Avira Internet Security

Manual do usuário

AVIRA

Marcas Registradas e Copyright

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 Internet Security. Agradecemos os detentores dos direitos autorais por disponibilizar o código para nós. Para obter informações detalhadas sobre copyright, consulte "Licenças de Terceiros" na Ajuda do Programa do Avira Internet Security.

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 Vista 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
- Avira SearchFree Toolbar, uma barra de ferramentas de procura integrada no navegador da web que fornece opções de procura rápidas e convenientes. Também inclui widgets das funções da Internet mais comuns.
- Web Protection para monitorar dados e arquivos transferidos da Internet usando o protocolo HTTP (monitoramento das portas 80, 8080, 3128)
- Componente de controle dos pais para filtragem baseada em função de sites indesejados e limitação de uso da Internet.
- O aplicativo Avira Free Android Security não está somente focado em medidas antirroubo. O aplicativo ajuda a recuperar o seu dispositivo móvel em caso de perda, ou pior, em caso de furto. Além disso, o aplicativo permite bloquear chamadas recebidas ou SMS. O Avira Free Android Security protege celulares e smartphones com o sistema operacional Android.
- Componente Backup para criar backups de seus dados (backups espelhados)
- 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
- 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

Os requisitos do sistema são os seguintes:

- Computador com processador Pentium ou superior de pelo menos 1 GHz
- Sistema operacional
  - Windows XP, SP mais recente (32 ou 64 bits) ou
  - Windows 7, SP mais recente (32 ou 64 bits)

> **Observação**
> Avira Internet Security está em processo de certificação para o Windows 8.

- Pelo menos 150 MB de espaço livre de memória em disco (mais se estiver usando a quarentena para armazenamento temporário)
- Pelo menos 512 MB de RAM no Windows XP
- Pelo menos 1024 MB de RAM no Windows 7
- Para a instalação do programa: Direitos de administrador
- Para todas as instalações: Windows Internet Explorer 6.0 ou superior
- Conexão com a Internet se apropriado (consulte Instalação)

Avira SearchFree Toolbar

- Sistema operacional
  - Windows XP, SP mais recente (32 ou 64 bits) ou
  - Windows 7, SP mais recente (32 ou 64 bits)
- Navegador da Web
  - Windows Internet Explorer 6.0 ou superior
  - Mozilla Firefox 3.0 ou superior
  - Google Chrome 18.0 ou superior

> **Observação**
> Se necessário, desinstale quaisquer barras de ferramenta de procura instaladas anteriormente antes de instalar o Avira SearchFree Toolbar. Caso contrário, você não conseguirá instalar o Avira SearchFree Toolbar.

Informações para usuários 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 esse motivo, a Microsoft está lançando o "Controle de Conta de Usuário" no Windows Vista. Isto oferece mais proteção para usuários que estão com logon efetuado como administradores: deste modo, no Windows Vista, um administrador tem apenas privilégios de um usuário final inicialmente. As ações para as quais os direitos de administrador são necessários são claramente marcadas no Windows Vista 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 somente após a obtenção dessa permissão.

O produto Avira requer direitos de administrador para algumas ações no Windows Vista. 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 Controle de Conta de Usuário do Windows Vista solicitará a inserção da senha de administrador. Se você não tiver uma senha de administrador, não poderá realizar essa ação.

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 fornecida na forma de um código de ativação. O código de ativação é um código formado por letras e números que você receberá após adquirir o produto Avira. O código de ativação contém os dados exatos de sua licença, isto é, os programas que foram licenciados e por quanto tempo.

O código de ativação será enviado para você por e-mail, se você tiver adquirido seu produto Avira na Internet ou ele será indicado na embalagem do produto.

Para licenciar seu programa, insira seu código de ativação para ativá-lo. A ativação do produto pode ser realizada durante a instalação. No entanto, você também pode ativar seu produto Avira após a instalação no Gerenciador de Licença, em **Ajuda > Gerenciamento de licenças**.

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. No entanto, também é possível estender a licença do seu produto Avira por meio do Gerenciador de licença em **Ajuda > Gerencimento de licença**

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.

2.3.3 Atualização

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

Para atingir alta confiabilidade e segurança para seu computador, o Avira envia um item pop-up para lembrar você para atualizar o sistema para a versão mais recente. Apenas clique no link **Atualizar** no item pop-up e você será guiado até o site de atualização específico do produto.

Você tem a possibilidade de atualizar seu produto atual ou pode obter um produto mais abrangente. A página de visão geral do produto mostra qual tipo de produto você está usando no momento e oferece a chance de comparar seu produto com outros produtos Avira. Se precisar de mais informações, clique no ícone **Informações** ao lado do nome do produto. Se desejar permanecer com o mesmo produto, clique em **Atualizar** e o download da nova versão iniciará imediatamente. Se desejar obter um produto mais abrangente, clique no botão **Comprar** na parte inferior da coluna do produto. Você será encaminhado automaticamente para a loja on-line da Avira, onde poderá efetuar o pedido de compra.

> **Nota**
> Dependendo do seu produto e sistema operacional, pode ser necessário ter direitos de administrador para executar a atualização. Efetue logon como um administrador antes de realizar uma atualização.

2.3.4 Gerenciador de licença

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

Gerenciador de Licença do Avira Internet 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 Internet 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 e desinstalação do produto Avira.

- consulte o Capítulo: Pré-Instalação: Requisitos, preparando o computador para instalação
- consulte o Capítulo: Instalação Expressa: Instalação padrão de acordo com as configurações padrão
- consulte o Capítulo: Instalação Personalizada: Instalação configurável
- consulte o Capítulo: Instalação do Produto de Teste
- consulte o Capítulo: Assistente de Configuração
- consulte o Capítulo: Alterar Instalação
- consulte o Capítulo: Módulos de instalação
- consulte o Capítulo: Desinstalação: Desinstalar

3.1 Tipos de Instalação

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

Expressa

- Os componentes padrão serão instalados.
- Os arquivos do programa são instalados em uma pasta padrão em *C:\Arquivos de Programas*.
- Seu produto Avira será instalado com as configurações padrão. Você tem a opção de definir configurações personalizadas usando o assistente de configuração.

Personalizar

- Você pode optar por instalar componentes individuais do programa (consulte o Capítulo Instalação e Desinstalação > Módulos de Instalação).
- Uma pasta de destino pode ser selecionada para os arquivos de programa a serem instalados.
- Você pode desativar **Criar um ícone na área de trabalho** e **grupo de programas** no menu **Iniciar**.
- Utilizando o assistente de configuração, você pode definir configurações personalizadas para o produto Avira e iniciar uma varredura rápida do sistema que é executada automaticamente após a instalação.

3.2 Pré-Instalação

Observação
Antes da instalação, verifique se seu computador preenche todos os requisitos mínimos do sistema. Se seu computador satisfizer todos os requisitos, você poderá instalar o produto Avira.

Pré-Instalação

✓ Feche seu programa de e-mail. Também é recomendável encerrar todos os aplicativos em execução.
✓ Verifique se nenhuma outra solução de proteção contra vírus está instalada. As funções de proteção automática de várias soluções de segurança podem interferir umas na outras.

↳ O produto Avira procurará qualquer software incompatível possível em seu computador.

↳ Se software potencialmente incompatível for detectado, o Avira 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**.

▸ Você deve confirmar manualmente a desinstalação de alguns programas. Selecione os programas e clique em **Avançar**.

↳ A desinstalação de um ou mais dos programas selecionados requer uma reinicialização do computador. Após a reinicialização, a instalação continuará.

Aviso
Seu computador não estará protegido até que a instalação do produto Avira seja concluída.

Instalação

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

Os botões mais importantes têm as seguintes funções:

- **OK**: Confirmar ação.
- **Anular**: Anular ação.
- **Avançar**: Ir para a próxima etapa.

- **Voltar**: Ir para a etapa anterior.

  - Estabeleça uma conexão com a Internet: A conexão com a Internet é necessária para realizar as seguintes etapas de instalação:
    - Download do arquivo 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
    - Quando apropriado, realizar uma atualização após a conclusão da instalação
  - Mantenha o código de ativação ou arquivo de licença para seu produto Avira acessível quando desejar ativar o programa.

Observação
Instalação baseada na Internet:
Para a instalação baseada na Internet do programa, um programa de instalação é fornecido, o qual carrega o arquivo do programa atual antes da instalação pelos servidores da web do Avira. Esse processo assegura que o produto Avira seja instalado com o arquivo de definição de vírus mais recente.

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

Nota
Para ativação do produto, o produto Avira usa o protocolo HTTP e a Porta 80 (comunicação na web), bem como o protocolo de criptografia SSL e a porta 443 para comunicação 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 estão bloqueados pelo firewall.

3.3 Instalação Expressa

Instalando seu produto Avira:

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

Instalação baseada na Internet

↳ A tela **Bem-vindo** é exibida.

- Clique em **Avançar** para continuar a instalação.
  - ↪ É exibido o diálogo **Seleção de Idioma**.
- Selecione o idioma que deseja usar para instalar seu produto Avira e confirme sua seleção de idioma clicando em **Avançar**.
  - ↪ É exibida a caixa de diálogo **Download**. Todos os arquivos necessários para instalação são baixados dos servidores da web do Avira. A janela **Download** fecha após a conclusão do download.

Instalação com um pacote de instalação

- ↪ É exibida a janela **Preparando a Instalação**.
- ↪ O arquivo de instalação é extraído. A rotina de instalação é iniciada.
- ↪ É exibida a caixa de diálogo **Escolher o tipo de instalação**.

Observação
A Instalação Expressa está predefinida como padrão. Todos os componentes padrão serão instalados, os quais não podem ser configurados. Para executar uma instalação personalizada, consulte o capítulo: Instalação e desinstalação > Instalação personalizada.

- A caixa de seleção **Quero melhorar a minha proteção usando o Avira ProActiv e o Protection Cloud** (Configuração > Geral > Proteção avançada) está predefinida como padrão. Se não desejar participar da Comunidade do Avira, desmarque esta caixa de seleção.
  - ↪ Se você confirmar sua participação na Comunidade do Avira, a Avira 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 **EULA**.
  - ↪ O **Assistente de licença** é aberto e ajuda a ativar seu produto.
  - ↪ Ali, você tem a oportunidade de configurar um Servidor Proxy.
- Clique, se necessário, em **Configurações de proxy** para configuração e confirme suas configurações com **OK**.
- Se você já recebeu um código de ativação, selecione **Ativar o produto** e insira o código de ativação.

  -OU-
- Se você não tiver um código de ativação, clique no link **comprar um código de ativação**.

↳ Você é encaminhado para o site da Avira.

Como alternativa, clique no link **Eu já tenho um arquivo de licença válido**.

↳ A caixa de diálogo **Abrir arquivo** é exibida.

- Selecione o arquivo de licença *.KEY* e clique em **Abrir**.
  ↳ O código de ativação é copiado para o Assistente de licença.
- Para testar o produto, continue a ler no capítulo Testar a instalação do produto.
- Clique em **Avançar**.
  ↳ O progresso da instalação é exibido por uma barra verde.
- Clique em **Avançar**.
  ↳ É exibida a caixa de diálogo **Juntar-se aos milhões de usuários Avira que já usam o Avira SearchFree**.
- Se não deseja instalar o Avira SearchFree Toolbar, desmarque a caixa de seleção com o Avira SearchFree Toolbar e o Avira SearchFree Updater **Contrato de Licença do Usuário Final**, e aquela que define **Avira SearchFree (search.avira.com)** como sua home page do navegador.

Observação
Se necessário, desinstale quaisquer barras de ferramenta de procura instaladas anteriormente antes de instalar o Avira SearchFree Toolbar. Caso contrário, você não conseguirá instalar o Avira SearchFree Toolbar.

- Clique em **Avançar**.
  ↳ O progresso da instalação da Avira SearchFree Toolbar é exibido por uma barra verde.
  ↳ O Ícone de Bandeja do Avira é colocado na barra de tarefas.
  ↳ Para garantir proteção efetiva do computador, o módulo **Atualizador** verificará as atualizações possíveis.
  ↳ A janela **Luke Filewalker** abre e é realizada uma breve varredura do sistema. O status da varredura, assim como os resultados, são exibidos.
- Se, após a varredura lhe for solicitado que reinicie o computador, clique em **Sim** para assegurar que o sistema fique totalmente protegido.

Após uma instalação bem-sucedida, recomendamos verificar se o programa está atualizado no campo **Status** do Centro de Controle.

- Se o produto Avira mostrar que o computador não está protegido, clique em **Corrigir problema**.
  ↳ A caixa de diálogo **Restaurar a proteção** abre.
- Ative as opções predefinidas para maximizar a segurança do sistema.
- Se apropriado, execute posteriormente uma varredura completa do sistema.

3.4 Instalação personalizada

Instalando seu produto Avira:

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

Instalação baseada na Internet

↳ A tela **Bem-vindo** é exibida.

- Clique em **Avançar** para continuar a instalação.
  ↳ É exibido o diálogo **Seleção de Idioma**.
- Selecione o idioma que deseja usar para instalar seu produto Avira e confirme sua seleção de idioma clicando em **Avançar**.
  ↳ É exibida a caixa de diálogo **Download**. Todos os arquivos necessários para instalação são baixados dos servidores da web do Avira. A janela **Download** fecha após a conclusão do download.

Instalação com um pacote de instalação

↳ É exibida a janela **Preparando a Instalação**.

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

↳ É exibida a caixa de diálogo **Escolher o tipo de instalação**.

> **Observação**
> A Instalação Expressa está predefinida como padrão. Todos os componentes padrão serão instalados, os quais não podem ser configurados. Para executar uma instalação Expressa, consulte o capítulo: Instalação e desinstalação > Instalação Expressa.

- Selecione **Personalizado** para instalar componentes de programa individuais.
- A caixa de seleção **Quero melhorar a minha proteção usando o Avira ProActiv e o Protection Cloud** é predefinida por padrão. Se não desejar participar da Comunidade do Avira, desmarque esta caixa de seleção.
  ↳ Se você confirmar sua participação na Comunidade do Avira, a Avira 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 EULA.
- Clique em **Avançar**.

↳ A janela **Escolher a pasta de destino** é exibida.

↳ A pasta padrão será *C:\Arquivos de Programas\Avira\AntiVir Desktop*

- Clique em **Avançar** para continuar.

  -OU-

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

  ↳ O **diálogo Instalar componentes** é exibido.

- Selecione ou desmarque os componentes na lista e confirme com **Avançar** para continuar.
- Se optar por instalar o componente **Protection Cloud**, mas desejar confirmar manualmente quais arquivos devem ser enviados para a Nuvem para análise, você poderá ativar a opção **Confirmar manualmente ao enviar arquivos suspeitos para Avira**.
- Clique em **Avançar**.
- Na próxima caixa de diálogo você pode decidir se deseja criar um atalho na área de trabalho e/ou um grupo de programas no menu **Iniciar**.
- Clique em **Avançar**.

  ↳ O **Assistente de licença** é aberto.

Você tem as seguintes opções para ativar o programa:

- Insira um código de ativação.

  ↳ Inserindo seu código de ativação, o produto Avira é ativado com a licença.

- Se você não tiver um código de ativação, clique no link **comprar um código de ativação**.

  ↳ Você é encaminhado para o site da Avira.

- Selecione a opção **Testar produto**

  ↳ Se você selecionar **Testar produto** uma licença de avaliação para ativar o programa será gerada durante o processo de ativação. Você pode testar o produto Avira com todasas funções por um determinado período de tempo (consulte Instalação do Produto de Teste).

Observação
Usando a opção **eu já tenho um arquivo de licença** é possível carregar um arquivo de licença válido. Durante a ativação do produto com um código de ativação válida, a chave de licença é gerada e salva no diretório do programa do produto Avira. Use esta opção se já tiver ativado um produto e desejar reinstalar seu produto Avira.

Nota
Em algumas versões de vendas dos produtos Avira, um código de ativação já foi incluído no produto. Por esse motivo, a ativação não precisa ser inserida. Se e quando necessário, o código de ativação é exibido no assistente de licença.

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

- Selecione um processo de ativação e clique em **Avançar** para confirmar.
- Se você já possuir um arquivo de licença válido, vá diretamente para o capítulo "Selecione a opção *eu já tenho um arquivo de licença*".

Ativação do produto

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

- Insira seus dados e clique em **Avançar**.
  - ↪ Seus dados são transmitidos para os servidores do Avira e verificados. Seu produto Avira é ativado por meio de sua licença.
  - ↪ Os dados de sua licença serão exibidos na próxima janela.
- Clique em **Avançar**.
- Ignore o seguinte capítulo em "Selecione a opção *eu já tenho um arquivo de licença*".

Selecione a opção "eu já tenho um arquivo de licença"

- ↪ Uma caixa é aberta para carregar o arquivo de licença.

- Selecione o arquivo de licença *.KEY* com seus dados de licença para o programa e clique em **Abrir**.
  - ↪ Os dados de sua licença serão exibidos na próxima janela.
- Clique em **Avançar**.

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

- ↪ É exibida a caixa de diálogo **Juntar-se aos milhões de usuários Avira que já usam o Avira SearchFree**.

- Se você não deseja instalar o Avira SearchFree Toolbar, desmarque a caixa de seleção com o **Contrato de Licença do Usuário final** do Avira SearchFree Toolbar e do Avira SearchFree Updater e aquela que define **Avira SearchFree (search.avira.com)** como sua home page do navegador.

Observação Se necessário, desinstale quaisquer barras de ferramenta de procura instaladas anteriormente antes de instalar o Avira SearchFree Toolbar. Caso contrário, você não conseguirá instalar o Avira SearchFree Toolbar.

- Clique em **Avançar**.
  - ↪ O progresso da instalação da Avira SearchFree Toolbar é exibido por uma barra verde.
  - ↪ O **Assistente de instalação** é fechado e o **Assistente de configuração** será aberto.

3.5 Instalação do produto de teste

Instalando seu produto Avira:

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

Instalação baseada na Internet

- ↪ A tela **Bem-vindo** é exibida.

- Clique em **Avançar** para continuar a instalação.
  - ↪ É exibido o diálogo **Seleção de Idioma**.
- Selecione o idioma que deseja usar para instalar seu produto Avira e confirme sua seleção de idioma clicando em **Avançar**.
  - ↪ É exibida a caixa de diálogo **Download**. Todos os arquivos necessários para instalação são baixados dos servidores da web do Avira. A janela **Download** fecha após a conclusão do download.

Instalação com um pacote de instalação

- ↪ É exibida a janela **Preparando a Instalação**.
- ↪ O arquivo de instalação é extraído. A rotina de instalação é iniciada.
- ↪ É exibida a caixa de diálogo **Escolher o tipo de instalação**.

Observação
Por padrão, a **Instalação Expressa** está predefinida. Todos os componentes padrão serão instalados, os quais não podem ser configurados. Se desejar executar uma instalação Personalizada, consulte o capítulo: Instalação e Desinstalação > Instalação Personalizada.

- A caixa de seleção **Quero melhorar a minha proteção usando o Avira ProActiv e o Protection Cloud** (Configuração > Geral > Proteção avançada) está predefinida

como padrão. Se não desejar participar da Comunidade do Avira, desmarque esta caixa de seleção.

- ↪ Se você confirmar sua participação na Comunidade do Avira, a Avira 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 EULA.
- Clique em **Avançar**.
  - ↪ O **Assistente de licença** é aberto e ajuda a ativar seu produto.
  - ↪ Você tem a oportunidade de configurar um **Servidor Proxy** aqui mesmo.
- Clique em **Configurações de Proxy** para configuração e confirme sua configuração com **OK**.
- Selecione a opção **Testar Produto** no Assistente de licença e clique em **Avançar**.
- Insira seus dados nos campos necessários do **Registro**. Decida se deseja assinar o **Boletim Informativo da Avira** e clique em **Avançar**.
  - ↪ O progresso da instalação é exibido por uma barra verde.
  - ↪ A caixa de diálogo **Juntar-se aos milhões de usuários Avira que já usam o Avira SearchFree Toolbar** é exibida.
- Se você não deseja instalar o Avira SearchFree Toolbar, desmarque a caixa de seleção com o **Contrato de Licença do Usuário final** do Avira SearchFree Toolbar e do Avira SearchFree Updater e aquela que define **Avira SearchFree (search.avira.com)** como sua home page do navegador.

Observação
Se necessário, desinstale quaisquer barras de ferramenta de procura instaladas anteriormente antes de instalar o Avira SearchFree Toolbar. Caso contrário, você não conseguirá instalar o Avira SearchFree Toolbar.

- Clique em **Avançar**.
  - ↪ O progresso da instalação da Avira SearchFree Toolbar é exibido por uma barra verde.
- Será solicitado para reiniciar seu sistema para que seu produto Avira seja ativado. Clique em **Sim** para reinicializar seu computador imediatamente.
  - ↪ O Ícone de Bandeja do Avira é colocado na barra de tarefas.
  - ↪ Sua licença de avaliação é válida oir 31 dias.

3.6 Assistente de Configuração

No final de uma instalação definida pelo usuário, o assistente de configuração é aberto. O assistente de configuração permite que você defina configurações personalizadas para o produto Avira.

- Clique em **Avançar** na janela de boas-vindas do assistente de configuração para iniciar a configuração do programa.
  - ↳ A caixa de diálogo **Configurar AHeAD** permite selecionar um nível de detecção para a tecnologia AHeAD. O nível de detecção selecionado é usado para as configurações da tecnologia AHeAD do Scanner (varredura por demanda) e do Real-Time Protection (varredura no acesso).
- Selecione um nível de detecção e continue a instalação clicando em **Avançar**.
  - ↳ Na próxima caixa de diálogo, **Seleçar de categorias de ameaças**, você pode adaptar as funções de proteção do produto Avira às categorias de ameaças especificadas.
- Quando apropriado, ative outras categorias de ameaças e continue a instalação clicando em **Avançar**.
  - ↳ Se tiver selecionado o módulo de instalação do Avira FireWall , a caixa de diálogo **Regras padrão para acessar a rede e usar recursos de rede** é exibida. Você pode definir se o Avira FireWall deve permitir acesso externo para recursos ativados bem como o acesso à rede por aplicativos de empresas confiáveis.
- Ative as opções necessárias e continue a configuração clicando em **Avançar**.
  - ↳ Se você tiver selecionado o módulo de instalação do Avira Real-Time Protection, a caixa de diálogo **Modo de inicialização do Real-Time Protection** será exibida. Você pode estipular o horário de início do Real-Time Protection. Em cada reinicialização do computador, o Real-Time Protection será iniciado no modo de início especificado.

Observação
O modo de início do Real-Time Protection especificado é salvo no registro enão pode ser alterado via Configuração.

Observação
Se o modo de início padrão para o Real-Time Protection (Início Normal) tiver sido escolhido e o processo de logon na inicialização for realizado rapidamente, os programas configurados para iniciar automaticamente na inicialização poderão não ser verificados, porque eles podem ser ativados antes de o Real-Time Protection ter sido completamente iniciado.

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

- Se você tiver selecionado o módulo de instalação do Avira Web Protection, a caixa de diálogo **Ativação Safe Browsing** será exibida. Você tem a opção de atribuir diferentes funções – crianças, jovens, adultos – aos usuários do computador para o uso da Internet. Você também pode desativar o **Safe Browsing**.

- Defina as configurações de Safe Browsing necessárias e continue a configuração clicando em **Avançar**.
  - Na caixa de diálogo **Atribuir senha** a seguir, você pode proteger com senha a Configuração contra acesso não autorizado. Isso é particularmente recomendado se o controle dos pais estiver ativado.
  - Na caixa de diálogo **Varredura do sistema** a seguir, uma varredura rápida do sistema pode ser ativada ou desativada. A varredura rápida do sistema é realizada após a conclusão da configuração e antes da reinicialização do computador, e verifica a presença de vírus e malwares nos programas em execução e nos arquivos mais importantes do sistema.
- Ative ou desative a opção **varredura rápida do sistema** e continue a configuração clicando em **Avançar**.
  - Na próxima caixa de diálogo, você pode concluir a configuração clicando em **Concluir**
  - As configurações especificadas e selecionadas são aceitas.
  - Se você tiver ativado a opção **Varredura rápida do sistema**, a janela **Luke Filewalker** será exibida. O Scanner executa uma varredura rápida do sistema.
- Se solicitado para reiniciar seu computador após a varredura, clique em **Sim** para assegurar que seu sistema esteja completamente protegido.

Após uma instalação bem-sucedida, recomendamos que você verifique se o programa está atualizado no campo **Status** do **Centro de Controle**.

- Se o produto Avira mostrar que o computador não está protegido, clique em **Corrigir problema**.
  - A caixa de diálogo **Restaurar a proteção** abre.
- Ative as opções predefinidas para maximizar a segurança do sistema.
- Se apropriado, execute uma varredura do sistema completa posteriormente.

3.7 Alterar Instalação

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

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

Selecione seu produto Avira e clique em **Alterar**. No diálogo **Bem-vindo** do programa, selecione a opção **Modificar**. Você será orientado pelas alterações de instalação.

3.8 Módulos de Instalação

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

- **Avira Internet Security**
  Este módulo contém todos os componentes requeridos para a instalação bem-sucedida de seu produto Avira.
- **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. Sempre que o usuário realiza uma operação de arquivo (por exemplo, carregar documento, executar, copiar), o produto Avira verifica o arquivo automaticamente. Renomear o arquivo não dispara uma varredura 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, são verificados quanto a vírus e programas indesejados e encaminhados ao programa de e-mail. Dependendo da configuração, o programa processa os e-mails afetados automaticamente ou solicita alguma ação ao usuário. Além disso, o Mail Protection pode proteger você contra e-mails de spam.
- **Avira FireWall**
  O Avira FireWall controla a comunicação de entrada e saída do computador. Ele permite ou nega comunicações com base em políticas de segurança.
- **Rootkits Protection**
  O Avira Rootkit Protection verifica se há software já instalado no computador que não pode mais ser detectado com métodos convencionais de proteção contra malware após invadir o 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 é integrado no Avira Real-Time Protection.
- **Protection Cloud**
  O componente Protection Cloud é um módulo para detecção online dinâmica de malware ainda desconhecido.
- **Backup**

  O componente Backup permite que você crie backups espelhados de seus dados manual e automaticamente.
- **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 serão movidos diretamente no cache do navegador para serem exibidos no navegador da web, de forma que uma varredura 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. 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.

3.9 Desinstalação

Se desejar remover o produto Avira de seu computador, você poderá usar a opção **Adicionar ou Remover Programas** para **Alterar/Remover** programas no Painel de Controle do Windows.

Para desinstalar seu produto Avira (por exemplo, no Windows 7):

- Abra o **Painel de Controle** através do menu **Iniciar** do Windows.
- Clique duas vezes em **Programas e Recursos**.
- Selecione o produto Avira na lista e clique em **Desinstalar**.
  - ↪ Será perguntado se você realmente deseja remover o programa.
- Clique em **Sim** para confirmar.
  - ↪ Será perguntado se você deseja reativar o Firewall do Windows (o Avira Firewall será desativado).
- Clique em **Sim** para confirmar.
  - ↪ Todos os componentes do programa serão removidos.
- Clique em **Concluir** para concluir a desinstalação.
  - ↪ Quando for apropriado, uma caixa de diálogo será exibida recomendando a reinicialização do computador.
- Clique em **Sim** para confirmar.
  - ↪ O produto Avira agora está desinstalado e todos os diretórios, arquivos e entradas de registro para o programa serão excluídos quando o computador for reiniciado.

Observação
O Avira SearchFree Toolbar não é incluído no programa de desinstalação e deve ser desinstalado separadamente seguindo as etapas detalhadas acima. Para fazer isto no Firefox, o Avira SearchFree Toolbar deve ser ativado por meio do Add-On Manager. Após a desinstalação, a barra de ferramentas de pesquisa não fica mais integrada em seu navegador da web.

4. Visão geral do Avira Internet 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 Avira SearchFree Toolbar
- consulte o Capítulo Como...?

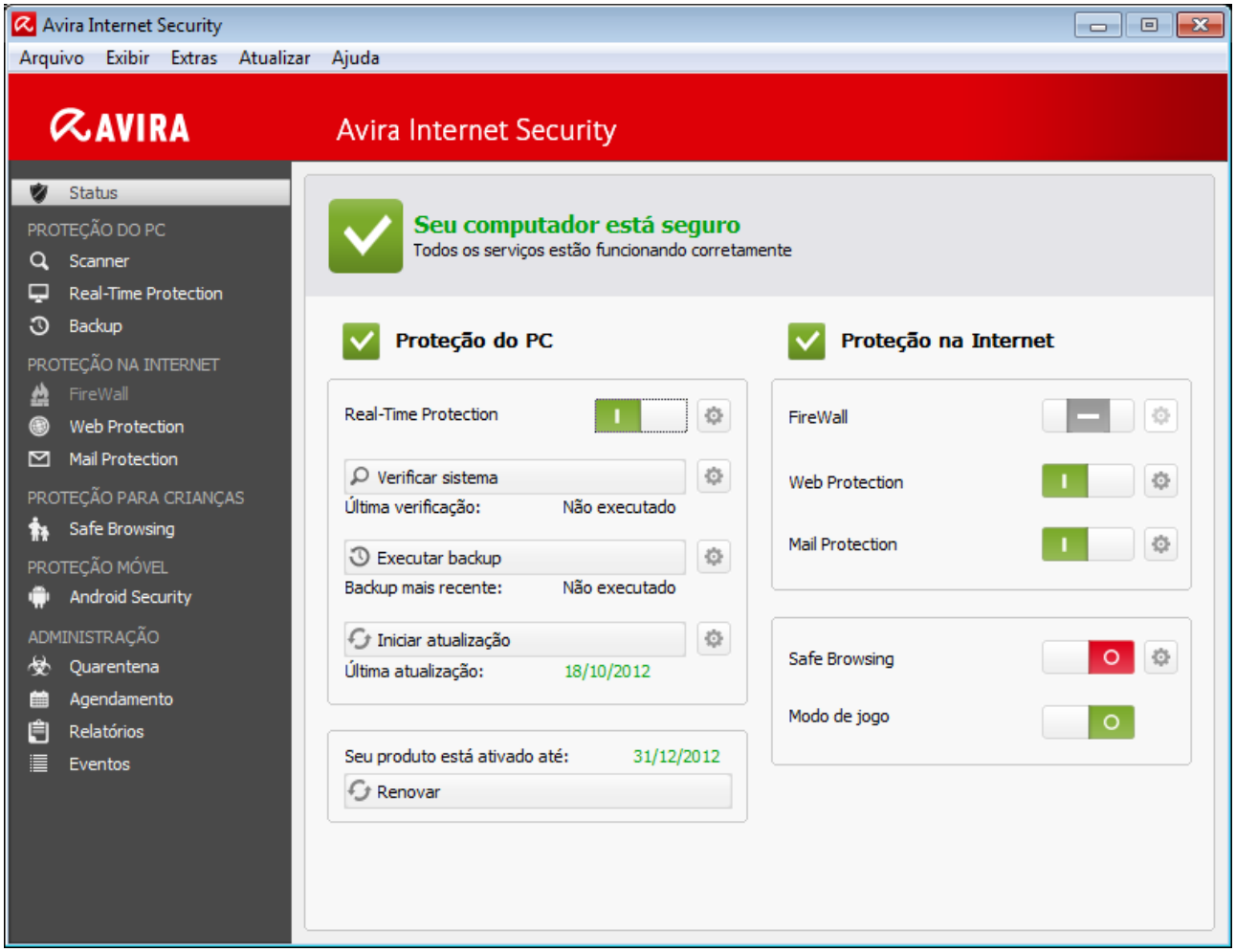
4.1 Interface de Usuário e Operação

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".
- Na seção Backup, é possível criar backups dos seus dados com rapidez e facilidade e iniciar trabalhos de backup.

- *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 treinar o filtro anti-spam e excluir endereços de e-mail da futura varredura de malware ou spam. Os e-mails também podem ser excluídos do buffer do Mail Protection.
- *PROTEÇÃO PARA CRIANÇAS*: Nesta seção você localizará os componentes para assegurar uma experência na Internet segura para seus filhos.
  - Na seção Safe Browsing os usuários do computador podem receber funções de usuário. Uma função do usuário é configurável e inclui um conjunto de URLs permitidos e bloqueados, categorias de URLs proibidos, duração do uso da Internet e, se necessário, períodos de uso permitidos em dias úteis.
- *PROTEÇÃO MÓVEL*: Desta seção você será redirecionado ao acesso on-line para dispositivos Android.
  - Avira Free Android Security gerencia todos os dispositivos baseados em Android.
- *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 Modo de Jogo

Se um aplicativo for executado em modo de tela cheia no sistema de computação, é possível suspender intencionalmente as notificações de área de trabalho como janelas pop-up e mensagens no produto ativando o Modo de Jogo. Todas as regras de aplicativo e de adaptador que foram configuradas no Avira FireWall se aplicam, mas nenhuma janela pop-up aparece na notificação de evento de rede.

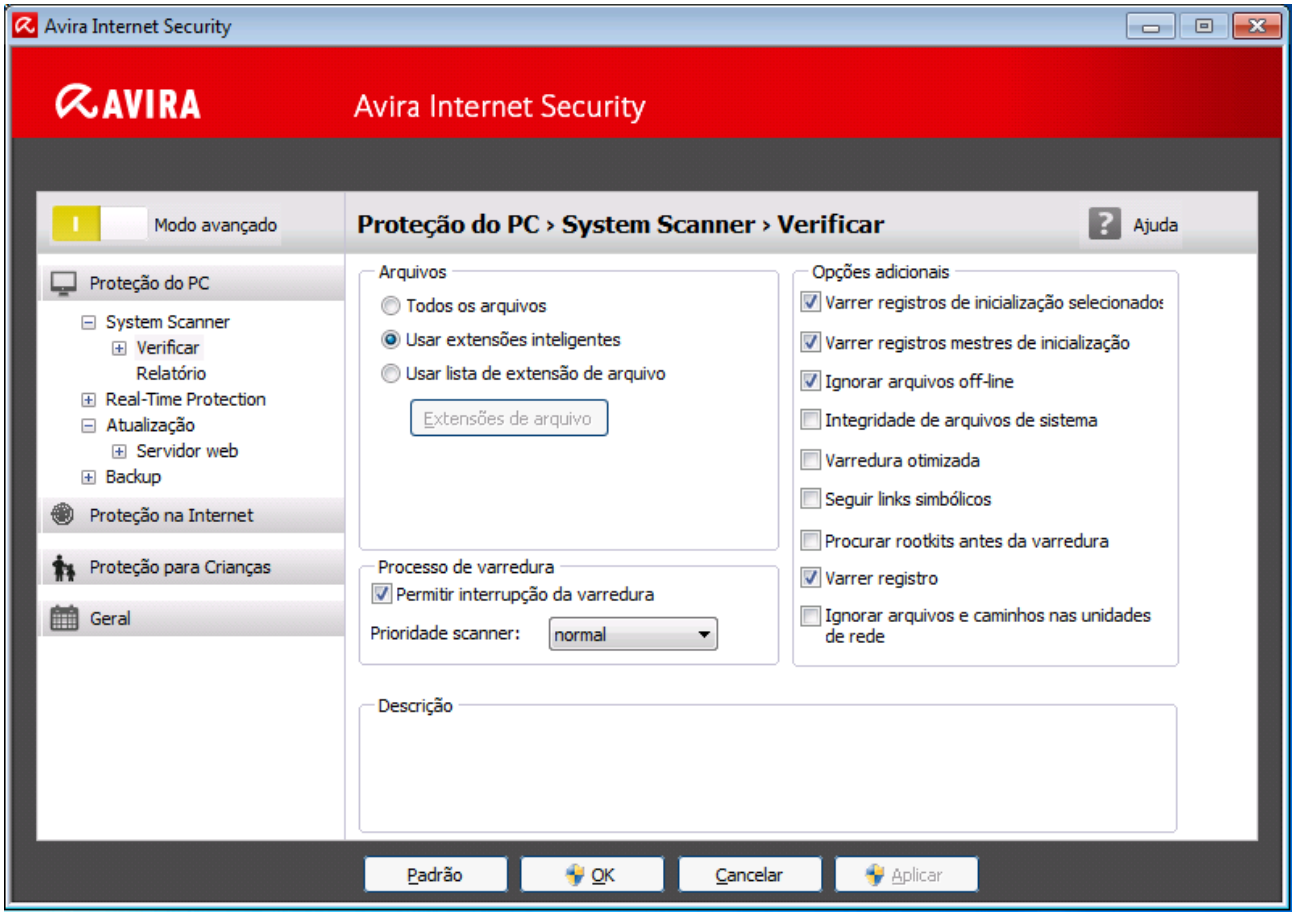
O Modo de Jogo pode ser ativado ou mantido em modo automático clicando no botão **LIGA/DESLIGA**. Por padrão o Modo de Jogo está definido para **automático** e é exibido em cor verde. A configuração padrão define o recurso para automático, de modo que toda vez que for executado um aplicativo que precisar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

- Clique no botão à esquerda do botão **DESLIGAR** para ativar o Modo de Jogo.
  - ↪ O Modulo de Jogo 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.

4.1.3 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 **Modo avançado** deve ser ativado para selecionar registros de configuração individuais. Nesse caso, uma caixa de diálogo é exibida solicitando a ativação do Modo avançado.

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.

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

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.

Visão geral das opções de configuração

As seguintes opções de configuração estão disponíveis:

- **Scanner**: Configuração da varredura por demanda
  - Resolução de na detecções
  - 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
- **Backup**:
  - Configuração do componente Backup (backup incremental, varredura de vírus durante o backup)
  - Exceções: definição de arquivos a serem salvos
  - Configuração da função de registro
- **Atualização**: Configuração das configurações de atualização
  - 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 do banco de dados de treinamento antispam, banco de dados de treinamento vazio
  - Configuração de um rodapé nos e-mails enviados
  - Configuração da função de registro
- **Proteção para crianças**:
  - Safe Browsing: Função de controle dos pais filtro baseado em função e limitação de tempo baseada em função do uso da Internet
- **Geral**:
  - 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
  - Configuração de alertas acústicos emitidos quando malwares são detectados

4.1.4 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
  - **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 Internet Security**: Abre o Centro de Controle.
- **Configurar Avira Internet Security**: Abre a Configuração.
- **Minhas mensagens**: Abre um slide com as informações atuais sobre seu produto Avira.
- **Minhas configurações de comunicação**: Abre o Product Message Subscription Center
- **Iniciar atualização** Inicia uma atualização.
- **Ajuda**: abre a ajuda online.
- **Sobre o Avira Internet 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 Avira SearchFree Toolbar

O Avira SearchFree Toolbar inclui dois componentes principais: o Avira SearchFree e o Toolbar.

O Avira SearchFree Toolbar é instalado como um complemento. Quando o navegador for acessado pela primeira vez (no Firefox e Internet Explorer), será exibida uma mensagem perguntando se você tem permissão para instalar a barra de ferramentas. Você precisará aceitar para concluir uma instalação com êxito do Avira SearchFree Toolbar.

O Avira SearchFree é um mecanismo de pesquisa e contém um logotipo clicável do Avira para o site do Avira e canais da web, de imagem e vídeo. Isto permite uma navegação na Internet mais segura aos usuários do Avira.

A barra de ferramentas, integrada em seu navegador da web, consiste em uma caixa de pesquisa, um logotipo do Avira vinculado ao site da Avira, duas exibições de status, três widgets e o menu **Opções**.

- Barra de Ferramentas de Pesquisa
  Use a barra de ferramentas de pesquisa gratuitamente para pesquisar rapidamente a Internet usando o mecanismo de pesquisa da Avira.
- Exibição de Status
  As exibições de status fornecem informações sobre o status do Web Protection e o status de atualização atual de seu produto Avira e o ajuda a identificar quais ações você precisa executar para proteger seu PC.
- Widgets
  O Avira oferece três widgets para as funções mais importantes relacionadas à Internet. Com um clique, você tem acesso direto ao Facebook e ao seu e-mail ou pode garantir a navegação na web segura (apenas Firefox e Internet Explorer).
- Opções
  Você pode usar o menu **Opções** para acessar as opções da barra de ferramentas, limpar o histórico, localizar a ajuda e informações da barra de ferramentas e também desinstalar o Avira SearchFree Toolbar diretamente através do navegador da web (apenas Firefox e Internet Explorer).

4.2.1 Uso

Avira SearchFree

Você pode usar o Avira SearchFree para definir qualquer número de termos para procurar na Internet.

Insira o termo na caixa de pesquisa e pressione a tecla **Enter** ou clique em **Pesquisar**. O mecanismo Avira SearchFree, então, pesquisa a Internet para você e exibe todas as ocorrências na janela do navegador.

Para descobrir como customizar a configuração do Avira SearchFree no Internet Explorer, Firefox e Chrome, vá para **Opções**.

Exibição de Status

Web Protection

É possível usar os seguintes ícones e mensagens para identificar quais ações você precisa executar para proteger seu PC:

Ícone	Exibição de Status	Descrição
	*Web Protection*	Se você mover o cursor sobre o ícone, as seguinte mensagem é exibida: *O Avira Web Protection está ativo. Sua navegação está protegida.* Nenhuma ação adicional é necessária.
	*Web Protection inativo*	Se você mover o cursor sobre o ícone, as seguinte mensagem é exibida: *O Avira Web Protection está desligado. Clique para saber como ligá-lo.* ↪ Você será redirecionado para um dos artigos da nossa Base de Conhecimento.

	*Sem Web Protection*	Se você mover o cursor sobre o ícone, uma das seguintes mensagens aparecerá: • *Você não tem Avira Web Protection instalado. Clique para saber como proteger sua navegação.* Essa mensagem aparecerá se você instalar incorretamente ou desinstalar o Avira Antivirus. • *O Web Protection é incluído gratuitamente com o antivírus Avira. Clique para saber como instalá-lo.* Essa mensagem aparecerá se você não instalar o Web Protection ou se desinstalá-lo. ↪ Nos dois casos você será redirecionado à home page da Avira, onde poderá fazer download do produto Avira.
	*Erro*	Se você mover o cursor sobre o ícone, a seguinte mensagem aparecerá: *O Avira relatou um erro. Clique para entrar em contato com o Suporte e obter ajuda.* ▸ Clique no ícone ou texto cinza para ir para a página Suporte do Avira.

Widgets

O Avira SearchFree contém três widgets com as funções mais importantes para a navegação da web na Internet atualmente: Facebook, E-mail e Navegador de segurança.

Facebook

Esta função permite receber todas as mensagens do Facebook e estar sempre atualizado.

E-mail

Se você clicar no símbolo de e-mail na barra de ferramentas, será mostrada uma lista suspensa. Você pode escolher entre os provedores de e-mail usados mais comumente.

Navegador de segurança

Este widget foi concebido para ofeecerr em um clique todas as opções de segurança na Internet necessárias diariamente. Esta opção está disponível apenas para Firefox e Internet Explorer. Além disso, os nomes das funções às vezes, mudam de um navegador para outro:

- *Bloqueador de Pop-up*

Se esta opção estiver ativada, todas as janelas pop-up serão bloqueadas.

- *Bloquear Cookies*

Se você ativar esta opção, nenhum cookie será salvo em seu computador.

- *Navegação Privada (Firefox) / Navegação InPrivate (Internet Explorer)*

Ative esta opção se você não desejar deixar nenhuma informação pessoal na Internet enquanto navega. Esta opção não está disponível para o Internet Explorer 7 e 8.

- *Limpar Histórico Recente (Firefox) / Excluir Histórico de Navegação (Internet Explorer)*

Com esta opção você apagará todos os rastros de suas atividades na Internet.

Website Safety Advisor

O Website Safety Advisor oferece uma classificação de segurança durante a navegação. Você pode avaliar a reputação do site que está sendo visitado e verificar se ele apresenta risco baixo ou alto para sua segurança.
Este widget também fornece informações adicionais sobre o site, como quem é o proprietário do domínio ou a razão pela qual o site foi categorizado como seguro ou arriscado.

O status do Website Safety Advisor é exibido no Toolbar e nos resultados da pesquisa, como um ícone de bandeja do Avira em combinação com outros ícones:

Ícone	Exibição de Status	Descrição
	*Seguro*	Uma marca de seleção verde para sites seguros.
	*Baixo Risco*	Um ponto de exclamação amarelo para sites que representam baixo risco.
	*Alto Risco*	Um sinal de pare vermelho para sites que representam alto risco para a sua segurança.
	*Desconhecido*	Um ponto de interrogação cinza aparece quando o status for desconhecido.

	*Verificação*	Este sinal aparecerá durante a verificação do status de um site.

Browser Tracking Blocker

Com o Browser Tracking Blocker, é possível parar a coleta de informações sobre você pelos controladores enquanto você está navegando.
O widget permite escolher quais controladores bloquear e quais permitir.

As empresas de controle são classificadas em três categorias:

- Redes sociais
- Redes de anúncios
- Outras empresas

4.3 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.

4.3.1 Ativar Licença

Para ativar a licença de seu produto Avira:

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

Caso ainda não tenha instalado seu produto Avira:

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

Se o produto Avira já foi 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 licenças for aberto.

  - OU -

  No Centro de Controle de seu produto Avira, selecione o item de menu **Ajuda > Gerenciamento de licençass**

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.

4.3.2 Ativar Produto

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

Ativação com uma licença completa válida

Para ativar o programa com uma licença completa, você precisa de um código de ativação válida, o qual contém dados da licença adquirida. Você recebeu o código de ativação por e-mail ou ele estava impresso na embalagem do produto.

Ativação com uma licença de avaliação

O produto Avira é ativado com uma licença de avaliação gerada automaticamente, com a qual é possível testar o produto Avira com todas as suas funções por um período limitado.

Observação
Para ativação do produto ou para uma licença de teste, você precisa de um link da Internet ativo.
Se nenhuma conexão puder ser estabelecida com os servidores do Avira, verifique as configurações do firewall usado: Conexões através do protocolo HTTP e da porta 80 (comunicação na web) e através do protocolo de criptografia SSL e da porta 443 são usadas para ativação do produto. Verifique se o seu firewall não bloqueia dados de entrada e de saída. Primeiro, verifique se você consegue acessar as páginas da web com seu navegador.

A seguir há uma descrição de como ativar seu produto Avira:

Caso ainda não tenha instalado seu produto Avira:

- Instale seu produto Avira.
  - ↪ Durante o processo de instalação, você deverá escolher uma opção de ativação
- **Ativar produto***:* Ativação com uma licença completa válida
- **Testar produto***:* Ativação com uma licença de avaliação

- Insira o código ativação para ativar o produto com uma licença completa.
- Confirme a seleção do procedimento de ativação clicando em **Avançar**.
- Se e quando necessário, insira seus dados pessoais de registro e confirme clicando em **Avançar**.
  - ↪ Os dados de sua licença serão exibidos na próxima janela. Seu produto Avira foi ativado.
- Continue a instalação.

Se o produto Avira já foi instalado:

- No Centro de Controle, selecione o item de menu **Ajuda > Gerenciamento de licenças**.
  - ↪ O *assistente de licença* é aberto, no qual você pode escolher uma opção de ativação. As próximas etapas de ativação do produto são idênticas ao procedimento descrito acima.

4.3.3 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: 2 horas.

- 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

4.3.4 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: 2 horas.

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

4.3.5 Usando um perfil de varredura para verificar a presença de vírus e malwares

Um perfil de varredura é um conjunto de unidades e diretórios a serem verificados.

As seguintes opções estão disponíveis para varredura com um perfil de varredura:

Usar perfil de varredura predefinido

Se o perfil de varredura predefinido corresponder aos seus requisitos.

Personalizar e aplicar perfil de varredura (seleção manual)

Se desejar verificar com um perfil personalizado.

Criar e aplicar novo perfil de varredura

Se desejar criar seu próprio perfil de varredura.

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

- No Windows XP:

   Esse ícone inicia a verificação através de um perfil.

- No Windows Vista:

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

  -  Esse ícone inicia uma verificação limitada através de um perfil de verificação. Somente os diretórios e arquivos aos quais o Windows Vista concedeu direitos de acesso são verificados.
  -  Esse ícone inicia a verificação com direitos de administrador estendidos. Após a confirmação, todos os diretórios e arquivos no perfil de varredura selecionado são verificados.

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

1. Vá para o Centro de Controle e selecione a seção *PROTEÇÃO DO PC* **> 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 varredura
3. Clique no ícone (Windows XP:  ou Windows Vista: ).
4. A janela **Luke Filewalker** aparece e uma verificação do sistema é iniciada.
   ↪ Quando a verificação termina, os resultados são exibidos.

Se desejar adaptar um perfil de varredura:

1. No perfil de varredura, 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.

▸ Realce os nós e os diretórios que deseja verificar clicando na caixa relevante do nível de diretório apropriado:

As seguintes opções estão disponíveis para selecionar diretórios:

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

Se desejar criar um novo perfil de varredura:

▸ Clique no ícone  **Criar novo perfil**.

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

▸ Quando apropriado, renomeie o perfil de varredura clicando no ícone  .

▸ Realce os nós e diretórios a serem salvos clicando na caixa de seleção do nível de diretório correspondente.

As seguintes opções estão disponíveis para selecionar diretórios:

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

4.3.6 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.

4.3.7 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.

4.3.8 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

4.3.9 Verificação direcionada para Rootkits e malware ativo

Para verificar rootkits ativos, use o perfil de varredura 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 varredura predefinido **Verificar rootkits e malware ativo**.
- Quando apropriado, realce outros nós e diretórios a serem verificados clicando na caixa de seleção do nível de diretório.
- Clique no ícone (Windows XP:  ou Windows Vista: ).
  - ↪ A janela **Luke Filewalker** aparece e uma verificação do sistema é iniciada.
  - ↪ Quando a verificação termina, os resultados são exibidos.

4.3.10 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.

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.

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.

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.**.

4.3.11 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.

Observação
Você pode carregar somente um arquivo por vez.

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).

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

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

Para restaurar os arquivos em quarentena:

Aviso
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 para 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 no diretório selecionado.

4.3.13 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)).

4.3.14 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.

4.3.15 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.

4.3.16 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:

- Backup
- FireWall
- Serviço de ajuda
- Mail Protection
- Real-Time Protection
- Safe Browsing
- Agendamento
- Scanner
- Atualizador

- Web Protection

Os seguintes tipos de evento são exibidos:

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

Para filtrar os eventos exibidos:

- No Centro de Controle, selecione a seção *ADMINISTRAÇÃO* **> Eventos**.
- Marque a caixa dos componentes do programa para exibir os eventos dos componentes ativados.

  - OU -

  Desmarque a caixa dos componentes do programa para ocultar os eventos dos componentes desativados.
- Marque a caixa de tipo de evento para exibir esses eventos.

  - OU -

  Desmarque a caixa de tipo de evento para ocultar estes eventos.

4.3.17 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 apropriado para excluir o email da verificação do Mail Protection:

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

▪  O endereço de email selecionado não será mais verificado em busca de spam.

  - ↪ O endereço do emissor do email é incluído na lista de exclusões e não será mais verificado em busca de vírus, malwares ou spam .

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 exclusão.

4.3.18 Treinar o módulo AntiSpam

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

Para categorizar os emails para o banco de dados de treinamento:

- 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 categorizar.
- Clique no ícone apropriado para identificar o email como spam  ou desejado, isto é, email 'válido'  .
  - ↪ O email é inserido no banco de dados de treinamento e aplicado ao próximo processo de reconhecimento de spam.

Observação
Você pode excluir o banco de dados de treinamento na configuração em **Mail Protection > Geral > AntiSpam**.

Nota
O módulo AntiSpam não funciona para emails recebidos via IMAP. Devido a isto, as funções de treinamento (**Email válido – usar para treinamento, Spam – usar para treinamento**) não podem ser aplicadas aos emails recebidos via IMAP. Se você selecionar um email do tipo IMAP, as funções de treinamento serão automaticamente desativadas.

4.3.19 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.

4.3.20 Criar backups manualmente

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

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

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

Para salvar seus dados usando a ferramenta de backup:

- No Centro de Controle, selecione a seção *PROTEÇÃO DO PC* **> Backup**.
  ↪ Os perfis de backup predefinidos são exibidos.
- Selecione um dos perfis de backup predefinidos.

  -OU-

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

  -OU-

  Crie um novo perfil de backup
- Insira um local de salvamento para o perfil selecionado na caixa **Diretório de Destino**.

  O local de salvamento do backup pode ser um diretório em seu computador, em uma unidade de rede conectada ou um disco removível, como um pendrive ou um disquete.
- Clique no ícone  .
  ↪ A janela **Avira Backup** é exibida e o backup começa. O status e os resultados do backup são exibidos na janela de backup.

Para modificar um perfil de backup:

- No perfil de varredura, expanda a árvore de arquivos **Seleção Manual** para que todas as unidades e todos os diretórios a serem salvos sejam abertos:

- Clique no ícone **+**: O próximo nível de diretório é exibido.
- Clique no ícone **-**: O próximo nível de diretório é ocultado.

- Realce os nós e diretórios a serem salvos clicando na caixa do nível de diretório correspondente:

  As seguintes opções estão disponíveis para selecionar diretórios:

- Diretório, incluindo os subdiretórios (marca de 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 backup:

- Clique no ícone **Criar novo perfil**.
  - ↳ O perfil **Novo perfil** aparece abaixo dos perfis criados anteriormente.
- Quando apropriado, forneça um nome ao perfil de backup clicando no ícone .
- Realce os nós e diretórios a serem salvos clicando na caixa de seleção de cada nível de diretório.

  As seguintes opções estão disponíveis para selecionar diretórios:

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

4.3.21 Criar backups de dados automáticos

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

- No Centro de Controle, selecione a seção *ADMINISTRAÇÃO* **> Agendamiento**.
- Clique no ícone .
  - ↳ A caixa de diálogo **Nome e descrição do trabalho** é exibida.
- Dê um nome ao trabalho e, quando apropriado, uma descrição.
- Clique em **Avançar**.
  - ↳ A caixa de diálogo **Tipo de trabalho** é exibida.
- Selecione **Trabalho de backup**.
- Clique em **Avançar**.
  - ↳ A caixa de diálogo **Selecionar perfil** é exibida.
- Selecione o perfil a ser verificado.

Observação
Somente perfis de backup para os quais um local de salvamento foi estipulado são exibidos.

- Clique em **Avançar**.
  - ↪ A caixa de diálogo **Tempo do trabalho** é exibida.
- Selecione um horário para a verificação:

- **Imediatamente**
- **Diariamente**
- **Semanalmente**
- **Intervalo**
- **Única**
- **Logon**
- **Plug&Play**
  Um backup é sempre criado para o evento Plug&Play se o disco removível selecionado como o local de salvamento do perfil de backup está conectado ao computador. O evento de backup Plug&Play requer uma inserção de um pendrive como local de salvamento.

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

Repetir o trabalho se o tempo 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 **Selecionar modo de exibição** é exibida.
- Selecione o modo de exibição da janela do trabalho:

- **Minimizado**: somente barra de progresso
- **Maximizado**: janela de backup inteira
- **Invisível**: nenhuma janela de backup

- Clique em **Concluir**.
  - ↪ Seu trabalho recém-criado aparece na página inicial da seção *ADMINISTRAÇÃO* **> Agendamiento** 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

5. 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. 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: 2 horas.

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 do fabricante. A ligação de rede existente é a ligação padrão com os servidores de transferência da Avira. Pode alterar esta configuração predefinida em Configuração > Atualização.

7. Backup

Existem várias opções disponíveis para criar backup dos seus dados:

Backup por meio da ferramenta de backup

A ferramenta de backup pode ser usada para selecionar ou criar perfis de backup e iniciar o backup de um perfil selecionado manualmente.

Backup por meio de um trabalho de backup no Agendamiento

O Agendamiento permite criar trabalhos de backup controlados por evento ou programados. O Agendamiento executa os trabalhos de backup automaticamente. Esse processo é particularmente útil se você desejar fazer backups regulares de dados específicos.

8. 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 e Vista) ou Windows Action Center (Windows 7 e 8)

8.1 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 do bate-papo não serão exibidas

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

Motivo: O arquivo está criptografado.

- Para ativar a licença não é necessário abrir o arquivo, basta salvá-lo no diretório do programa .

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

Motivo: sua conexão com a Internet não está ativa. 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 (modo avançado) 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 (modo avançado).
- 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 (modo avançado) 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*.
- Ative a opção **Modo avançado**.
- 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**).

8.2 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.

8.2.1 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.

8.2.2 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.

8.2.3 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)

8.3 Central de Segurança do Windows

- Windows XP Service Pack 2 para Windows Vista -

8.3.1 Geral

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

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

8.3.2 A Central de Segurança do Windows e seu produto Avira

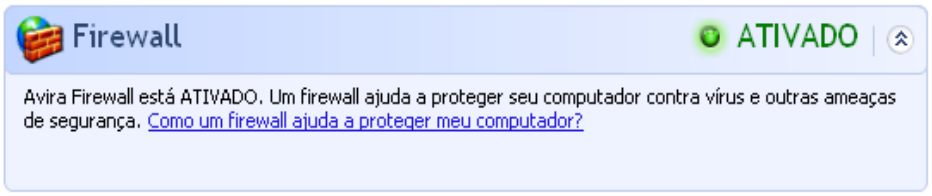
FireWall

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

- Firewall ATIVO / Firewall ativado
- Firewall INATIVO / Firewall desativado

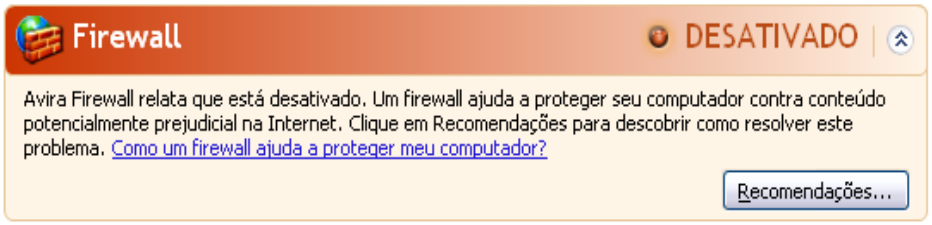
Firewall ATIVO / Firewall ativado

Após instalar o produto Avira e desativar o Firewall do Windows, você receberá a mensagem a seguir:



Firewall INATIVO / Firewall desativado

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



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

Aviso
Se você desativar o Avira FireWall, utilizadores não autorizados podem ter acesso ao seu computador através de uma rede ou da Internet.

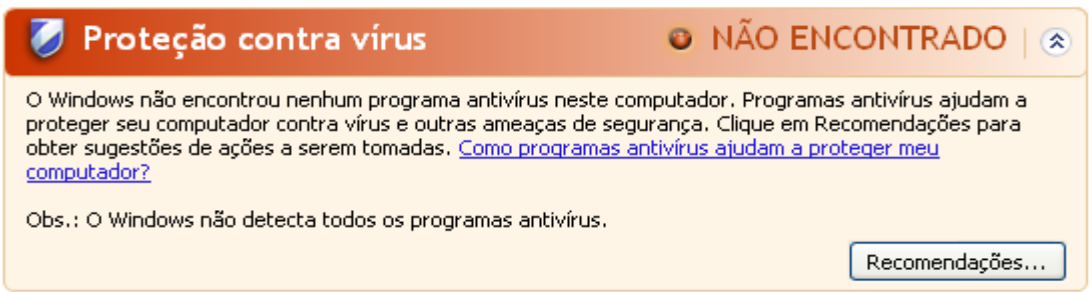
Software de proteção contra vírus/Proteção contra software malicioso

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

- Proteção contra vírus NÃO ENCONTRADA
- Proteção contra vírus DESATUALIZADA
- Proteção contra vírus ATIVADA
- Proteção contra vírus DESATIVADA
- Proteção contra vírus NÃO MONITORADA

Proteção contra vírus NÃO ENCONTRADA

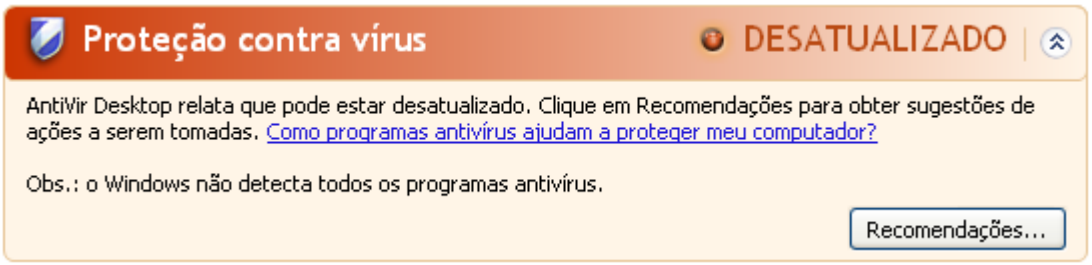
Essas informações aparecem quando a Central de segurança do Windows não encontra nenhum software antivírus em seu computador.



Observação
Instale o produto Avira em seu computador para protegê-lo contra vírus e outros programas indesejados!

Proteção contra vírus DESATUALIZADA

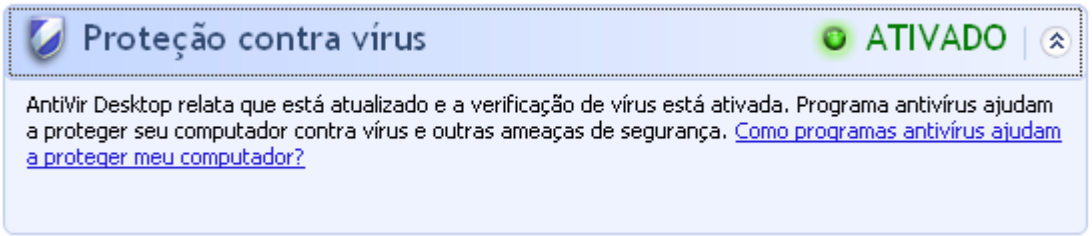
Se você já tinha instalado o Windows XP Service Pack 2 ou o Windows Vista e, em seguida, instalar o produto Avira ou se você instalar o Windows XP Service Pack 2 ou o Windows Vista em um sistema no qual o produto Avira já está instalado, receberá a seguinte mensagem:



Observação
Para que a Central de Segurança do Windows reconheça seu produto Avira como atualizado, uma atualização deverá ser executada após a instalação. Atualize o sistema executando uma atualização.

Proteção contra vírus ATIVADA

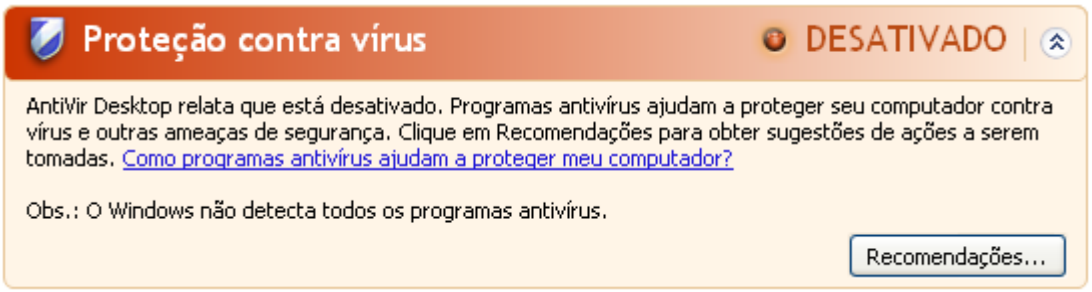
Após instalar o produto Avira e executar uma atualização subsequente, você receberá a seguinte mensagem:



Seu produto Avira agora está atualizado e o Avira Real-Time Protection está ativado.

Proteção contra vírus DESATIVADA

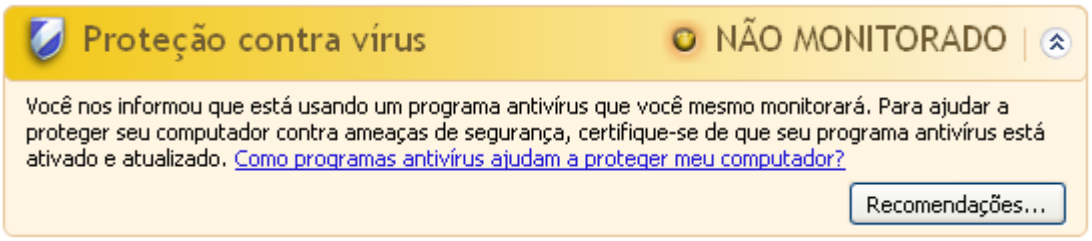
Você recebe a mensagem a seguir se desativar o Avira Real-Time Protection ou parar o serviço Real-Time Protection.



Nota
É possível ativar ou desativar o Avira Real-Time Protection na seção Status do **Centro de Controle**. Você também pode verificar que o Avira Real-Time Protection está ativado se o guarda-chuva vermelho em sua barra de tarefas está 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
Esta função não é suportada pelo Windows Vista.

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 ou o Windows Vista, 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!

8.4 Central de Ações do Windows

- Windows 7 e Windows 8 -

8.4.1 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*).

8.4.2 A Central de Ações do Windows e seu produto Avira

Firewall de rede

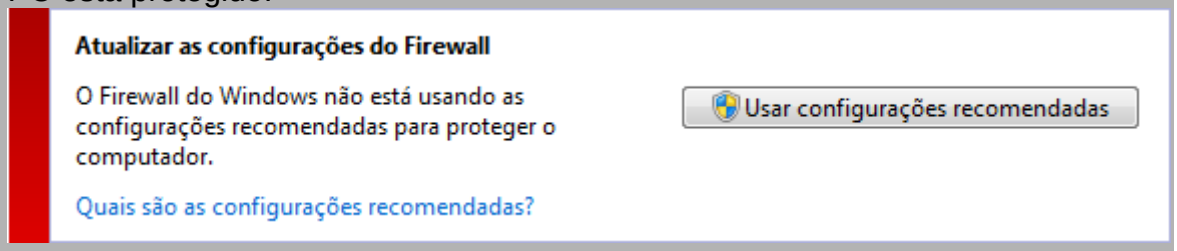
Você poderá receber as seguintes informações do **Central de Ações do Windows** com relação ao seu firewall:

- 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

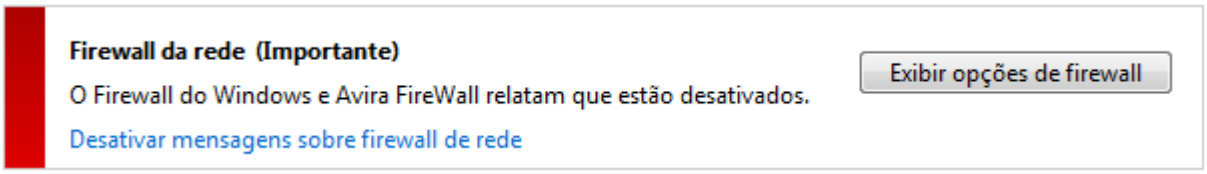
Após instalar o produto Avira e desativar o Firewall do Windows, você verá a seguinte mensagem em **Central de Ações > Segurança > Firewall de rede**: *O Avira FireWall relata que está ativado*. Isso significa que você escolheu o Avira FireWall como a sua solução de firewall. (Observe a diferença entre 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.



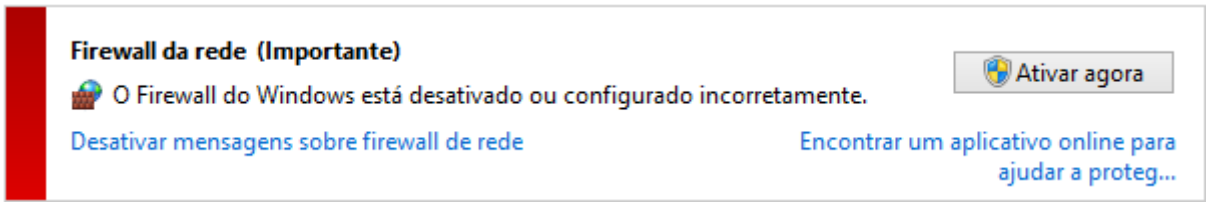
O Firewall do Windows e o Avira FireWall relatam que estão desligados

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.

- **No Windows 7**

  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.

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

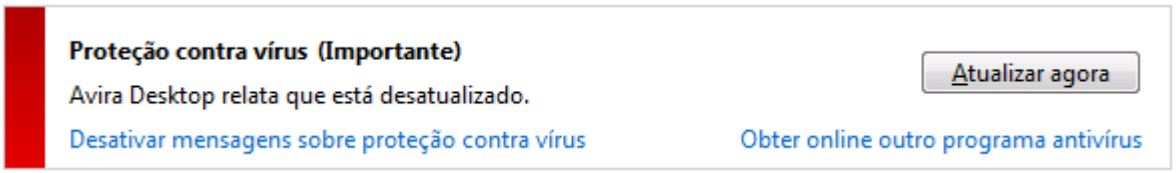
Você recebe a mensagem a seguir se desativar o Avira Real-Time Protection ou parar o serviço Real-Time Protection.

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

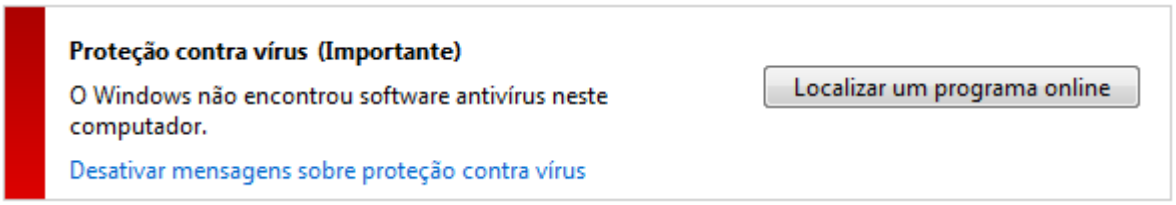
atualizados automaticamente (por exemplo, se foi feita uma atualização de um sistema operacional Windows mais antigo, no qual o produto Avira já está instalado) você receberá a seguinte mensagem:



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:

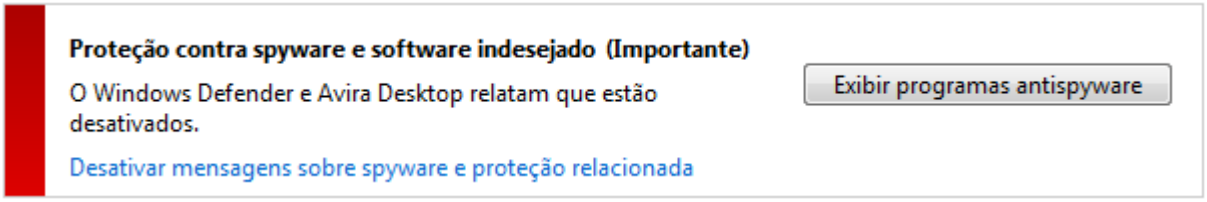
- O Avira Desktop relata que está ativado.
- O Windows Defender e o Avira Desktop relatam que estão desativados.
- O Avira Desktop relata que está desatualizado.
- O Windows Defender está desligado.
- O Windows Defender está desligado.

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.

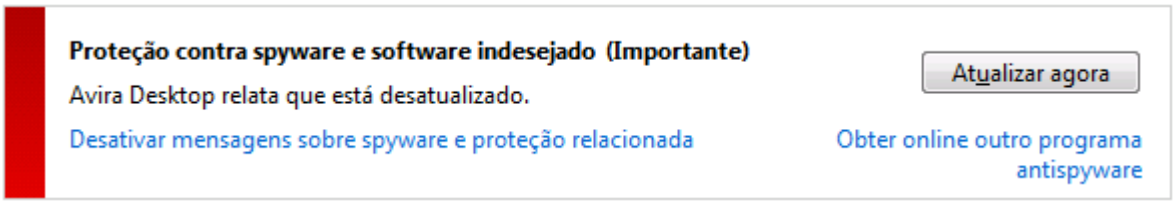


Nota
O Avira Real-Time Protection pode ser ativado ou desativado na seção **Status** do **Centro de Controle Avira**. Você também pode verificar que o Avira Real-Time Protection está ativado com o guarda-chuva vermelho aberto na barra de

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

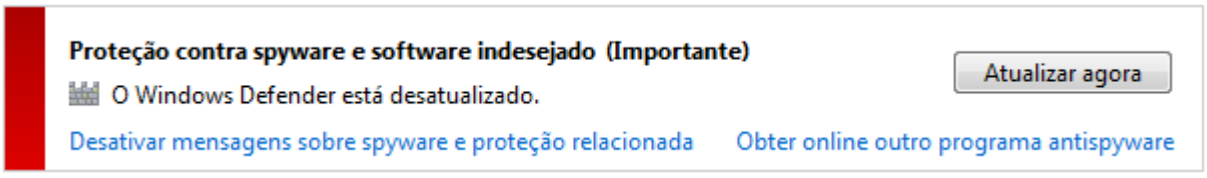
Se você acabou de instalar o Avira ou se por algum motivo o arquivo de definição de vírus, o mecanismo de varredura ou os arquivos de programa do produto Avira não foram atualizados automaticamente (por exemplo, se foi feita uma atualização de um sistema operacional Windows mais antigo, no qual o produto 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

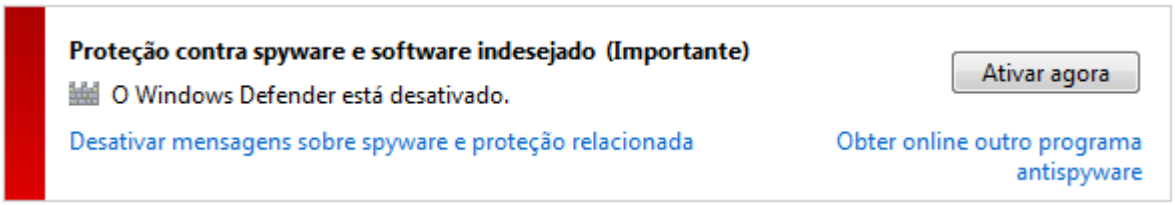
Você pode receber a mensagem a seguir se o Windows Defender estiver ativado. Se já tiver instalado o produto Avira, esta mensagem não deve ser exibida. Verifique se a instalação ocorreu corretamente.



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.



9. Vírus e mais

Avira Internet 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

9.1 Categorias de ameaça

Adware

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

Seu produto Avira 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.

9.2 Vírus e outros malwares

Adware

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

Backdoors

Um backdoor pode obter acesso a um computador 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.

10. Informações e Serviço

Este capítulo contém informações sobre como entrar em contato conosco.

- consulte o Capítulo Endereço de Contato
- consulte o Capítulo Suporte Técnico
- consulte o Capítulo Arquivos Suspeitos
- consulte o Capítulo Registrar falso-positivos
- consulte o Capítulo Seus comentários para mais segurança

10.1 Endereço de Contato

Se você tiver qualquer dúvida ou solicitação relacionada ao produto Avira, teremos prazer em ajudar. Para obter nossos endereços de contato, consulte o Centro de Controle em **Ajuda > Sobre o Avira Internet Security**.

10.2 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/premium-suite-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 Internet 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 Internet Security > Informações 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.

10.3 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 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-premium-suite-pt-br@avira.com
  Como alguns gateways de email 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

10.4 Relatando Falso-Positivos

Se achar que o produto Avira está relatando uma detecção em um aquivo 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-premium-suite-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).

10.5 Seus comentários para mais segurança

No Avira, a segurança de nossos clientes é prioridade. 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 em um de nossos produtos, envie-nos um email para os endereços a seguir:

vulnerabilities-premium-suite-pt-br@avira.com

11. Referência: Opções de Configuração

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

11.1 Scanner

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

11.1.1 Varredura

É possível definir o comportamento da rotina de varredura por demanda (Opções disponíveis somente no modo avançado). 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.

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.

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 detecções

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

Interativo

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

Nota
A ação **Quarentena** é pré-selecionada por padrão na notificação do System Scanner. Outras ações podem ser selecionadas em um menu contextual.

Arquivos compactados

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. (Opções disponíveis somente no modo avançado.)

Varrer arquivos compactados

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

Todos os tipos de arquivamento

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 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.

Recursividade máxima

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

Valores padrão

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

Arquivos compactados

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

Exceções

Objetos do arquivo devem ser ignorados do Scanner. (Opções disponíveis somente no modo avançado.)

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.

Heurística

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

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.

11.1.2 Relatório

O System Scanner tem uma função de relatório abrangente. Com ela, você obtém informações precisas sobre os resultados de uma verificação sob demanda. O arquivo de relatório contém todas as entradas do sistema, bem como alertas e mensagens da verificação sob demanda. (Opções disponíveis somente no modo avançado.)

> **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 modo avançado.

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.

11.2 Real-Time Protection

A seção **Real-Time Protection** da configuração é responsável pela configuração da varredura durante o acesso. (Opções disponíveis somente no modo avançado.)

11.2.1 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. (Opções disponíveis somente no modo avançado.)

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.

Modo de varredura

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

Verificar durante a leitura

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

Verificar durante a escritura

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

Verificar durante a leitura e escritura

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

Unidades

Monitorar unidades de rede

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

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. (Opções disponíveis somente no modo avançado.)

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.

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. (Opção disponível somente no modo avançado.)

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. (Opções disponíveis somente no modo avançado.)

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 objetos quando forem acessados com nomes curtos de arquivo DOS (convenção de nome DOS 8.3), o nome curto relevante do arquivo também 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.

Heurística

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

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.

11.2.2 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. (Opções disponíveis somente no modo avançado.)

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.

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.

11.3 Atualização

Na seção **Atualizar** é possível configurar o recebimento automático de atualizações. Você pode especificar vários intervalos de atualização.

Atualização automática

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. (Opção disponível somente no modo avançado.)

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. (Opção disponível somente no modo avançado.)

11.3.1 Servidor da web

Servidor da web

A atualização pode ser realizada diretamente através de um servidor da web na Internet. (Opções disponíveis somente no modo avançado.)

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.

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`

11.4 Backup

A funcionalidade Avira Backup pode ser configurada em **Configuração > Proteção local > Backup**. (Opções disponíveis apenas no Modo avançado.)

11.4.1 Configurações

Em **Configurações** é possível configurar o comportamento do componente Backup.

Fazer backup somente dos arquivos modificados

Se essa opção for ativada, um backup incremental é criado. Somente arquivos que foram modificados desde o último backup são salvos no perfil de backup. Se essa opção for desativada, um backup completo é criado para cada perfil de backup salvo: todos os arquivos são salvos no perfil de backup. Essa opção é ativada como configuração padrão e é recomendada, pois os backups incrementais podem ser criados com mais rapidez e consomem menos recursos que backups completos.

Verificar por malware antes do backup

Se essa opção for ativada, os arquivos que estão sendo salvos serão verificados quanto a vírus e malware durante o backup. Os arquivos infectados não são salvos. Essa opção é ativada como configuração padrão e é recomendada.

11.4.2 Exceções

Em **Exceções** é possível especificar quais objetos de arquivo e tipos de arquivo são salvos e quais não são salvos no backup.

Arquivos ignorados no backup

A lista dessa janela contém os arquivos e os caminhos que não são salvos no backup.

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

Nota
Os arquivos incluídos nessa lista são registrados no Arquivo de relatório.

Caixa de entrada

Insira os nomes dos objetos de arquivo que não devem ser salvos nessa caixa. O caminho do diretório temporário das configurações locais do usuário conectado é inserido como padrão.

O botão abre uma janela na qual é possível selecionar o arquivo ou caminho desejado.
Um arquivo específico do backup pode ser isolado se você tiver o nome completo e o caminho do arquivo. Se tiver inserido um nome ou caminho de arquivo, todos os arquivos com esse nome (independentemente do caminho ou da unidade) não serão salvos.

Adicionar

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

Excluir

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

Redefinir lista

Esse botão restaura os valores padrão predefinidos.

Observe o seguinte:

- O nome do arquivo pode conter somente os caracteres curinga * (qualquer número de caracteres) e ? (um único caractere).
- A lista é processada de cima para baixo.
- Se um diretório for excluído, todos os subdiretórios também são excluídos automaticamente.
- Extensões de arquivo individuais também podem ser excluídas (inclusive curingas).
- Para excluir também objetos quando forem acessados com nomes curtos de arquivo DOS (convenção de nome DOS 8.3), o nome curto relevante do arquivo também deve ser inserido na lista.

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

```
C:\Program Files\Application\applic*.exe\
```
Essa entrada não é válida e não é tratada como exceção!

Exemplos:

- `application.exe`
- `\Arquivos de programas\`
- `C:\*.*`
- `C:\*`
- `*.exe`
- `*.xl?`
- `*.*`
- `C:\Program Files\Application\application.exe`
- `C:\Program Files\Application\applic*.exe`
- `C:\Program Files\Application\applic*`
- `C:\Program Files\Application\applic?????.e*`
- `C:\Program Files\`
- `C:\Program Files`
- `C:\Program Files\Application\*.mdb`

Listas de extensões de arquivo

Considerar todas as extensões de arquivo

Se essa opção for ativada, todos os arquivos do perfil de backup são salvos.

Permitir que a lista de extensões seja excluída

Se essa opção for ativada, todos os arquivos do perfil de backup serão salvos, exceto os arquivos cujas extensões estiverem inseridas na lista de extensões de arquivo excluídas.

Extensões de arquivo

Esse botão abre uma caixa de diálogo que exibe todas as extensões de arquivo não salvas durante um backup quando a opção "**Permitir que a lista de extensões seja excluída** estiver ativada. Entradas padrão são definidas para as extensões, mas as entradas podem ser adicionadas ou excluídas.

Permitir que a lista de extensões seja incluída

Se essa opção for ativada, somente os arquivos cujas extensões tenham sido inseridas na lista de extensões a serem consultadas são salvos.

Extensões de arquivo

Esse botão abre uma caixa de diálogo que exibe todas as extensões de arquivo salvas durante um backup quando a opção "**Permitir que a lista de extensões de**

arquivo seja incluída estiver ativada. Entradas padrão são definidas para as extensões, mas as entradas podem ser adicionadas ou excluídas.

11.4.3 Relatório

O componente Backup inclui uma função de registro abrangente.

Relatório

Este grupo permite determinar o conteúdo do arquivo do relatório.

Desligado

Se essa opção for ativada, o componente Backup não cria um registro. Desative a função de registro somente em casos excepcionais.

Padrão

Se essa opção for ativada, o componente Backup registra informações importantes (sobre salvamento, detecções de vírus, alertas e erros) no arquivo de relatório e as informações menos importantes são ignoradas para facilitar a compreensão. Essa opção é ativada como configuração padrão.

Estendido

Se essa opção for ativada, o componente Backup inclui informações menos importantes no arquivo de relatório.

Concluído

Se essa opção for ativada, o componente Backup inclui todas as informações sobre o processo de backup e a verificação de vírus no arquivo de relatório.

11.5 FireWall

11.5.1 Avira FireWall

A seção **FireWall** em **Configuração > Proteção na Internet** é responsável pela configuração do Avira FireWall .

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. (Opções disponíveis somente no modo avançado.)

- 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. **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. **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 monitorar o 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 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**.

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.

- Para alterar a configuração avançada das regras de aplicativo, primeiro ative a opção **Modo Especialista** na janela **Configuração**.
- Em seguida, 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 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. (Opção disponível somente no modo avançado.)
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**. (Opções disponíveis apenas no Modo avançado.)

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 automaticamente permissão 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 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 disponíveis apenas no Modo avançado.

Opções avançadas

Interromper o Firewall do Windows na inicialização

Se essa opção for ativada, o Firewall do Windows é desativado quando o computador for reiniciado. Essa opção é ativada como 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 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 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.

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

Opções disponíveis apenas no Modo avançado.

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 usadoLembrar 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 usadoLembrar 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.

11.6 Web Protection

A seção **Web Protection** em **Configuração > Proteção na Internet** é responsável pela configuração da Web Protection.

11.6.1 Varredura

A Web Protection 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 Web Protection. (Opções disponíveis somente no modo avançado.)

Verificar

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 detecções

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

Interativo

Se essa opção for ativada, uma caixa de diálogo aparecerá quando um vírus ou programa indesejado for detectado durante uma verificação sob demanda, na qual você poderá especificar o que deve ser feito com o arquivo afetado. Essa opção é ativada como configuração padrão.

Mostrar barra de andamento

Se essa opção for ativada, uma notificação será exibida na área de trabalho com uma barra de andamento de download se o download de um conteúdo do site ultrapassar o tempo limite de 20 segundos. Esta notificação foi criada especialmente para fazer download de sites com volumes maiores de dados: se estiver navegando com a Web Protection, o conteúdo do site não será baixado de modo incremental no navegador, pois ele será verificado quanto à presença de vírus e malware antes de ser exibido no navegador. Essa opção é desativada como configuração padrão.

Clique aqui para obter mais informações.

Automático

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

Ação primária

Ação primária é a ação realizada quando a Web Protection 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 Web Protection 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 Web Protection para seu navegador. O acesso ao arquivo é permitido e o arquivo é ignorado.

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

Solicitações bloqueadas

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 Web Protection. O filtro da Web permite que você bloqueie URLs conhecidos de phishing e malware. A Web Protection impede a transferência de dados da Internet para seu computador. pecialista. (Opções disponíveis somente no modo avançado.)

A Web Protection 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 Web Protection.

Caixa de entrada

Nessa caixa, insira os nomes dos tipos MIME e dos tipos de arquivo que devem ser bloqueados pela Web Protection. Para tipos de arquivo, insira a extensão, 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 Web Protection > 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 Web Protection.
- `application/olescript` = os arquivos de tipo MIME application/olescript (arquivos de script ActiveX *.axs) são bloqueados pela Web Protection.
- `.exe` = todos os arquivos com a extensão .exe (arquivos executáveis) são bloqueados pela Web Protection.
- `.msi` = todos os arquivos com a extensão .msi (arquivos do Windows Installer) são bloqueados pela Web Protection.

Adicionar

O botão permite copiar os tipos MIME e de arquivo do campo de entrada na janela de exibição.

Excluir

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

Filtro da Web

O filtro da Web baseia-se em um banco de dados interno, atualizado diariamente, que classifica os URLs de acordo com o conteúdo.

Ativar filtro da Web

Quando a opção está ativada, todos os URLs que correspondem às categorias selecionadas na lista de filtro da Web são bloqueados.

Lista de filtro da Web

Na lista de filtro da Web, é possível selecionar as categorias de conteúdo cujos URLs devem ser bloqueados pela Web Protection.

Nota
O filtro da Web é ignorado para as entradas na lista de URLs excluídos em Web Protection > 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 Web Protection. Os tipos MIME e os URLs especificados são ignorados pela Web Protection, isto é, os dados não são verificados em busca de vírus e malwares quando são transferidos para seu computador. (Opções disponíveis somente no modo especialista.)

Tipos MIME ignorados pela Web Protection

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

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

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

Caixa de entrada

Nessa caixa, é possível inserir o nome dos tipos MIME e dos tipos de arquivo a serem ignorados pela Web Protection durante a verificação. Para tipos de arquivo, insira a extensão, por exemplo, **.htm**. Para tipos MIME, indique o tipo de mídia e, quando aplicável, o subtipo. As duas instruções são separadas uma da outra por uma única barra, por exemplo, **video/mpeg** ou **audio/x-wav**.

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 Web Protection > Verificar > Solicitações bloqueadas) ou pela Web Protection: 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 Web Protection
- `video/quicktime` = Todos os arquivos de vídeo do subtipo Quicktime (*.qt, *.mov) são excluídos das verificações da Web Protection
- `.pdf` = Todos os arquivos Adobe PDF são excluídos das verificações da Web Protection.

Adicionar

O botão permite copiar os tipos MIME e de arquivo do campo de entrada na janela de exibição.

Excluir

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

URLs ignoradas pela Proteção da Web

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

Caixa de entrada

Nessa caixa, é possível inserir os URLs (endereços da Internet) a serem excluídos das verificações da Web Protection, por exemplo, `www.domainname.com`. Você pode especificar 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 Web Protection: Para todas as entradas na lista de URLs excluídos, as entradas no filtro de web (consultar Web Protection > 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 Web Protection.

Adicionar

O botão permite copiar o URL inserido no campo de entrada (endereço da Internet) na janela do visualizador.

Excluir

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

Exemplos: URLs ignorados

- `www.avira.com` -OU- `www.avira.com/*`
  = Todos os URLs com o domínio `www.avira.com` são excluídos das verificações da Web Protection: *www.avira.com/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 Web Protection.

- `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 Web Protection: A especificação implica todos os subdomínios existentes para `.avira.com`: *www.avira.com*, *forum.avira.com*, etc.
- `avira.` -OU- `*.avira.*`
  = Todos os URLs com o domínio de segundo nível `avira` são excluídos das verificações da Web Protection: A especificação implica todos os domínios de nível superior ou subdomínios 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 Web Protection: *www.domain.com*, *www.new-domain.de*, *www.sample-domain1.de*, ...
- `net` -OU- `*.net`
  = Todos os URLs com o domínio de nível superior `net` são excluídos das verificações da Web Protection: *www.name1.net*, *www.name2.net*, etc.

Aviso
Insira o URLs que deseja excluir da verificação da Web Protection 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 Web Protection através das especificações globais em exclusões. É recomendado especificar pelo menos o domínio de segundo nível completo e o domínio de nível superior: `domainname.com`

Heurística

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

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.

11.6.2 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.

11.7 Mail Protection

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

11.7.1 Varredura

Use a Mail Protection para executar varredura de e-mails de entrada em busca de vírus, malware e spam. 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.

Varredura de e-mails de entrada

Se essa opção for ativada, os e-mails de entrada serão verificados em busca de vírus, malware e spam. 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. (Opção disponível somente no modo avançado.)

Padrão

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

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. (Opção disponível somente no modo avançado.)

Padrão

Esse botão redefine a porta especificada como a porta IMAP padrão. (Opção disponível somente no modo avançado.)

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. (Opção disponível somente no modo avançado.)

Padrão

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

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 disponível somente no modo avançado e 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. (Opções disponíveis somente no modo avançado.)

> **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.

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 Mail Protection encontra um vírus ou programa indesejado em um email ou anexo. (Opções disponíveis somente no modo avançado.)

> **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 verificação. (Opções disponíveis somente no modo avançado.)

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

Seu produto Avira contém uma heurística para vírus de macro altamente poderosa. Se essa opção for ativada, todas as macros no documento em questão serão excluídas em caso de reparo, como alternativa, 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 malwares (novos) desconhecidos. Se essa opção for ativada, você poderá definir até que ponto essa heurística deve ser agressiva. Essa opção é ativada como configuração padrão.

Nível de detecção baixo

Se essa opção for ativada, 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 Mail Protection 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 Mail Protection 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. (Opções disponíveis somente no modo avançado.)

> **Nota**
> A função AntiBot só poderá ser usada se a verificação de emails de saída da Mail Protection estiver ativada (consulte a opção **Verificar nos emails de saída** em Mail Protection > Verificar).

Servidores permitidos

Todos os servidores dessa lista são autorizados pela Mail Protection para enviar e-mails: emails enviados para esses servidores **não** são bloqueados pela Mail Protection. 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 Mail Protection 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 Mail Protection para enviar e-mails: E-mails enviados deste endereço de email **não** são bloqueados pela Mail Protection. 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 Mail Protection 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.

11.7.2 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.

Note
É possível usar os curingas ao inserir os endereços de email: ***** para qualquer número de caracteres **?** somente para um caractere. No entanto, os caracteres curinga podem ser usados exclusivamente para os endereços de email que não são verificados quanto a spam. Uma mensagem de erro será exibida se você tentar excluir um endereço que contém caracteres curinga da verificação de malware marcando a caixa de listagem de exclusão **Malware**. Ao inserir endereços com caracteres curinga, a sequência de caracteres especificada deve condizer com a estrutura de um endereço de email (*@*.*).

Aviso
Observe os exemplos fornecidos quanto ao uso de caracteres curinga. Use os caracteres curinga somente de modo seletivo e tome cuidado com os endereços de email que contêm caracteres curinga e estão incluídos na lista de permissões de spam.

Exemplos: O uso de curingas em endereços de email (lista de permissões de spam)

- `virus@avira.* /` = todos os e-mails com este endereço e qualquer domínio de nível superior: virus@avira.de, virus@avira.com, virus@avira.net, etc.

- `*@avira.com` = todos os e-mails enviados do domínio **avira.com**: info@avira.com, virus@avira.com, contakt@avira.com, employee@avira.com
- `info@*.com` = todos os endereços de email com domínio de nível superior **com** e o endereço **info**: o domínio de segundo nível pode ser qualquer coisa: info@name1.com, info@name2.com,...

Adicionar

Com esse botão, é possível adicionar o endereço de 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.

Spam

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

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.

Importar catálogo de endereços do Outlook

Com esse botão, você importa os endereços de email do catálogo de endereços do programa de email MS Outlook para a lista de exceções. Os endereços de email importados não são verificados quanto a spam.

Importar catálogo de endereços do Outlook Express (Windows XP) / Importar catálogo de endereços do Windows Mail (Windows Vista, Windows 7)

Use esse botão para importar o endereço de email do catálogo de endereços dos programas de email MS Outlook Express ou Windows Mail para a lista de exceções. Os endereços de email importados não são verificados quanto a spam.

Cache

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

Cópias dos emails de entrada também são armazenadas no cache. Os emails também podem ser usados para as funções de treinamento do módulo antispam (*Bom email use para treinamento*, *Spam use para treinamento*).

> **Nota**
> O módulo antispam deve ser ativado para que o backup dos emails de entrada seja feito no cache.

Número máximo de emails em cache

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

Máximo de dias de armazenamento de email

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

Esvaziar cache

Clique nesse botão para excluir os emails armazenados no cache.

Rodapé

Em **Rodapé**, é possível configurar um rodapé de e-mail que é exibido nos e-mails enviados. (Opções disponíveis somente no modo avançado.)

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.

AntiSpam

O serviço do Avira Mail Protection verifica emails e anexos em busca de vírus e programas indesejados. Além disso, ele pode proteger você contra emails de spam de modo confiável. (Opções disponíveis somente no modo especialista.)

Ativar módulo AntiSpam

A ativação dessa opção ativa a função antispam da Mail Protection.

Marcar assunto do email

Se essa opção é ativada, uma observação é adicionada à linha de assunto original quando um email de spam é detectado.

Simples

Se o email de spam ou phishing for recebido, a marca [SPAM] ou [Phishing] será adicionada. Essa opção é ativada como configuração padrão.

Detalhado

A linha de assunto de um email de spam ou phishing tem uma marca no início que chama a atenção para a probabilidade da mensagem ser spam.

Ativar registro

Se essa opção for ativada, a Mail Protection criará um arquivo de relatório antispam especial.

Usar blacklists em tempo real (RBL)

Quando essa opção é ativada, a chamada "lista negra" é consultada em tempo real, fornecendo informações adicionais para classificar email de origem duvidosa como spam.

Tempo limite: n segundo(s)

Se as informações da lista negra não forem disponibilizadas depois de n segundos, a tentativa de consultar a lista negra será cancelada.

Limpar banco de dados de treinamento

Clique no botão para excluir o banco de dados de treinamento.

Adicionar automaticamente o destinatário do email enviado na whitelist

Se essa opção for ativada, os endereços dos destinatários dos emails de saída serão adicionados automaticamente à lista de permissões de spam (lista dos emails não verificados em busca de spam, definida em **Mail Protection > Geral > Exceções**). Os emails de entrada enviados dos endereços da lista de permissões de spam não são verificados em busca de spam. No entanto, eles são verificados quanto a vírus e malwares. Essa opção é desativada como configuração padrão.

Nota
Esta função só poderá ser usada se a verificação de emails de saída da Mail Protection estiver ativada (Consulte a opção **Verificar nos emails de saída** em Mail Protection > Verificar)

11.7.3 Relatório

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

Relatório

Este grupo permite determinar o conteúdo do arquivo do relatório.

Desativado

Se essa opção for ativada, a Mail Protection não criará um registro.
É recomendado desativar a função de registro somente em casos excepcionais, por exemplo, se você executar avaliações com vários vírus ou programas indesejados.

Padrão

Se essa opção for ativada, a Mail Protection registrará informações importantes (sobre detecções, alertas e erros) no arquivo de relatório, e as informações menos importantes serão ignoradas para facilitar a compreensão. Essa opção é ativada como configuração padrão.

Estendido

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

Concluído

Se essa opção for ativada, a Mail Protection registrará todas as informações no arquivo de relatório.

Limitar arquivo de relatório

Limitar tamanho 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 relatório

Se essa opção for ativada, o backup do arquivo de relatório será feito antes de sua redução.

Gravar configuração no relatório

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

11.8 Proteção para crianças

Use os recursos *PROTEÇÃO PARA CRIANÇAS* do Avira, para assegurar uma experiência na Internet segura para seus filhos ou outras pessoas que usam seu computador.

- Com o recurso **Safe Browsing**, você pode designar uma função para cada usuário do Windows em seu computador. Para cada função, você pode definir quais URLs ou categorias de conteúdo da Internet devem ser permitidas ou negadas, bem como os períodos de navegação diária ou limites de tempo.

Tópicos relacionados:

- Sobre Safe Browsing

11.8.1 Safe Browsing

Você pode usar a função **Safe Browsing** para filtrar conteúdo da Internet indesejável ou ilegal e para limitar a duração de uso da Internet. A função **Safe Browsing** faz parte do componente *Proteção para Crianças*.

Você pode designar funções de usuário às contas de usuário do Windows em seu computador. Cada função de usuário contém um conjunto de regras com os seguintes critérios:

- URLs permitidas e bloqueadas (endereços de Internet)
- Categorias de URL proibidas
- Duração do uso da Internet e, se necessário, períodos de uso permitidos durante a semana

Para bloquear o conteúdo da Internet de acordo com categorias específicas, o Avira usa listas de URL poderosas, que filtram as URLs com base no conteúdo da página da web. As listas de filtros de URL são atualizadas, adaptadas e expandidas por hora. As funções de **Criança**, **Adolescente** e **Adulto** são pré-configuradas com as categorias proibidas relevantes. O uso da Internet é registrado com base em solicitações da Internet que duram pelo menos 5 minutos.

Se **Safe Browsing** estiver ativado, todas as páginas da web solicitadas pelo usuário serão filtradas de acordo com a função de usuário. Se uma página da web for bloqueada, uma mensagem será exibida no navegador. Se a duração de uso permitida for excedida ou se o uso ocorrer fora do período permitido, os sites solicitados serão bloqueados e uma mensagem será exibida no navegador.

Aviso
Observe que, para usar a função **Safe Browsing**, você deve ativar o serviço **Web Protection**.

Aviso
Proteja a configuração de seu produto Avira com uma senha quando ativar o **Safe Browsing**. Se a configuração não for protegida por uma senha, todos os usuários do computador poderão alterar ou desativar as configurações de **Safe Browsing**. A proteção por senha é ativada em Configuração > Geral > Senha.

Tópicos relacionados:

- Ativando o Safe Browsing
- Designando uma Função de Safe Browsing
- Configuração de Safe Browsing

Ativando o Safe Browsing

- Abra o Avira Control Center e clique em **Status** na barra de navegação.

  Para usar a função Safe Browsing, você deve ativar o serviço **Web Protection**.

- Se necessário, ative o serviço **Web Protection** clicando no comutador vermelho próximo a ele na visualização **Status** em *Proteção na Internet*.

  O status de **Web Protection** deve ser verde (I), quando ativado.

  Ative o serviço **Safe Browsing**, clicando no comutador vermelho próximo a ele na visualização **Status**.

  O status de **Safe Browsing** deve ser verde (I), quando ativado.

- Para configurar o perfil de Safe Browsing para seu filho ou um outro usuário, clique no botão de configuração próximo a **Safe Browsing** na visualização **Status**.

Tópicos relacionados:

- Sobre Safe Browsing
- Designando uma Função de Safe Browsing
- Configuração de Safe Browsing

Designando uma Função de Safe Browsing

Pré-requisitos:

✓ Verifique se você configurou contas do Windows separadas para cada pessoa que usa o computador no qual o Avira está instalado. Você pode designar uma função de Safe Browsing para cada conta de usuário do Windows.
✓ Ative a função **Safe Browsing** em seu produto Avira.
✓ Verifique as configurações para cada função e, eventualmente, altere-as antes de designar as funções aos usuários.

- Na visualização **Status**, clique no botão de configuração próximo a **Safe Browsing**.
- Na lista suspensa **Seleção do Usuário**, selecione o nome do usuário ao qual deseja designar uma função.

  A lista contém as contas do usuário do Windows configuradas em seu computador.

- Clique no botão **Adicionar**.

  ↳ O usuário é adicionado à lista.

  O Avira Internet Security é fornecido com três funções do usuário pré-configuradas:

  - **Criança**
  - **Adolescente**
  - **Adulto**

  Por padrão, quando você adiciona um usuário na lista, a função designada é **Criança**.

- Você pode designar uma outra função clicando na função para o respectivo usuário diversas vezes.

Observação
Quando **Safe Browsing** é ativado, os usuários padrão do computador, que não tiveram uma função designada durante a configuração de Safe Browsing, têm a função **Criança** designada. Você também pode alterar a função do usuário **Padrão**.

- Clique em **Aplicar**, para salvar a configuração.

Tópicos relacionados:

- Alterando as propriedades de uma função
- Adicionando ou removendo uma função

Alterando as propriedades de uma função

- Na visualização **Status**, clique no botão de configuração próximo a **Safe Browsing**.
- Se necessário, ative o **Modo avançado** clicando no comutador verde próximo a ele.

  Quando ativado, o status do **Modo avançado** é amarelo (I).

  ↪ Na janela de configuração **Safe Browsing**, são exibidas as opções de **Funções**.
- Clique no nome da função que deseja alterar (por exemplo, **Adolescente**), em seguida, clique no botão **Alterar**.

  ↪ É exibida a janela **Propriedades** para a função selecionada.
- Faça as alterações desejadas, em seguida, clique em **OK**.

Tópicos relacionados:

- Propriedades da Função
- Configuração de Safe Browsing

Adicionando ou removendo uma função

- Na visualização **Status**, clique no botão de configuração próximo a **Safe Browsing**.
- Se necessário, ative o **Modo avançado** clicando no comutador verde próximo a ele.

  Quando ativado, o status do **Modo avançado** é amarelo (I).

  ↪ Na janela de configuração Safe Browsing, são exibidas as opções de **Funções**.
- Para excluir uma função, clique no nome da função (por exemplo, **Adolescente**), em seguida, clique no botão **Remover**.

Observação
Você não pode excluir uma função se ela foi designada a um usuário.

- Para adicionar uma nova função, digite um nome de função no campo de entrada (máximo de 30 caracteres), em seguida, clique no botão **Novo**.
- Selecione o nome da nova função na lista de funções e clique no botão **Alterar**, para editar suas propriedades.

Tópicos relacionados:

- Configuração de Safe Browsing
- Propriedades da Função
- Designando uma Função de Safe Browsing

Se você tiver definido uma senha para a **Safe Browsing**, a configuração será ocultada e o botão **Protegido por senha** será exibido.

Protegido por senha

Para ativar a configuração "**Safe Browsing**", pressione o botão "**Protegido por senha**" e insira a senha na janela "**Inserir senha**".

Safe Browsing ativar

Se essa opção for ativada, todas as páginas da Web solicitadas pelo usuário enquanto navega na Internet serão verificadas com base na função atribuída ao usuário registrado na função "**Safe Browsing**". As páginas da Web solicitadas serão bloqueadas se tiverem sido classificadas como bloqueadas na função atribuída.

Nota
Quando a **Safe Browsing** for ativada, usuários *padrão* do computador, que não foram atribuídos um papel durante a configuração **Safe Browsing** são atribuídos o papel de **Criança**. É possível alterar a função do usuário *padrão*. Após a instalação, as funções de **Criança**, **Adolescente** e **Adulto** são criadas. A restrição do tempo de uso da Internet está desativada para funções pré-configuradas.

Seleção do usuário

Lista suspensa do usuário

A lista contém todos os usuários do sistema.

Adicionar

O botão pode ser usado para adicionar o usuário selecionado à lista de usuários protegidos.

Excluir

O botão exclui uma entrada selecionada da lista.

Lista de funções de usuário

A lista mostra todos os usuários adicionados e suas respectivas funções. Quando um usuário é adicionado, o programa atribui a função de **Criança** por padrão. Com o mouse, clique na função exibida para alternar para outra função.

> **Nota**
> O usuário *Padrão* não pode ser excluído.

Funções (Opções disponíveis somente no modo avançado.)

Caixa de entrada

Nesse campo, é possível inserir o nome da função que deseja adicionar às funções de usuário.

Alterar

O botão **Alterar** pode ser usado para configurar a função selecionada. Uma caixa de diálogo é exibida na qual é possível definir os URLs bloqueados e permitidos para a função e o conteúdo da Web proibido selecionado por categoria. (consulte Propriedades de função).

Novos

Com esse botão, é possível adicionar a função inserida na caixa de entrada à lista de funções disponíveis.

Remover

O botão exclui uma função realçada da lista.

Lista

A lista mostra todas as funções adicionadas. Clique duas vezes em uma função exibida para abrir a caixa de diálogo que permite definir a função.

> **Nota**
> As funções que já foram atribuídas a um usuário não podem ser excluídas.

Tópicos relacionados:

- Sobre a Navegação segura
- Propriedades de função
- Duração de uso
- Período de uso

Propriedades de função

A janela **Propriedades de função** permite definir uma função selecionada para usar a Internet. (Opções disponíveis somente no modo avançado.)

Você pode permitir ou proibir explicitamente o acesso aos URLs. É possível bloquear categorias específicas de conteúdo da Web com base na seleção. Você também pode restringir o tempo de uso da Internet.

Controlar acesso aos seguintes URLs

A lista mostra todos os URLs adicionados com as funções **Bloquear** ou **Permitir**. Quando um URL é adicionado, o programa atribui a regra **Bloquear** por padrão. Para alternar a regra atribuída, clique nela.

Adicionar URL

Nesse campo, é possível especificar os URLs a serem controlados pela função de controle dos pais. 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`). Você também pode usar o caractere curinga ***** para qualquer número de caracteres. Os pontos no início ou no final também podem ser usados junto com os caracteres curinga para indicar o nível do domínio.

Nota
As regras de URL são priorizadas de acordo com o número de rótulos especificados do domínio. Quanto mais rótulos do domínio forem especificados, maior será a prioridade da regra. Por exemplo:
URL: `www.avira.com` - regra: `Permitir`
URL: `.avira.com` - regra: `Bloquear`
O conjunto de regras permite todos os URLs no domínio *www.avira.com*. O *forum.avira.com* URL é bloqueado.

Nota
O . ou * engloba todos os URLs. Você pode usar estes detalhes, se, por exemplo, você só desejar liberar um pequeno número de páginas da web explicitamente especificadas para o papel de **Criança** como no conjunto de regras a seguir:
URL: ***** ou **.** regra: `Bloquear`
URL: `kids.yahoo.com` - regra: `Permitir`
URL: `kids.nationalgeographic.com` - regra: `Permitir`

O conjunto de regras bloqueia todas os URLs, exceto os URLs com os domínios *kids.yahoo.com* e *kids.nationalgeographic.com*.

Adicionar

Com esse botão, você pode adicionar o URL inserido à lista de URLs controlados.

Excluir

O botão exclui um URL realçado da lista de URLs controlados.

Bloquear acesso aos URLs que pertencem às seguintes categorias

Quando essa opção está ativada, o conteúdo da Web que pertence às categorias selecionadas na lista de categorias é bloqueado.

Duração de uso permitida

A opção **Duração de uso permitida** abre uma caixa de diálogo na qual é possível definir restrições de tempo de uso da Internet para as funções que estão sendo configuradas. Você pode estipular o uso da Internet por mês, por semana ou diferenciar dias úteis e fins de semana. Um diálogo permite estipular períodos exatos de uso durante a semana. Consulte Duração de uso.

Exemplos de URLs a serem controlados

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

Tópicos relacionados:

- Sobre a Navegação segura

- Configuração da navegação segura
- Duração de uso
- Período de uso

Duração de uso

Na janela **Duração de uso**, é possível estabelecer um tempo de uso da Internet máximo para uma função de usuário. Os registros de uso da Internet baseiam-se em solicitações da Internet que duram pelo menos 5 minutos. O tempo máximo de navegação obrigatório para a função pode ser especificado por semana, por mês ou diferenciado entre dias úteis e fins de semana.

Tempo limite de uso da Internet

Essa opção permite que você restrinja o tempo de uso da Internet para todos os usuários do computador com funções atribuídas. Se a duração do uso permitido for ultrapassada, os sites solicitados ou acessados pelo usuário do computador serão bloqueados. Um alerta é exibido no navegador.

Limite de tempo por semana, por mês, por dia (Segunda-feira a sexta-feira, sábado e domingo)

O tempo de uso obrigatório pode ser ajustado com o controle deslizante ou as teclas de seta para a direita da caixa de entrada. Você também pode inserir o tempo de uso diretamente nos campos de hora. Observe o formato específico para a especificação de hora.

Especificações diferentes de tempo de uso não são alinhadas pelo programa. O programa usa o menor valor aplicável a qualquer momento para restringir o tempo de uso.

Período exato de uso

O botão **Período exato de uso** abre uma caixa de diálogo na qual é possível estipular os horários do dia para o tempo máximo de uso definido. Consultar Período de uso.

Tópicos relacionados:

- Sobre a Navegação segura
- Navegação segura configuração
- Propriedades de função
- Período de uso

Período de uso

Na janela **Período de uso** você pode definir os tempos de uso permitidos para a função selecionada. Você pode definir horários específicos do dia para o uso da Internet.

Permitir somente o uso da Internet nos períodos especificados

Essa opção permite que você estipule horas do dia para “navegar” para todos os usuários do computador com uma função configurada. Se o usuário tentar usar a internet fora das horas estipuladas, os sites solicitados serão bloqueados. Uma mensagem é exibida no navegador.

- Para especificar horários do dia para o uso da Internet, realce os campos de hora desejados.

  Você tem as seguintes opções para definir os intervalos de tempo permitidos e proibidos:

  - **Para definir um tempo de navegação permitido**: Clique nos campos de tempo não realçados ou arraste o botão esquerdo do mouse sobre os mesmos.
  - **Para definir um tempo de navegação**: Clique nos campos de tempo não realçados ou arraste o botão esquerdo do mouse sobre os campos de tempo realçados.

- Clique com o botão direito do mouse em uma área realçada ou não realçada na linha do dia, para exibir uma janela de detalhes, contendo o intervalo definido para esse dia da semana. Exemplo:
  Uso da Internet bloqueado de 00:00 até 11:00.

Tópicos relacionados:

- Sobre a Navegação segura
- Configuração da navegação segura
- Propriedades de função
- Duração de uso

11.9 Proteção Móvel

11.9.1 Proteção Móvel

Avira não só protege o seu computador de malware e vírus, mas também protege de perda e roubo o seu smartphone que opera com o sistema operacional Android. Com o Avira Free Android Security você também pode bloquear chamadas ou SMS indesejados. Basta adicionar números de telefone do Registro de chamadas, Registro de SMS e da lista de contatos à lista negra, ou criar manualmente um contato que pretende bloquear.

Mais informações podem ser encontradas no nosso site:

http://www.avira.com/android

11.9.2 Android Security

Avira Free Android Security

O Avira Free Android Security consiste em dois componentes:

- o próprio aplicativo, instalado no dispositivo Android
- o Console da web Avira Android para registro e controle de recursos

Requisitos do sistema

Sistema operacional:

- Android 2.2 (Froyo)
- Android 2.3.x (Gingerbread)
- Android 4.0.x (Ice Cream Sandwich)
- Android 4.1.x (Jelly Bean)

Memória:

- 1,72 MB de espaço livre na memória interna.

Navegadores:

- Mozilla Firefox
- Google Chrome
- Opera
- Internet Explorer IE7 ou superior.

> **Nota**
> Observe que Java deve estar instalado, JavaScript deve estar ativado e é necessário uma conexão com a Internet em funcionamento.

Recursos

Para proteger a sua privacidade e os seus dados pessoais, se não encontrar o seu dispositivo, o Avira Free Android Security oferece quatro funcionalidades por meio do Console da web Avira Android:

Grito remoto

É acionado um alarme no dispositivo que dura 20 segundos.

Rastreio de Localização remota

É ativado um comando de localização que devolve os parâmetros de localização do dispositivo.

Bloqueio remoto

É possível bloquear o dispositivo imediatamente utilizando um PIN de 4 dígitos.

Apagamento remoto

É possível remover dados do cartão SIM ou dos cartões de memória internos e externos. Também é possível efetuar redefinição de fábrica do dispositivo no Console da web.

> **Nota**
> Para disparar um comando **Redefinição de Fábrica** para excluir todos os dados do seu dispositivo em caso de perda ou furto, a função **Administrador do dispositivo** deve ser ativada durante a configuração.

Para bloquear determinados números de telefone, o Avira Free Android Security oferece no seu dispositivo a funcionalidade chamada de lista negra.

Lista negra

É possível adicionar contatos à lista negra a partir do Registro de chamadas, do Registro de SMS e da sua lista de contatos ou você pode criar manualmente um contato que deseja bloquear.

O Console da web

O Console da web Avira Android é um centro de controle baseado em navegador concebido para gerenciar as funções de segurança. O Painel de instrumentos do Console da web é utilizado para tratar da conta e disparar recursos remotos como **Localizar dispositivo**, **Bloquear**, **Disparar grito** ou **Apagar**.

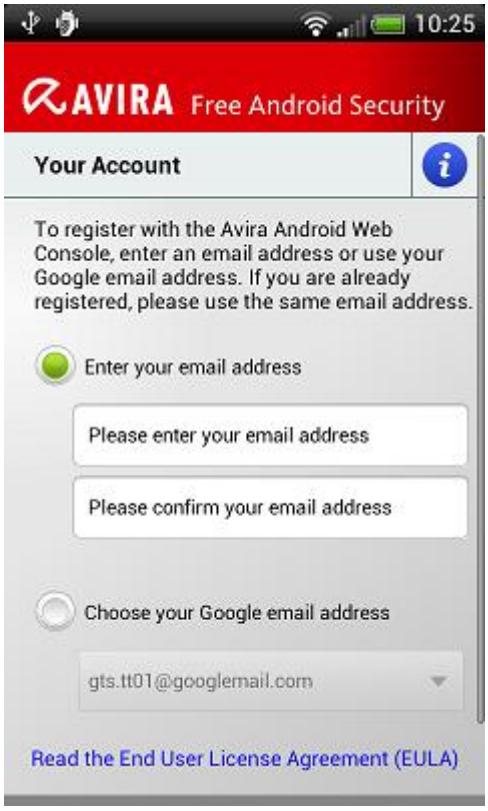
O Console da web Avira Android consiste em uma barra de título, uma barra lateral e a tela principal com várias guias. A barra de título apresenta as credenciais do logon e contém links para a seção Suporte e para o gerenciamento da Conta. Na barra lateral são listados os dispositivos registrados. Na tela principal do Console da web estão todos os recursos de segurança do aplicativo e informações sobre a funcionalidade de **Lista negra** no seu dispositivo.

Instalação e Desinstalação

Instalação e desinstalação do Avira Free Android Security

Download e instalação

Baixe o aplicativo Avira Free Android Security diretamente do Google Play para o dispositivo e instale o aplicativo. Após a instalação bem sucedida, os novos recursos do aplicativo são apresentados a você. Depois disso você é solicitado a registrar o dispositivo na tela de registro do Avira Free Android Security. Para tal, pode utilizar a sua Conta do Google ou um endereço de email de um provedor diferente. É necessária uma conexão estável com a Internet para o processo de registro.



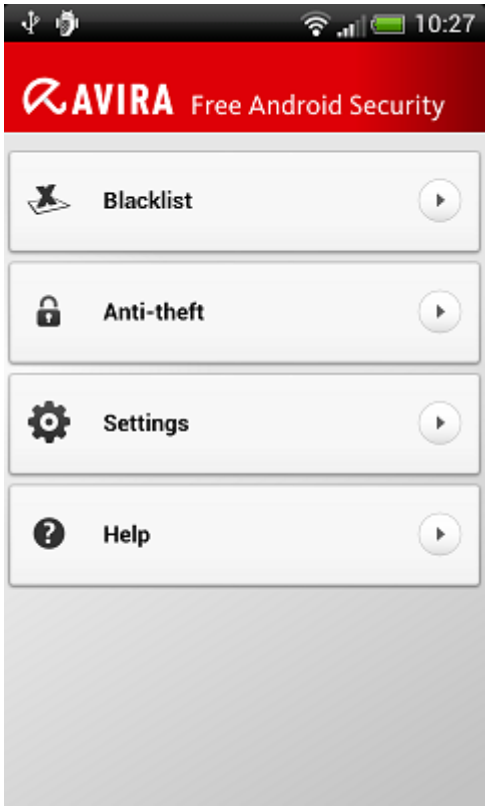
- Toque em **OK** no dispositivo para abrir o formulário de registro.
- Insira a sua conta do Google ou um endereço de email diferente.
- Toque em **Aceitar o EULA e Continuar** para continuar.
  - ↪ A Avira enviará um email de confirmação da nova conta do Avira Free Android Security para o endereço de email que estiver definido. Esse email de confirmação inclui um link que permite definir uma senha pessoal para o logon no Console da web Android.
- Clique no link no email de confirmação para definir uma senha e ativar o Console da web Android.
  - ↪ Agora é possível controlar remotamente os dispositivos utilizando o Console da web.

Para permitir que Avira Free Android Security apague todos os dados com um comando de **Redefinição de Fábrica** a partir do dispositivo – por exemplo, em caso de perda ou roubo – é necessário ativar a função **Administrador do dispositivo** durante a configuração:

- Para ativar a função **Administrador do dispositivo**, toque no botão **Ativar**.
  - ↪ O diálogo **Ativar administrador do dispositivo** será aberto.
- Confirme a ativação do **Administrador do dispositivo** tocando no botão **Ativar**.
  - ↪ Dessa forma você permite que o Avira Free Android Security apague todos os dados do dispositivo no caso de alguma vez você desejar executar um comando de **Redefinição de fábrica**.

Se não estiver seguro sobre a instalação da função **Administração do dispositivo** durante a configuração, essa opção de configuração sempre pode ser ativada mais tarde. Siga estas etapas:

- Abra o Avira Free Android Security no seu dispositivo.



- Toque no botão **Configurações**.
  - ↪ Agora pode ver que a opção para apagar todos os dados com um comando **Redefinição de fábrica** está desativada.
- Toque no campo **Apagar configurações**.
  - ↪ O diálogo **Apagar com redefinição de fábrica** é aberto. É solicitado que você ative o **Administrador do dispositivo**.
- Toque no botão **Ativar** na parte inferior do diálogo.
- Confirme a ativação do **Administrador do dispositivo** tocando em **Ativar**.
  - ↪ É informado que **Apagar com redefinição de fábrica está ativado**.

> **Nota**
> É possível ativar ou desativar a função **Administrador do dispositivo** a qualquer momento com o aplicativo Avira Free Android Security no dispositivo, escolhendo **Configurações > Apagar configurações > Apagar com redefinição de fábrica > Ativar / Desativar**.

Instalação com PC

É possível baixar o aplicativo Avira Free Android Security com o PC.

- Abra o Google Play no PC.
- Procure o aplicativo Avira Free Android Security.

- Clique em **Instalar** para baixar o aplicativo para o PC.
  - ↪ É solicitado que entre para instalar o aplicativo.
- Clique em **Entrar** para acessar a sua conta do Google.
- Insira as suas credenciais de logon
- Clique em **OK** para baixar o aplicativo para um dispositivo selecionado.
  - ↪ O aplicativo Avira Free Android Security será baixado para este dispositivo.
- Clique em **OK** para fechar o diálogo de download.
  - ↪ O site do Google Play é aberto novamente e o botão **Instalado** indica que o aplicativo já foi baixado para o dispositivo.

Desinstalação

Para desinstalar o Avira Free Android Security, duas etapas devem ser realizadas. Deve-se desinstalar o aplicativo do dispositivo e excluir o dispositivo da conta do Console da web Avira Android.

> **Nota**
> Certifique-se de que desativou a função **Administrador do dispositivo** no dispositivo antes de desinstalar o Avira Free Android Security.

Para desinstalar o Avira Free Android Security, use o assistente de desinstalação do Avira Free Android Security ou acesse o Gerenciamento de aplicativo do dispositivo.

Se usar o assistente de desinstalação, navegue do botão **Ajuda** para o botão **Acessar desinstalação**.

- Toque em **Ajuda > Desinstalar > Acessar desinstalação**.
  - ↪ A tela de informação de status sobre o administrador do dispositivo é exibida.
- Toque em **Administrador do dispositivo** para desativar o recurso, se necessário.
- Toque em **Continuar** para continuar o processo de desinstalação.
  - ↪ A tela de pesquisa de desinstalação é exibida.
- Selecione todas as respostas que se aplicam.
- Você pode escrever um comentário mais detalhado no campo de comentário.
- Toque em **Continuar** para continuar a desinstalação.
- Toque em **OK** para concluir o processo de desinstalação.

Para desinstalar o aplicativo por meio do gerenciamento de aplicativo do dispositivo, navegue do botão **Configurações** do dispositivo para a função **Gerenciar aplicativos**.

- Toque no aplicativo Avira Free Android Security e escolha **Desinstalar**.

- Confirme o processo de desinstalação.

Além disso, deve excluir o dispositivo da Conta do Avira Free Android Security do Console da web.

- Abra o Console da web Avira.
- Clique no link **Conta** na barra de título.
- Acesse Administração do Dispositivo e abra o menu suspenso **Dispositivos disponíveis**.
- Selecione o dispositivo do qual pretende excluir o Aplicativo Avira Free Android Security.
- Clique em **Excluir dispositivo** para remover o dispositivo da sua conta.

Instalação renovada

Após desinstalar todos os dispositivos, não é mais possível acessar o Console da web Avira.

É possível instalar o Avira Free Android Security novamente no dispositivo utilizando a conta de email anterior.

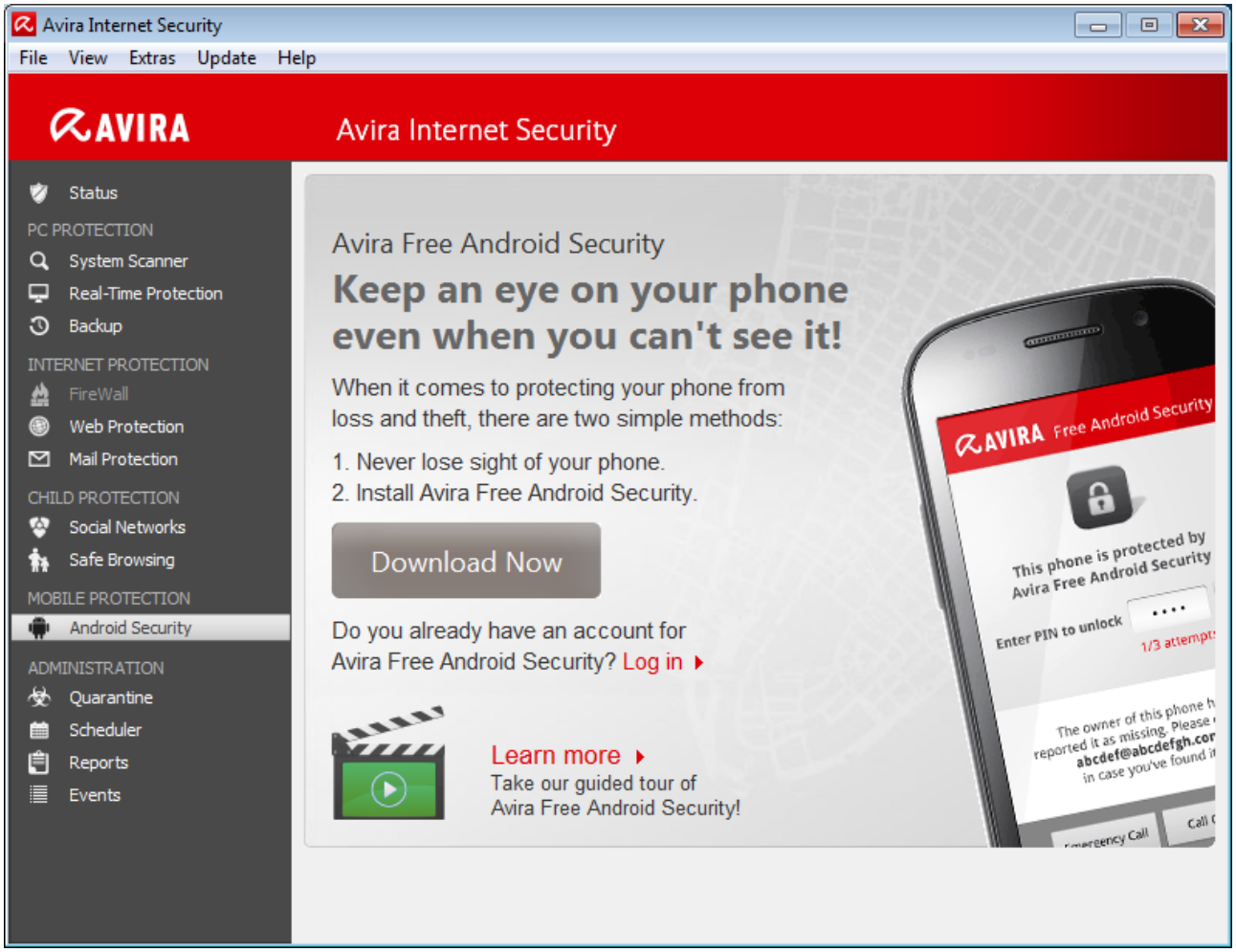
- Entre no Console da web com as credenciais de logon anteriores.
- A senha pode ser alterada após o logon navegando para o **Gerenciamento da senha**.

  Escolha **Conta > Gerenciamento da senha**, escreva a nova senha e confirme.
- Caso não se lembrar da senha, clique no link **Esqueceu sua senha?** no logon.
  - ↪ Será solicitado que nos envie o seu endereço de email e nós enviaremos um link de recuperação para que possa definir novamente a sua senha.

Criar uma conta Android

Para ficar de olho no seu dispositivo e proteger os seu dados pessoais por controles remotos a partir do Console da web é necessário criar uma conta Avira Free Android Security.

- Abra o Centro de Controle do seu produto Avira.
- Clique em **Centro de Controle > Proteção móvel > Avira Free Android Security**.
  - ↪ A página de download Avira Free Android Security é aberta.



- Clique em **Baixar Agora**.
  - ↪ A página Google Play Android Apps é aberta.

  Clique em **Instalar**.
  - ↪ É solicitado que entre para baixar o aplicativo Avira Free Android Security.

  Clique em **Entrar** no Google.

  Digite seu endereço de email e sua senha.

  Clique em **Entrar**.

  Selecione o dispositivo para o qual o Avira Free Android Security será baixado.

  Clique em **Instalar**.
  - ↪ O aplicativo é baixado para o seu dispositivo.
- Abra o Avira Free Android Security no seu dispositivo.
  - ↪ Os novos recursos do aplicativo são apresentados a você. Depois disso você é solicitado a registrar o dispositivo na tela de registro do Avira Free Android Security. Para tal, pode utilizar a sua Conta do Google ou um endereço de email de um provedor diferente.
  - ↪ A tela Sua Conta é aberta.

- Insira as suas credenciais de logon.
- Toque em **Aceitar o EULA e Continuar** para continuar.
  - ↪ A Avira enviará um email de confirmação da nova conta. Esse email de informação inclui um link que permite definir uma senha pessoal para o logon no Console da web do Avira Free Android Security.
- Clique no link no email de confirmação para definir uma senha e ativar a conta.
  - ↪ Agora você pode controlar os dispositivos utilizando o Console da web do Avira Free Android Security: https://android.avira.com

Iniciar sessão na sua conta Android

- Clique em **Centro de Controle > Proteção Móvel > Avira Free Android Security**.
  - ↪ A página de download Avira Free Android Security é aberta.
- Clique em **Iniciar sessão**.
  - ↪ A página de logon Avira Free Android Security é aberta.
- Digite o seu endereço de email registrado e a sua senha.
- Clique em **Iniciar sessão** para abrir o Console da web com as suas funções de controle.

Manipulação

O Console da web

Após a instalação com êxito é necessário registrar o dispositivo para acessar o Console da web Avira.

- O Console da web Avira consiste em uma barra de título, uma barra lateral e a tela principal com várias guias.
- A barra de título apresenta as credenciais de logon e contém links para a seção de **Suporte** e para o gerenciamento da **Conta**. Além disso, as configurações de idioma do Console da web Avira podem ser selecionadas aqui.
- Na barra lateral são listados os dispositivos registrados.
- Cada dispositivo registrado é apresentado em um único campo:
  - Clique no botão **Editar** no campo do dispositivo para ser encaminhado diretamente para a guia **Configurações** do Console da web, onde pode gerenciar o nome e o número de telefone do seu dispositivo.
- Na parte inferior da barra lateral encontra-se um link para especificar e salvar uma pergunta de segurança pessoal.
- Na tela principal do Console da web estão todos os recursos de segurança para controlar o dispositivo e informações sobre o conteúdo da lista negra.

As guias da tela Console da web

- A tela do Console da web tem as seguintes guias:
  - Painel de instrumentos
  - Localizar dispositivo
  - Apagar
  - Grito
  - Bloquear
  - Lista negra
  - Configurações

O Painel de instrumentos do Console da web do Avira Free Android Security

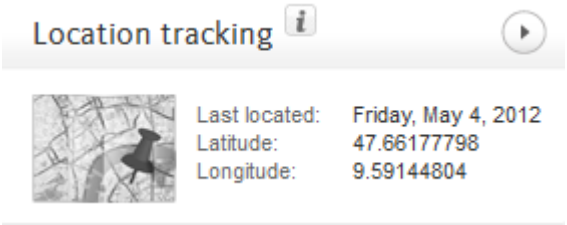
A guia Painel de instrumentos contém diversas informações sobre o dispositivo e também botões de controle para disparar ações de segurança do dispositivo.

Informações do dispositivo

- Marca: a marca do dispositivo.
- Modelo: a identificação do modelo do dispositivo.

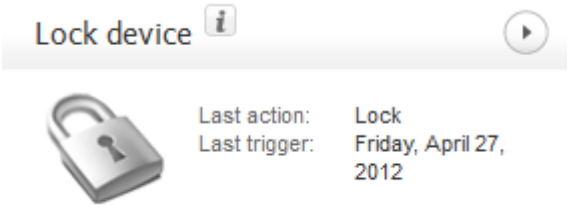
- IMEI: o IMEI (Identidade de Equipamento Móvel Internacional) é um número exclusivo de 15 dígitos para identificar celulares e alguns telefones de satélite.
- Versão de SO: o número da versão do Sistema Operacional Android.
- Versão do aplicativo: o número da versão do aplicativo Avira instalado atualmente. Um símbolo de aviso vermelho é apresentada se a versão que estiver sendo utilizada não for a atual.
- Admin. Disp.: mostra se o Administrador do Dispositivo está habilitado no momento. Um símbolo de advertência vermelho é exibido se a função não estiver habilitada.
- Bateria: informações sobre o nível de carga da bateria em porcentagem.
- N.º telefone: o número de telefone armazenado no cartão SIM.
- Rede: a rede móvel à qual pertence o cartão SIM.
- País: o país do cartão SIM.
- **Atualizar**: o botão para atualizar as informações do dispositivo.

Localização remota



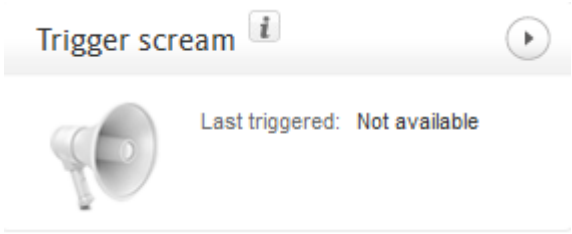
- Última localização: a hora da última vez que um dispositivo foi localizado, por exemplo, "5 horas atrás", "3 dias atrás".
- Latitude: a latitude exata da localização do dispositivo.
- Longitude: a longitude exata da localização do dispositivo.

Bloquear dispositivo



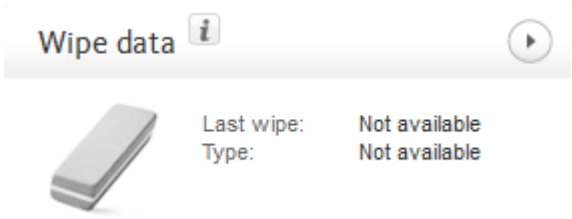
- Última ação: a última ação que foi realizada com o Console da web, por exemplo "Bloquear".
- Último gatilho: a hora da última vez que um dispositivo foi bloqueado / desbloqueado.

Disparar grito



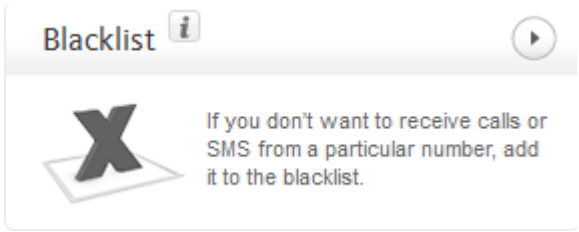
- Último gatilho: a hora da última vez em que um alarme foi enviado para o dispositivo.

Apagar dados



- Último apagamento: a hora da última vez que um dispositivo foi apagado.
- Tipo: o tipo de ação de apagamento efetuada no dispositivo.

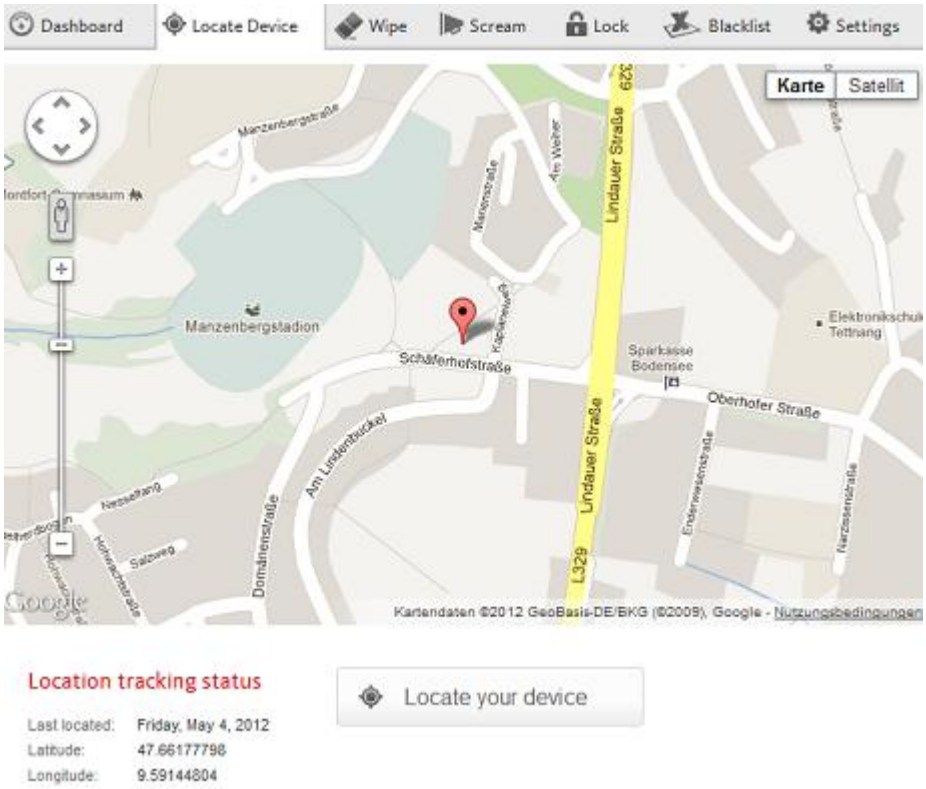
Lista negra



- Utilize esta funcionalidade para bloquear chamadas e SMS indesejados.

Localizar dispositivo

A guia Localizar dispositivo apresenta um extrato do Google Maps. Embaixo do mapa é apresentado o estado do rastreio de localização.



- Clique no botão **Localizar o dispositivo** para iniciar um rastreio de localização do dispositivo perdido.
  - ↪ O rastreio pode demorar vários minutos dependendo dos desempenhos da rede e da força do sinal do dispositivo.

Avira Free Android Security procura o dispositivo via GPS, tecnologia de torre celular e LAN sem fio.

O tempo de rastreio decorrido é mostrado durante o processo de localização.

- ↪ O resultado é que a localização do dispositivo perdido é apontada em um mapa. É possível ampliar e reduzir o mapa.

Apagar

> **Nota**
> Se a versão do Avira Free Android Security utilizada não suportar a funcionalidade **Apagar**, atualize o aplicativo do dispositivo como descrito pela nossa Base de conhecimentos. Em seguida, basta atualizar essa página para acessar a funcionalidade completa da funcionalidade **Apagar**.

Na guia Apagar encontram-se três opções para excluir dados do dispositivo. Também é possível selecionar uma combinação dessas opções de Apagar. A função Apagar leva à exclusão permanente dos dados, ou seja, os dados destruídos pelo procedimento de apagar não podem ser recuperados.

Nota
é fortemente recomendável bloquear o dispositivo para disparar um comando de apagar. Faça backup regularmente dos dados importantes. Quando for necessário apagar o dispositivo, não há oportunidade de fazer backup dos dados nesse momento.

Cartão SIM

Disparar **Apagar cartão SIM** exclui todos os dados do cartão SIM. Todos os dados de contatos e SMS armazenados no cartão SIM serão removidos. Depois de excluídos, esses dados não podem ser recuperados. Apagar o cartão SIM não afeta os dados armazenados no dispositivo ou no cartão SD.

Nota
Dependendo do tipo de cartão, pode não ser possível **Apagar o cartão SIM**.

- Clique em **Apagar cartão SIM** para excluir todos os dados armazenados no cartão SIM.
- Confirme o apagamento clicando em **OK**.
  - ↪ A mensagem **O cartão SIM foi apagado com êxito!** é exibida.
- Clique em **OK** para fechar a mensagem e retornar à guia **Apagar**.

Todos os armazenamentos

Disparar **Apagar todos os armazenamentos** exclui todos os dados armazenados no cartão SD e no armazenamento USB interno. Depois de excluídos, esses dados não podem ser recuperados. A função **Apagar todos os armazenamentos** não afeta os dados armazenados no cartão SIM.

- Clique em **Apagar armazenamentos** para excluir os dados armazenados diretamente no dispositivo e no cartão SD.
- Confirme o apagamento clicando em **OK**.
  - ↪ A mensagem **O armazenamento foi apagado com êxito!** é apresentada.
- Clique em **OK** para fechar a mensagem e retornar à guia **Apagar**.

Redefinição de fábrica

Uma **Redefinição de fábrica** redefine as configurações do dispositivo para o estado padrão e também exclui todas as contas, aplicativos e dados de aplicativos armazenados no dispositivo. Uma **Redefinição de fábrica** não afeta os dados armazenados no cartão SIM nem no cartão SD.

Nota
Para disparar um comando de **Redefinição de Fábrica** para excluir todos os dados do seu dispositivo em caso de perda ou furto, a função **Administrador do dispositivo** deve ser ativada durante a configuração.

- Clique em **Redefinição de fábrica** para redefinir as configurações do dispositivo para o estado padrão.
- Confirme esse tipo de apagamento clicando em **OK**.
- Clique novamente em **OK** para continuar.
- Para fechar a mensagem que informa sobre o êxito da **Redefinição de fábrica**, clique em **OK**.

Aviso
Uma **Redefinição de fábrica** também desinstala o Avira Free Android Security. Não será possível continuar a enviar comandos para o dispositivo por meio do Console da web, ou seja, não será possível bloquear nem localizar o dispositivo.

Apagamento combinado

Com um **Apagamento combinado** é possível disparar um, dois ou todos os três tipos de apagamento ao mesmo tempo.

- Selecione os tipos de apagamento que pretende disparar ou clique em **Selecionar tudo** para disparar uma combinação de todos os tipos de apagamento ao mesmo tempo.
- Clique em **Apagar seleção**.
- Confirme a sua escolha clicando em **OK**.
  - ↳ Dependendo da sua seleção e do tamanho da memória do dispositivo, pode demorar até 60 minutos.
- Clique em **OK** para continuar.

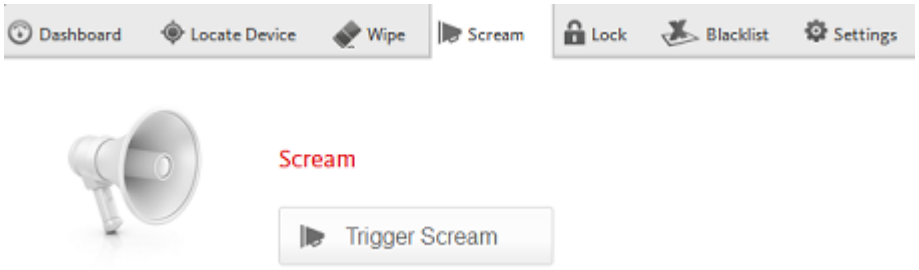
- Para fechar a mensagem que informa sobre o êxito do **Apagamento combinado**, clique em **OK**.

Os resultados dos três comandos **Apagar** são os seguintes:

Armazenamento afetado	Apagar o cartão SIM	Apagar todos os armazenamentos	Redefinição de fábrica
SMS no dispositivo			excluído
SMS no SIM	excluído		
Contatos no dispositivo			excluído
Contatos no SIM	excluído		
Conteúdo do cartão SD		excluído	
Conteúdo do armazenamento USB interno		excluído	
Contas, aplicativos, dados de aplicativo			excluído

Grito

Na guia **Grito** é disparado um alarme sonoro emitido pelo dispositivo. Essa função ajuda a localizar o dispositivo rapidamente.



- Clique no botão **Disparar grito** para iniciar a função de grito.
- Confirme o alarme clicando em **OK**.
  - ↳ O dispositivo emite um ruído alto durante 20 segundos. O grito não pode ser terminado ou pausado durante esse tempo.

Bloquear

Na guia **Bloquear** deve ser inserido um PIN de 4 dígitos para bloquear e desbloquear o dispositivo. É possível digitar uma mensagem personalizada que será apresentada na tela bloqueada do dispositivo. É possível adicionar um número de telefone que pode ser ligado utilizando o botão **Ligar para proprietário** no dispositivo bloqueado.

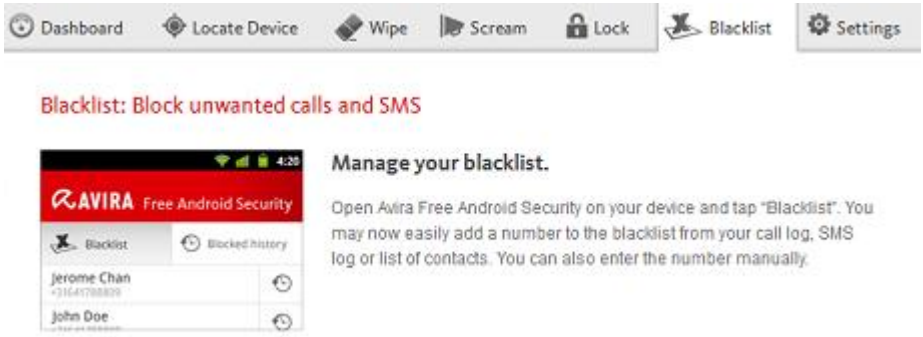
Nota
é fortemente recomendável bloquear o dispositivo para disparar um comando de apagar. Faça backup regularmente dos dados importantes. Quando for necessário apagar o dispositivo, não há oportunidade de fazer backup dos dados nesse momento.

- Digite um PIN de 4 dígitos no campo **Inserir PIN**.
- Confirme o PIN no campo a seguir.
- Clique em **OK**para disparar o bloqueio.
  - ↳ O dispositivo pode ser bloqueado inserindo o PIN no dispositivo ou clicando no botão **Desbloquear** na guia **Bloquear** da sua conta no Console da web.
  - ↳ O dispositivo só poderá ser desbloqueado manualmente se um PIN tiver sido definido previamente. Caso tenha esquecido o PIN que definiu, será necessário desbloquear o dispositivo com o botão **Desbloquear** da sua conta do Console da web.
- Digite uma mensagem personalizada no campo **Exibir mensagem quando perdido** adequada para ser exibida no dispositivo bloqueado, por exemplo, digite um texto e o seu endereço de e-mail para facilitar ao localizador entrar em contato com você.
- Insira um número de telefone que possa ser ligado com o botão **Ligar para proprietário** no dispositivo bloqueado no campo **Número alternativo para ligar se for encontrado**. Utilize um número de telefone confiável, como o número de telefone de casa ou o número de telefone de um amigo.
- Clique em **Bloquear** para salvar o PIN no dispositivo.
- Clique em **OK** para bloquear o dispositivo.

- Clique em **Desbloquear** para desbloquear o dispositivo com o Console da web

Lista negra

Caso não pretenda ser perturbado por certas chamadas ou SMS, você pode facilmente adicionar números de telefone à Lista negra. A funcionalidade bloqueia chamadas e SMS indesejados. É possível adicionar números da sua lista de contatos, do registro de chamadas e do registro de SMS ou inserir um número manualmente.



Adicionar um número de um dos registros do dispositivo à Lista negra

É possível adicionar facilmente um número à lista negra a partir do registro de chamadas, do registro de SMS ou da sua lista de contatos.

- Abra o Avira Free Android Security no seu dispositivo.
- Toque em **Lista negra**.
  - ↪ A tela Lista negra é aberta.
- Toque no botão **Adicionar**.
  - ↪ A tela **Adicionar contato à lista negra** é aberta.
- Selecione o registro a partir do qual pretende adicionar um número de telefone à lista negra e toque no botão adequado.

  Toque em **Cancelar** caso não pretenda adicionar um número à lista negra.

  Toque no número que pretende bloquear.
  - ↪ A próxima tela **Inserir detalhes de contato** exibe o número de telefone e o nome do contato que você deseja bloquear.
- Selecione uma opção de bloqueio. Você tem a opção de escolher **Chamadas e SMS**, somente **Chamadas** ou somente **SMS**.
- Clique em **Salvar** para armazenar o número na lista negra.
- O número bloqueado é apresentado na tela da Lista negra.

Nota
Se o contato que pretende adicionar já existir na Lista negra, você receberá uma mensagem de erro.

Adicionar um número à Lista negra manualmente

Você pode adicionar um número à lista negra digitando-o manualmente.

- Abra o Avira Free Android Security no seu dispositivo.
- Toque em **Lista negra**.
  - ↪ A tela Lista negra é aberta.
- Toque no botão **Adicionar**.
  - ↪ A tela **Adicionar contato à lista negra** é aberta.
- Toque em **Criar contato manualmente** para inserir um número de telefone.
  - ↪ A tela **Inserir detalhes do contato** é aberta.
- Toque no campo **Nome** para abrir o teclado para digitar as letras.
- Toque no campo **Número de telefone** para abrir o teclado para digitar os números.
- Selecione uma opção de bloqueio. Você tem a opção de escolher **Chamadas e SMS**, somente **Chamadas** ou somente **SMS**.
- Clique em **Salvar** para armazenar o número na lista negra.
- O número bloqueado é apresentado na tela da Lista negra.

Editar um contato bloqueado

Você pode editar o número de telefone e o nome do contato bloqueado.

- Abra o Avira Free Android Security no seu dispositivo.
- Toque em **Lista negra**.
  - ↪ A tela Lista negra é aberta.
- Toque no contato que pretende editar.
  - ↪ A tela **Editar contato bloqueado** abre.
- Toque no campo **Nome** para abrir o teclado para editar o nome.
- Toque no campo **Número de telefone** para abrir o teclado para editar o número de telefone.
- Clique em **Salvar** para armazenar o contato editado na lista negra.
- Clique em **Cancelar** caso não pretenda salvar as alterações que efetuou.

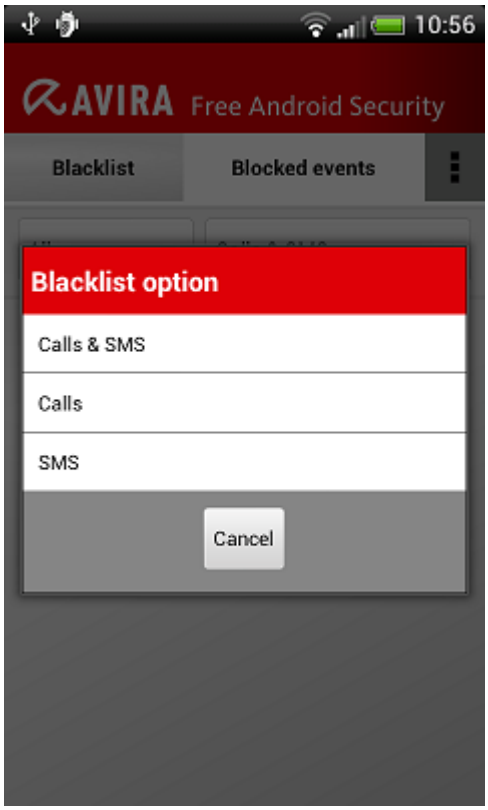
Eventos bloqueados

Você pode verificar o histórico de todos os contatos bloqueados na guia **Eventos bloqueados**. É possível filtrar a lista por determinadas opções. São apresentados o nome do contato, a data e hora da tentativa de contato e a forma de contato.

- Toque no botão **Todos** para selecionar entre os eventos **Todos**, **Hoje** ou **Novos**.
- Toque no botão **Chamadas e SMS** para ver as chamadas e tentativas de SMS bloqueadas. Escolha a opção **Chamadas** para verificar qual dos seus contatos bloqueados tentou ligar para você. Ou selecione **SMS** para chamar os números de telefone das mensagens curtas bloqueadas.

Excluir entradas dos Eventos bloqueados

É possível excluir entradas dos **Eventos bloqueados**. Filtre a lista de eventos bloqueados por **Todos**, **Hoje** ou **Novo** e selecione entre **Chamadas e SMS**, **Chamadas** ou apenas **SMS**. É possível excluir apenas um evento bem como todos os eventos. Por exemplo, se você escolher o filtro **Todos** e **Chamadas**, todas as chamadas bloqueadas são exibidas na lista. Agora você pode excluir todas as chamadas bloqueadas dos seus contatos ao mesmo tempo. Também tem a opção de verificar um só contato e excluir as chamadas listadas mais tarde.



- Toque no contato cujos eventos bloqueados deseja excluir.
  - ↪ São apresentados a hora e o número das chamadas bloqueadas recebidas e/ou SMS bloqueados.
- Toque no campo **SMS** para ver o conteúdo dos SMS bloqueados.
  - ↪ Agora pode abrir e ler as mensagens breves.
  - ↪ É possível excluir somente um SMS ou todos os SMS.

Toque em **Selecionar tudo** para marcar todo o histórico de SMS para o processo de remoção ou marque cada SMS separadamente.

Toque em **Excluir** para apagar essas mensagens breves ou toque em **Voltar** para parar a exclusão.

↪ É solicitado que confirme a exclusão dos SMS bloqueados.

Toque em **Excluir** para remover os SMS selecionados do histórico.

Toque em **Cancelar** para parar o processo de remoção.

- Toque no campo das **chamadas** para ver todas as chamadas do seu contato bloqueado.

  ↪ É possível excluir um único ou todos os eventos de chamada.

  Toque em **Selecionar tudo** para marcar todo o histórico de chamadas para o processo de remoção ou assinale chamadas separadamente.

  Toque em **Excluir** para apagar essas chamadas ou toque em **Voltar** para parar a exclusão.

  ↪ É solicitado que confirme a exclusão das chamadas bloqueadas.

  Toque em **Excluir** para remover as chamadas selecionadas do histórico.

  Toque em **Cancelar** para parar o processo de remoção.

Relatórios

No painel da guia **Configurações** encontra-se a seção **Relatório** que apresenta todas as atividades de Avira Free Android Security executadas com o Console da web.

As informações registradas são listadas por data e hora.

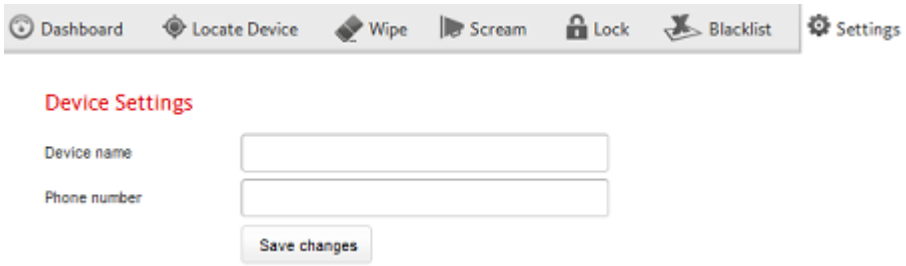
Um exemplo das informações apresentadas pelo relatório Atividade:

Data	Hora	Mensagem
Terça-feira, 07 de agosto de 2012	3:17 PM	Informações do dispositivo atualizadas com êxito
Terça-feira, 07 de agosto de 2012	2:05 PM	Dispositivo localizado com êxito

Segunda-feira, 13 de agosto de 2012	6:11 PM	Dispositivo desbloqueado com êxito

Configurações

No painel da guia **Configurações** é gerenciado o nome e o número de telefone do seu dispositivo. Além disso, é possível verificar aqui a seção **Relatório** que apresenta todas as atividades de Avira Free Android Security executadas com o Console da web.

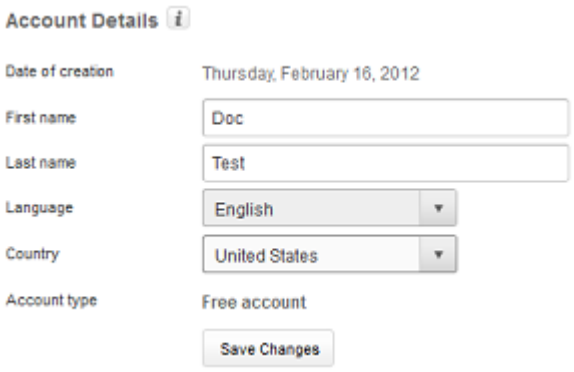


- Clique no dispositivo que deseja gerenciar na barra lateral.
- Digite um nome para esse dispositivo no campo **Nome do dispositivo**.
- Digite o número de telefone desse dispositivo no campo **Número de telefone**.
- Clique em **Salvar alterações** para salvar as configurações efetuadas para esse dispositivo.
  - ↪ O Console da web Avira Android mostra que as configurações foram salvas com êxito.

Barra de Título do Console da Web

Detalhes da conta

A barra de título do Console da web Avira contém o link para a sua **Conta** onde pode gerenciar os detalhes da conta.



- Clique no link.
  - ↪ O painel **Detalhes da Conta** é aberto com os seguintes campos:

Data de criação

Apresenta a data e a hora em que a conta foi registrada.

Nome

É possível inserir o seu nome aqui.

Sobrenome

É possível inserir o seu sobrenome aqui.

Idioma

Selecione o seu idioma preferido no menu suspenso.

País

Selecione o país de residência no menu suspenso.

Tipo de conta

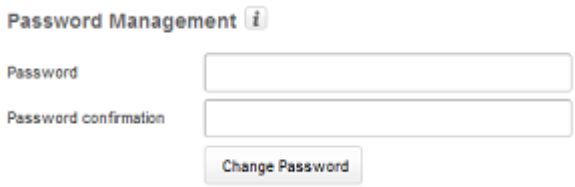
Apresenta o tipo de conta que está utilizando, ou seja, se comprou o aplicativo ou está utilizando uma versão gratuita, etc.

Salvar alterações

- Clique em **Salvar alterações** para salvar os detalhes da conta que alterou.

Gerenciamento da senha

A barra de título do Console da web Avira contém o link para a sua **Conta** onde pode gerenciar a sua senha.



- Clique no link **Conta**.
  - ↪ O painel **Gerenciamento da senha** é aberto com os seguintes campos:

Senha

Insira uma nova senha para a sua conta de Avira Free Android Security.

Confirmação da senha

Insira novamente a senha que inseriu para confirmá-la.

Alterar senha

- Clique no botão para salvar as alterações que efetuou.

Segurança da conta

A barra de título do Console da web Avira contém o link para a sua **Conta** onde você determina a pergunta de segurança. A Pergunta de segurança foi concebida para adicionar segurança extra a sua conta. Pode ser utilizada para você se identificar caso tenha perdido ou esquecido as suas credenciais de logon ou desejar alterar o endereço de email.

- Clique no link **Conta**.
  - ↪ O painel **Segurança da Conta** é aberto com os seguintes campos:

Pergunta de segurança

Abre o menu suspenso para selecionar uma pergunta de segurança que não pode ser respondida por outra pessoa além de você. Selecione uma pergunta que se adeqúe a você.

Resposta

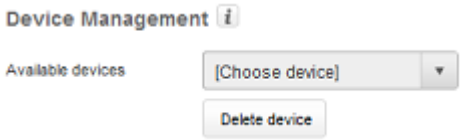
- Digite a sua resposta no campo **Resposta**.
- Certifique-se de que digitou corretamente e em um formato que seja fácil de lembrar.

Salvar alterações

- Clique em **Salvar Alterações** para salvar a resposta da sua Pergunta de segurança.

Administração do dispositivo

A barra de título do Console da web Avira contém o link para a sua **Conta** onde pode gerenciar o seu dispositivo.



- Clique no link **Conta**.
  - ↪ O painel **Administração do Dispositivo** é aberto com os seguintes campos:

Dispositivos disponíveis

Abre o menu suspenso para selecionar um dos dispositivos.

Excluir dispositivo

- Clique no botão para remover o dispositivo selecionado da sua conta.

Como

Como alterar meu endereço de email?

Caso necessite alterar seu endereço de email, entre em contato com o Suporte da Avira. O seu endereço de email não é utilizado somente para entrar em contato com você, também funciona como sua identidade de usuário ao mesmo tempo. Por isso não pode ser alterado por você no Console da web nem no aplicativo do dispositivo.

Como manter seguros os dados armazenados no dispositivo?

A maneira mais fácil e mais simples de manter seguros os dados armazenados no dispositivo é bloquear o dispositivo.

- Faça logon no Console da web.
- Navegue para a guia **Bloquear**.
- Insira um PIN de 4 dígitos.
- Confirme o PIN.
- Clique em **Bloquear**.
  - ↪ O PIN pode agora ser utilizado para bloquear e desbloquear o dispositivo.

> **Nota**
> O PIN é válido apenas temporariamente. Cada comando de bloquear/desbloquear exige um novo PIN.

Como desbloquear o dispositivo se tiver esquecido o PIN/inserido um PIN incorreto três vezes?

> **Nota**
> Se um PIN incorreto for inserido no dispositivo três vezes, será necessário desbloquear o dispositivo por meio do Console da web primeiro. Em seguida, você pode enviar o outro comando de bloqueio ao seu dispositivo.

- Faça logon no Console da web.
- Navegue para a guia **Bloquear**.
- Clique no botão **Desbloquear**.
  - ↳ O dispositivo é desbloqueado imediatamente.
- Insira um novo PIN de 4 dígitos.
- Confirme o PIN.
- Clique em **Bloquear**.
- Confirme o comando de bloqueio clicando em **OK**.
  - ↳ O PIN pode agora ser utilizado para bloquear e desbloquear o dispositivo.

Como alterar o PIN?

O PIN pode ser alterado somente no Console da web. Não é possível alterar o PIN no próprio aplicativo.

- Faça logon no Console da web.
- Navegue para a guia **Bloquear**.
- Insira um PIN de 4 dígitos.
- Confirme o PIN.
- Clique em **Bloquear**.
  - ↳ O PIN pode agora ser utilizado para bloquear e desbloquear o dispositivo.

Como encontrar o dispositivo se ele foi perdido ou roubado?

Se o dispositivo for perdido ou roubado, Avira Free Android Security oferece duas opções para recuperá-lo:

Disparar um grito

A funcionalidade Disparar grito foi concebida para facilitar a localização do dispositivo. É particularmente útil se for perdido por perto, por exemplo, em casa.

- Faça logon no Console da web.
- Selecione a guia Grito e clique em Disparar grito.
  - ↪ O dispositivo emite um ruído alto durante 20 segundos para facilitar a sua localização. O grito continua durante 20 segundos e não pode ser terminado ou pausado durante esse tempo. O grito também é emitido se o dispositivo estiver silenciado.

> **Nota**
> O grito não será emitido se o dispositivo estiver desligado ou sem bateria.

Localizar o seu dispositivo

Se não souber onde perdeu o dispositivo ou acreditar que foi roubado, você pode rastrear a localização do dispositivo.

> **Nota**
> O processo de rastreio pode demorar até 3 minutos. Não é possível disparar o comando Localizar dispositivo novamente enquanto um dispositivo estiver sendo rastreado. Mas é possível disparar um comando Localizar dispositivo para um dispositivo diferente registrado na sua conta.

- Faça logon no Console da web.
- Selecione a guia **Localizar dispositivo**.
  - ↪ É apresentado um extrato do Google Maps no Console da web Avira.
- Clique em **Localizar dispositivo** abaixo do mapa apresentado.
  - ↪ O tempo decorrido é apresentado durante o processo de localização. O tempo decorrido é apresentado durante o processo de localização. Os dados geofísicos são apresentados como latitude e longitude.

Como registrar um novo dispositivo em uma conta existente?

É possível adicionar até 5 dispositivos à sua conta. Todos os dispositivos adicionados à mesma conta do Google ou ao mesmo endereço de email por meio do aplicativo são registrados na mesma conta do Avira Free Android Security, ou seja, uma conta de email tem uma conta do Avira Free Android Security com até cinco dispositivos diferentes.

- Utilize o dispositivo que pretende adicionar à conta para baixar o Avira Free Android Security.
- Instale o aplicativo no dispositivo.

- Selecione a Conta do Google ou insira um endereço de email diferente e toque em **Aceitar EULA e continuar**.
  - ↪ Você receberá um email de confirmação nesse endereço confirmando o registro de um novo dispositivo na sua conta do Avira Free Android Security existente.
  - ↪ Se fizer logon no Console da web agora, o novo dispositivo terá sido adicionado à seção **Todos os seus dispositivos** no lado esquerdo do Console da web.
- Agora pode clicar em **Editar** na guia do dispositivo para entrar nas configurações e alterar o nome do dispositivo e o número do telefone.

Nota
Como pode haver somente cinco dispositivos adicionados a uma conta do Avira Free Android Security, um novo dispositivo poderá ser adicionado somente se um dispositivo for excluído da conta e o aplicativo for excluído de um dos dispositivos registrados. Primeiro acesse as configurações da **Conta** no Console da web da sua conta do Avira Free Android Security e selecione um dispositivo na lista suspensa em **Gerenciamento de dispositivo** e clique em **Excluir dispositivo**. Em seguida, exclua o aplicativo do dispositivo selecionado.

Solução de problemas

Solução de problemas

Mensagens

Mensagem	Significado
Estabeleça conexão com uma rede móvel ou Wi-Fi para continuar.	Nenhuma conexão de rede foi encontrada durante o processo de registro. Ative a conectividade de rede para continuar.
O serviço não está disponível atualmente. Tente novamente mais tarde.	O serviço Google não está disponível atualmente.

Falha do Avira Free Android Security. Toque aqui para nos ajudar a resolver o problema.	Ocorreu um erro inesperado que forçou o aplicativo a parar. Ao tocar na notificação e confirmar com OK, o log de erros será enviado para nós automaticamente.
É necessário ter uma Conta do Google para registrar o dispositivo. Crie uma conta e tente novamente.	Não foi encontrada uma Conta do Google no dispositivo.
A senha da Conta do Google foi alterada. Abra o Gmail ou o aplicativo Google Play para atualizar a senha no dispositivo.	A Conta do Google padrão neste dispositivo tem uma senha inválida. Verifique se a autenticação da Conta do Google foi alterada. Atualize e sincronize a sua senha no dispositivo iniciando o Gmail ou o aplicativo Google Play.
Muitos aplicativos no dispositivo estão utilizando o serviço de envio por push do Google (GCM). Desinstale um deles e tente novamente.	Google define um limite para aplicativos com GCM ativado instalados em um dispositivo.
Ocorreu um erro. Tente novamente mais tarde.	Ocorreu um erro desconhecido.
Há mais que cinco dispositivos registrados com esta conta. Exclua um para adicionar outro.	Foi atingido o máximo de cinco dispositivos registrados no Avira Free Android Security.
Este dispositivo não está mais registrado com uma Conta do Avira Free Android Security. O aplicativo foi redefinido.	O seu registro foi redefinido porque este dispositivo foi excluído da lista de dispositivos registrados.
Ocorreu um erro do servidor. Tente novamente mais tarde.	Ocorreu um erro desconhecido do servidor.

Ocorreu um erro inesperado que forçou o aplicativo a parar. Ajude-nos a resolver este problema. Clique em OK e o log de erros será enviado automaticamente para nós. Você também pode adicionar comentários sobre o problema a seguir:	Ocorreu um erro inesperado que finalizou o aplicativo.
Erro inesperado. Consulte a barra de notificação.	Ocorreu um erro inesperado.
Obrigado!	Obrigado por relatar o problema, as informações foram enviadas com êxito.
Em caso de perda ou roubo do dispositivo, o Avira Free Android Security pode ajudar a efetuar uma redefinição de fábrica para apagar dados do dispositivo. Para efetuar uma redefinição de fábrica, o administrador do dispositivo deve estar ativado.	Se perder o seu dispositivo, o Avira Free Android Security pode ajudar a apagar dados do dispositivo com uma redefinição de fábrica. Para isso, a função **Administrador do dispositivo** deve estar ativada.
Apagar com redefinição de fábrica ativada/desativada.	A função Apagar com o comando **Redefinição de fábrica** está ativada/desativada.
O dispositivo foi registrado com êxito no Avira Free Android Security!	O Avira Free Android Security foi registrado com êxito!
Foi enviado um email para <joao.silva@gmail.com>. Verifique a sua conta de email para obter informações e mais instruções.	Foi enviado um email com as informações de ativação para <joao.silva@gmail.com>. Verifique o seu email para iniciar a sua experiência conosco!
Se tiver perguntas, visite o Fórum de Suporte ou entre em contato com a Avira.	Se tiver perguntas, visite o nosso Fórum ou entre em contato com a Avira.

O registro falhou. Reinicie o aplicativo e tente novamente.	Ocorreu um erro inesperado durante o processo de registro. Reinicie o aplicativo e tente registrar novamente.
O registro falhou. É possível que esteja utilizando tecnologia incompatível com o Avira Free Android Security. Reinicie o aplicativo e tente novamente.	O seu dispositivo pode estar utilizando tecnologia não compatível com o Avira Free Android Security. Consulte os requisitos do sistema, que são os seguintes: Sistema operacional: Android 2.2 (Froyo) - Android 4.1. (Jelly Bean). Memória: 1,28 MB de espaço livre na memória. Navegadores: Mozilla Firefox, Google Chrome, Opera e Internet Explorer IE7 ou superior.
A criação do contato falhou	O contato não foi adicionado à lista negra porque já está na lista.
Nome já existe na lista negra	Esse nome já está na lista negra, por isso não pode ser adicionado novamente.
O contato já existe na lista negra	Esse contato já está na lista negra, por isso não pode ser adicionado novamente.
O número já existe na lista negra para <João Silva>	Esse número de telefone já está na lista negra e encontra-se sob o nome <João Silva>, por isso não pode ser adicionado novamente.

Glossário

Abreviação	Significado
GCM	Google Cloud Messaging é um serviço que ajuda a enviar dados de servidores para o aplicativo no seu dispositivo.
IMEI	A Identidade de Equipamento Móvel Internacional (International Mobile Equipment Identity) é um número exclusivo, semelhante a uma impressão digital exclusiva, para identificar o seu dispositivo.
Cartão SIM	O cartão de Módulo de Identificação do Assinante (Subscriber Identification Module) é um cartão do provedor no qual são armazenadas diferentes informações, como o número de série, o número de telefone e o seu PIN.
PIN	Número de Identificação Pessoal (Personal Identification Number), geralmente um número de 4 dígitos.
SO	O sistema operacional do dispositivo.
GPS	Sistema de Posicionamento Global (Global Positioning System) é um sistema baseado em satélites que fornece dados de localização e de hora a receptores de GPS.
Tecnologia de torre celular	Tecnologia avançada de rádio que recolhe sinais de celulares e os transmite a outras torres utilizando ondas de rádio.
WiFi	É um padrão que permite a troca de dados e o acesso sem fio à Internet por meio de um ponto de acesso à rede.

W-LAN	Acesso por rede sem fio.
Nuvem	É uma localização de servidor remota e uma infraestrutura de computação. Os dados armazenados na nuvem não são armazenados localmente no seu computador.
Número de telefone alternativo	O número de telefone que pode ser ligado a partir do seu dispositivo bloqueado, utilizando o botão **Ligar para proprietário**.
Latitude	Coordenada geográfica que especifica a posição norte-sul na Terra.
Longitude	Coordenada geográfica que especifica a posição-leste-oeste na Terra.

Serviço

Suporte

Serviço de suporte

Todas as informações necessárias sobre o nosso serviço de suporte abrangente podem ser obtidas no nosso site http://www.avira.com.

Fórum da Comunidade

Antes de contatar a linha direta, recomendamos que visite o nosso fórum de usuário em http://forum.avira.com.

Perguntas frequentes

Leia também a seção de Perguntas frequentes no nosso site http://www.avira.com/en/support-for-home-knowledgebase.
A sua pergunta pode já ter sido feita e respondida por outros usuários nesta seção.

Contato

Endereço

Avira Operations GmbH & Co. KG
Kaplaneiweg 1
D-88069 Tettnang
Alemanha

Internet

É possível encontrar mais informações sobre nós e os nossos produtos no seguinte endereço:
http://www.avira.com

11.10 Geral

11.10.1 Categorias de ameaça

Seleção de categorias de ameaças (Opções disponíveis somente no modo avançado)

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.

11.10.2 Proteção avançada

ProActiv (Opção disponível apenas no modo avançado.)

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 (Opções disponíveis apenas no modo avançado.)

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.

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.

11.10.3 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 (Opções disponíveis somente no modo avançado)

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.
Safe Browsing ativar / desativar	Se essa opção for ativada, a senha predefinida será necessária para ativar/desativar o controle dos pais.
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.
Configuração	Se essa opção for ativada, a configuração do programa somente poderá ser feita depois que a senha predefinida for inserida.
Instalação / desinstalação	Se essa opção for ativada, a senha predefinida é necessária para a instalação ou desinstalação do programa.

11.10.4 Segurança

Opções disponíveis apenas no modo avançado.

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 !

11.10.5 WMI

Opções disponíveis apenas no modo avançado.

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 por meio de uma interface. A WMI oferece a opção de baixar dados operacionais do programa

Ativar o suporte a WMI

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

11.10.6 Eventos

Opções disponíveis apenas no modo avançado.

Limitar tamanho do banco de dados de eventos

Limitar tamanho para no máx. 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.

11.10.7 Relatórios

Opções disponíveis apenas no modo avançado.

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.

11.10.8 Diretórios

Opções disponíveis apenas no Modo avançado.

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.

11.10.9 Alertas acústicos

Opções disponíveis apenas no modo avançado.

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 Scanner é definido na configuração em Scanner > Varredura > 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.

11.10.10 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

Alerta, se a última atualização for mais antiga que n dia(s)

Nessa caixa você pode inserir o número máximo de dias que podem transcorrer desde a última atualização. Se esse número de dias tiver passado, um ícone vermelho 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/observações com as seguintes situações

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. Existe o risco de a conexão ter sido criada por um discador desconhecido e indesejado e de a conexão ser cobrada. (consulte Vírus e mais > Categorias de Ameaça: Discador)

Arquivos foram atualizados com êxito

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.

Edição Q2-2013

AVIRA

live free.™

Avira Operations GmbH & Co. KG
Kaplaneiweg 1
88069 Tettnang
Alemanha

Telefone: +49 7542-500 0
Fax: +49 7542-500 3000
www.avira.com/pt-br