com um visto na configuração em Categorias de ameaça, um alerta correspondente será emitido 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 registros.
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.

Seu produto Avira reconhece "Phishing". Se a opção **Phishing** estiver ativada com um visto na configuração em Categorias de ameaça, você receberá um alerta correspondente se seu produto Avira detectar tal comportamento.

Programas que violam o domínio privado

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

Seu produto Avira detecta o software "Security Privacy Risk". Se a opção **Programas que violam o domínio privado** estiver ativada com um visto na configuração em Categorias de ameaça, você receberá um alerta correspondente se seu produto Avira detectar tal software.

Compactadores de tempo de execução incomuns

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

Seu produto Avira reconhece "Compactadores de tempo de execução incomuns". Se a opção **Compactadores de tempo de execução incomuns** estiver ativada com um visto na configuração em Categorias de ameaça, você receberá um alerta correspondente se seu produto Avira detectar tais compactadores.

13.2 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 enganando os mecanismos de segurança de acesso do computador.

Um programa que está sendo executado em segundo plano geralmente concede ao invasor direitos quase ilimitados. Os dados pessoais do usuário podem ser vistos com a ajuda de um backdoor. Mas 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 piores consequências: o sistema do computador não pode mais ser carregado...

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 Tróia) executados sob um comando e uma infraestrutura de controle comuns. Os Boot-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 a dimensão de milhares de computadores e a soma de suas larguras de banda sobrecarrega 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 de uma vulnerabilidade que leva ao escalamento de privilégios ou à negação de serviço em um sistema de computador. Por exemplo, um tipo de exploit são ataques a partir da Internet com a ajuda de pacotes de dados manipulados. Os programas podem ser infiltrados para obter acesso de nível mais alto.

Software fraudulento

Também conhecido como "scareware" ou "rogueware", ele é um software fraudulento que deseja que seu computador seja infectado por vírus ou malware. Este software se parece enganosamente com um software Antivírus profissional, mas seu objetivo é provocar incertezas ou assustar 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 por email com a solicitação para 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 os pontos de 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 da Web 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 específica de um sistema é realizada com a ajuda de um cavalo de Tróia ou vírus. O resultado disso é que o sistema agora só poderá 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 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 Tróia. 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 software que são instaladas após o sistema do computador ser invadido para dissimular logons do invasor, ocultar processos e registrar dados – em outras palavras: torná-los invisíveis. Eles tentam atualizar programas espiões 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 chamada 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 não podem 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 Tróia (abreviação: Tróias)

Os cavalos de Tróia são bastante comuns hoje em dia. Eles 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 Tróia 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 Tróia. 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 Tróia 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. Sob comando, o computador afetado inicia, por exemplo, ataques DoS (Negação de Serviço) ou envia spam e emails de phishing.

14. Informações e Serviço

Este capítulo contém informações sobre Informações e Serviços do Avira.

- Endereço de Contato
- Suporte Técnico
- Arquivo Suspeito
- Relatando Falso-Positivos
- Seus comentários para mais segurança

14.1 Endereço de Contato

Se você tiver qualquer dúvida ou solicitação relacionada à gama de produtos Avira, teremos o prazer em ajudá-lo. Para obter nossos endereços de contato, consulte o Centro de controle em **Ajuda > Sobre o Avira Professional Security**.

14.2 Suporte Técnico

O suporte do 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**. Você pode localizar estas informações na interface do programa no item de menu **Ajuda > Sobre o Avira Professional Security > Informações de Licença**. Consulte Informações de Licença.
- **Informações da versão**. Você pode localizar estas informações na interface do programa, no item de menu **Ajuda > Sobre o Avira Professional Security > Inormações da Versão**. Consulte Informações da Versão.
- **Versão do sistema operacional** e quaisquer Service Packs instalados.
- **Pacotes de software instalados**, por exemplo, software antivírus de outros fornecedores.
- **Mensagens exatas** do programa ou do arquivo de relatório.

14.3 Arquivo Suspeito

Arquivos suspeitos ou vírus que podem não ter sido detectados ou removidos ainda por nossos produtos podem ser enviados para nós. Fornecemos várias maneiras para fazer isso.

- Identifique o arquivo no gerenciador de quarentena do Centro de controle do Avira Server Security Console e selecione o item **Enviar arquivo** por meio do menu contextual ou do botão correspondente.
- Envie o arquivo requerido compactado (WinZIP, PKZip, Arj, etc.) no anexo de um email para o seguinte endereço:
  virus-professional-pt-br@avira.com
  Como alguns gateways de e-mail funcionam com software antivírus, você também deve fornecer ao(s) arquivo(s) uma senha (lembre-se de nos informar a senha).
- Você também pode nos enviar o arquivo suspeito através de nosso site:
  http://www.avira.com/pt-br/sample-upload

14.4 Relatando Falso-Positivos

Se achar que o Avira Professional Security esteja relatando uma detecção em um arquivo que está mais provavelmente "limpo", envie o arquivo relevante compactado (WinZIP, PKZip, Arj, etc.) como um anexo de e-mail para o seguinte endereço:

virus-professional-pt-br@avira.com

Como alguns gateways de e-mail funcionam com software antivírus, você também deve fornecer ao(s) arquivo(s) uma senha (lembre-se de nos informar a senha).

14.5 Seus comentários para mais segurança

No Avira, a segurança de nossos clientes é superior. Por este motivo, nós não apenas temos uma equipe de especialistas interna que testa a qualidade e a segurança de cada solução Avira antes de o produto ser lançado. Também damos grande importância às indicações relacionadas a lacunas relevantes na segurança que poderiam se desenvolver e tratamos isso com seriedade.

Se você achar que detectou uma lacuna na segurança de um de nossos produtos, envie-nos um e-mail para os endereços a seguir:

vulnerabilities-professional-pt-br@avira.com

Avira

Edição Q4-2013.

Avira | Kaplaneiweg 1 | 88069 Tettnang | Alemanha | Telefone: +49 7542-500 0
www.avira.com/pt-br