McAfee®

internetsecuritysuite wirelessedition

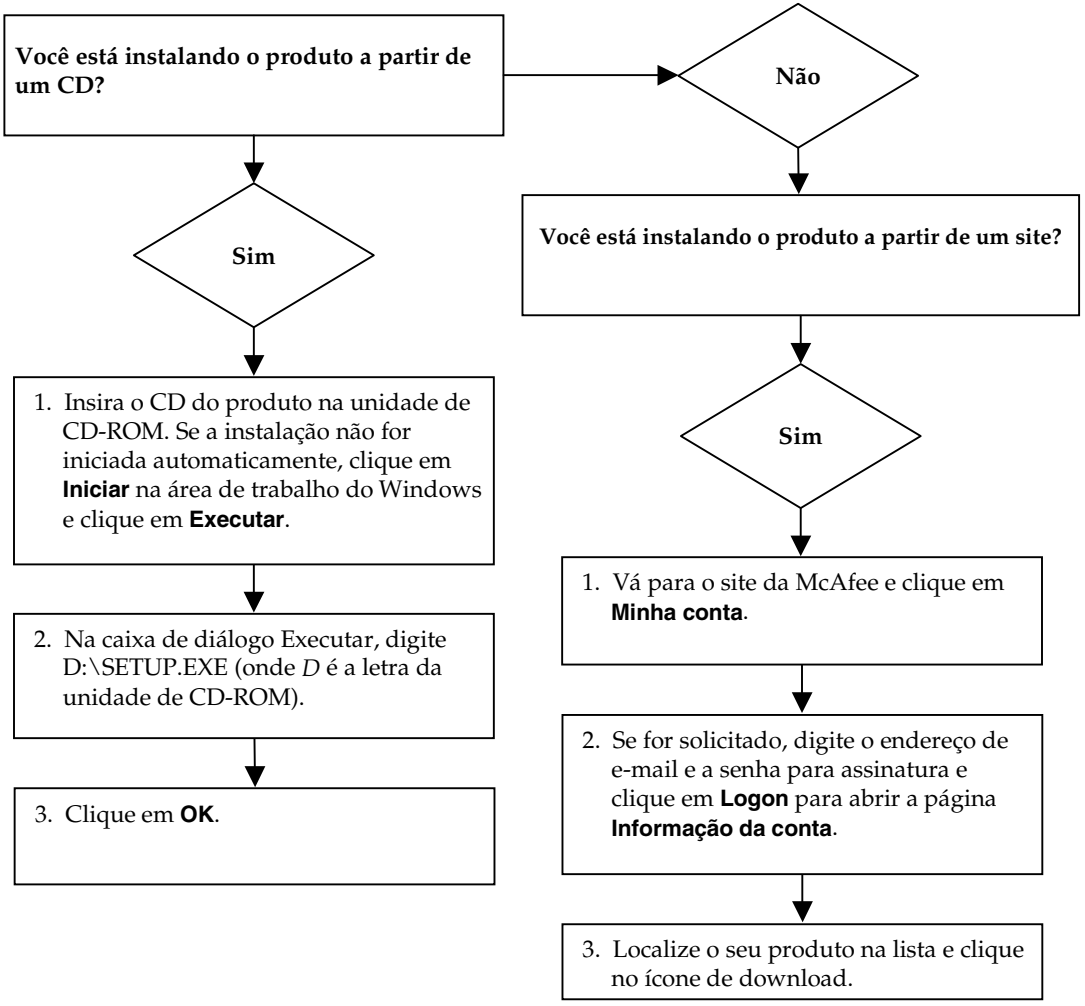
Guia do Usuário

Versão 1.1

McAfee®

Cartão de início rápido

Se você estiver instalando o produto de um CD ou de um site da Web, imprima esta página de referência.



Para obter mais informações

Para ver os Guias do Usuário contidos no CD do produto, verifique se o Acrobat Reader está instalado. Se não estiver, instale-o agora com o CD do produto da McAfee.

1. Insira o CD do produto na unidade de CD-ROM.
2. Abra o Windows Explorer: Clique em **Iniciar** na área de trabalho do Windows e, em seguida, em **Pesquisar**.
3. Localize a pasta Manuals e clique duas vezes no arquivo .PDF do Guia do Usuário a ser aberto.

Vantagens do registro

A McAfee recomenda que você siga as etapas fáceis indicadas no produto para que o seu registro seja transmitido diretamente para nós. O registro garante que você receba uma assistência técnica adequada e confiável, além das seguintes vantagens:

- Suporte eletrônico GRATUITO
- Atualizações de arquivos de definição de vírus (.DAT) por um ano após a instalação quando você adquire o software VirusScan

  Visite http://br.mcafee.com/ para obter o preço de um ano adicional de assinaturas de vírus.
- Garantia de 60 dias, que cobre a substituição do CD do software se ele apresentar defeito ou se estiver danificado
- Atualizações do filtro SpamKiller por um ano após a instalação quando você adquire o software SpamKiller

  Visite http://br.mcafee.com/ para obter o preço de um ano adicional de atualizações do filtro.
- Atualizações do McAfee Internet Security Suite por um ano após a instalação quando você adquire o software MIS

  Visite http://br.mcafee.com/ para obter o preço de um ano adicional de atualizações de conteúdo.

Suporte técnico

Para obter suporte técnico, visite

http://www.mcafeeajuda.com/.

Nosso site de suporte oferece acesso ininterrupto ao Assistente de respostas de fácil utilização, que contém soluções para as questões de suporte mais comuns.

Os usuários mais experientes também podem experimentar as opções avançadas, que incluem uma pesquisa por palavra-chave e nossa árvore de ajuda. Se você não encontrar uma solução para o seu problema, ainda poderá acessar as opções GRATUITAS Chat Now! e E-mail Express!. O Chat (bate-papo) e o e-mail ajudam a contatar nossos engenheiros de suporte qualificados de forma rápida pela Internet, sem custo algum. Como alternativa, é possível obter informações do suporte telefônico em

http://www.mcafeeajuda.com/.

Sumário

Introdução 1

A Internet coloca ao seu alcance uma imensa variedade de informações e opções de entretenimento. No entanto, assim que a conexão é estabelecida, o seu computador fica exposto a inúmeras ameaças à privacidade e à segurança. Proteja a privacidade e a segurança do seu computador e dos seus dados com o Internet Security Suite-Wireless Network Edition. Incorporando as tecnologias premiadas da McAfee, o McAfee Internet Security Suite-Wireless Network Edition é um dos conjuntos mais abrangentes de ferramentas de segurança e privacidade disponíveis. O McAfee Internet Security Suite-Wireless Network Edition oferece uma proteção avançada para a sua rede sem fio, os seus dados pessoais e o seu computador. Além disso, ele destrói vírus, derrota hackers, protege informações pessoais, dá privacidade à navegação na Web, bloqueia anúncios e pop-ups, gerencia cookies e senhas, bloqueia arquivos, pastas e unidades, filtra conteúdo censurável e permite controlar as conexões de entrada e saída de Internet no computador.

O McAfee Internet Security Suite-Wireless Network Edition é uma solução de segurança comprovada, que fornece proteção total aos usuários da Internet de hoje.

O McAfee Internet Security Suite-Wireless Network Edition compreende os seguintes produtos:

Software McAfee Internet Security Suite-Wireless Network Edition

- **McAfee SecurityCenter —** Avalia, informa e adverte sobre as vulnerabilidades de segurança do seu computador. Cada índice de segurança avalia rapidamente sua exposição a ameaças de segurança baseadas na Internet e explica como proteger com rapidez e segurança o computador.
- **McAfee Wireless Home Network Security —** Protege a privacidade da sua experiência computacional criptografando os seus dados pessoais e privados quando estes são enviados pela sua rede sem fio protegida e bloqueia o acesso de hackers às suas informações.
- **McAfee VirusScan —** Faz varredura, detecta, corrige e remove vírus da Internet. Você pode personalizar varreduras de vírus e determinar a resposta e a ação quando um vírus é detectado. Também é possível configurar o VirusScan para registrar as ações relacionadas a vírus executadas no seu computador.
- **McAfee Personal Firewall Plus —** Protege o computador enquanto ele está conectado à Internet e torna seguras as conexões de entrada e saída de Internet.
- **McAfee Privacy Service —** Combina proteção de informações pessoais, bloqueio de anúncios on-line e filtragem de conteúdo. Esse serviço protege as informações pessoais e proporciona melhor controle do uso da Internet pela sua família. O McAfee Privacy Service garante que as informações confidenciais não fiquem expostas a ameaças on-line e protege você e sua família de conteúdo on-line inadequado.
- **McAfee SpamKiller —** O aumento de e-mails fraudulentos, inadequados e ofensivos enviados a adultos, crianças e empresas torna a proteção contra spam um componente essencial à estratégia de segurança do computador.

Requisitos de sistema

- Microsoft® Windows 98SE, Me, 2000 ou XP
- PC com processador compatível com Pentium
  - Windows 98, 2000: 133 MHz ou superior
  - Windows Me: 150 MHz ou superior
  - Windows XP (Home e Pro): 300 MHz ou superior
- RAM
  - Windows 98, Me, 2000: 64 MB
  - Windows XP (Home e Pro): 128 MB
- 100 MB de espaço em disco rígido

- Microsoft Internet Explorer 5.5 ou posterior

  NOTA
  Para atualizar para a versão mais recente do Internet Explorer, visite o site da Microsoft em http://www.microsoft.com/.

- Sistema operacional desenvolvido e testado para oferecer suporte ao idioma português do Brasil

Plug-in AntiPhishing:

- Outlook Express 6.0 ou superior
- Outlook 98, 2000, 2003 ou XP
- Internet Explorer 6.0 ou superior

Mensagens instantâneas:

- AOL Instant Messenger 2.1 ou superior
- Yahoo Messenger 4.1 ou superior
- Microsoft Windows Messenger 3.6 ou superior
- MSN Messenger 6.0 ou superior

E-mail:

- POP3 (Outlook Express, Outlook, Eudora, Netscape)
- MAPI (Outlook)
- Web (MSN/Hotmail ou conta de e-mail com acesso POP3)

Adaptador de rede sem fio:

- Adaptador de rede sem fio padrão

Roteador ou ponto de acesso sem fio:

- Adaptador de rede sem fio padrão
- Roteador ou ponto de acesso sem fio padrão, incluindo a maioria dos modelos Linksys®, NETGEAR®, D-Link® e Belkin®.

Instalação do Internet Security Suite-Wireless Network Edition

Você pode instalar o Internet Security Suite-Wireless Network Edition a partir de um CD ou do site.

Instalação a partir de um CD

1. Insira o CD do produto na unidade de CD-ROM. Se a instalação não for iniciada automaticamente, clique em **Iniciar** na área de trabalho do Windows e, em seguida, clique em **Executar**.
2. Na caixa de diálogo **Executar**, digite D:\SETUP.EXE (onde D é a letra da unidade de CD-ROM).
3. Clique em **OK**.
4. Vá para *Utilização do assistente de configuração* na página 23.

Instalação a partir do site

Ao instalar o McAfee Internet Security Suite-Wireless Network Edition a partir do site, você precisa salvar o arquivo de instalação. Esse arquivo é usado para instalar o McAfee Internet Security Suite-Wireless Network Edition em outros computadores.

1. Visite o site da McAfee e clique em **Minha conta**.
2. Se for solicitado, digite o endereço de e-mail e a senha para assinatura e clique em **Logon** para abrir a página **Informação da conta**.
3. Localize o seu produto na lista e clique em **Salvar destino como...** O arquivo de instalação será salvo no computador.

Instalação a partir do arquivo de instalação

Se você obteve o pacote de instalação através de um download (em vez de ter um CD), é necessário instalar o software em todos os computadores sem fio. Quando a rede estiver protegida, os computadores sem fio não poderão se conectar à rede sem inserir a chave. Escolha uma das opções seguintes:

- Antes de proteger a rede, faça download do pacote de instalação para cada computador sem fio.
- Copie o arquivo de instalação para uma "memory key" USB ou CD gravável e instale o software nos outros computadores sem fio.
- Se a rede já estiver protegida, conecte um cabo no roteador para fazer download do arquivo. Você também pode clicar em **Exibir chave atual** para ver a chave atual e conectar-se à rede sem fio usando essa chave.

Após instalar o McAfee Internet Security Suite-Wireless Network Edition em todos os computadores sem fio, siga as instruções da tela. Quando você clicar em **Concluir**, o Assistente de configuração aparecerá. Vá para *Utilização do assistente de configuração* na página 23.

Utilização do McAfee SecurityCenter

O McAfee SecurityCenter é a sua central de produtos de segurança, acessível a partir do ícone correspondente na área de notificação do Windows ou na área de trabalho do Windows. Com ele, você pode executar as seguintes tarefas:

- Obter uma análise gratuita de segurança do seu computador.
- Iniciar, gerenciar e configurar todas as suas assinaturas da McAfee usando um único ícone.
- Exibir alertas de vírus continuamente atualizados e as informações mais recentes sobre os produtos.
- Obter links rápidos para perguntas freqüentes e detalhes da conta no site da McAfee.

> **NOTA**
> Para obter mais informações sobre os recursos do SecurityCenter, clique em **Ajuda** na caixa de diálogo **SecurityCenter**.

Enquanto o SecurityCenter estiver sendo executado e todos os recursos da McAfee instalados no computador estiverem ativados, um ícone com um **M** vermelho será exibido na área de notificação do Windows. Geralmente, essa área se encontra no canto inferior direito da área de trabalho do Windows e contém o relógio.

Se um ou mais aplicativos da McAfee instalados no computador estiverem desativados, o ícone da McAfee se tornará preto .

Para abrir o McAfee SecurityCenter:

1. Clique com o botão direito do mouse no ícone da McAfee na área de notificação do Windows.
2. Clique em **Abrir o SecurityCenter**.

Para acessar o produto da McAfee:

1. Clique com o botão direito do mouse no ícone da McAfee na área de notificação do Windows.
2. Aponte para o produto da McAfee apropriado e selecione o recurso a ser utilizado.

Remoção de programas do Internet Security Suite-Wireless Network Edition

Em algumas situações, talvez você queira remover programas do Internet Security Wireless Network.

> **NOTA**
> Os usuários precisam ter direitos de administrador para remover programas do Internet Security Suite-Wireless Network Edition.

Para remover programas do Internet Security Wireless Network:

1. Salve todo o seu trabalho e feche todos os aplicativos abertos.
2. Abra o **Painel de controle**.
   - Na barra de tarefas do Windows, selecione **Iniciar**, aponte para **Configurações** e clique em **Painel de controle** (Windows 98, ME e 2000).
   - Na barra de tarefas do Windows, selecione **Iniciar** e clique em **Painel de controle** (Windows XP).
3. Clique em **Adicionar ou remover programas**.
4. Selecione o Assistente de desinstalação da McAfee, selecione um ou mais programas e, em seguida, clique em **Desinstalar**.
5. Clique em **Sim** para continuar a remoção.

Se solicitado, reinicie o computador.

McAfee Wireless Home Network Security 2

Bem-vindo ao McAfee Wireless Home Network Security, que oferece uma proteção avançada para a sua rede sem fio, os seus dados pessoais e o seu computador.

Este produto foi desenvolvido para computadores com conexões sem fio. Ao instalar este produto em computadores que se conectam à sua rede com cabos, você não obtém total funcionalidade a partir desses computadores com fio.

O McAfee Wireless Home Network Security melhora a privacidade da sua experiência computacional criptografando os seus dados pessoais e privados quando estes são enviados pela sua rede sem fio protegida, bloqueando o acesso de hackers às suas informações.

Utilização do McAfee Wireless Home Network Security

Antes de proteger a sua rede, observe o seguinte.

- Conexões de cabos - os computadores que são conectados ao roteador com um cabo não precisam ser protegidos porque os sinais transmitidos através de um cabo não podem ser interceptados.
- Conexões sem fio - os computadores que possuem conexões sem fio precisam ser protegidos porque seus dados podem ser interceptados. Um computador sem fio precisa ser utilizado para proteger uma rede porque apenas um computador sem fio pode conceder acesso a um outro computador sem fio.

Proteção da sua rede

Não é necessário proteger a sua rede se você está conectado com um cabo.

1. Em um computador sem fio, instale o seu adaptador sem fio e verifique se ele está ativado. O adaptador sem fio pode ser uma placa inserida na lateral do computador ou em uma porta USB. Muitos computadores mais novos vêm com um adaptador sem fio integrado, de modo que não é necessário instalá-lo.
2. Instale o seu roteador ou ponto de acesso sem fio (os pontos de acesso são usados para ampliar o alcance sem fio) e verifique se ele está ligado e ativado. Para obter uma definição mais completa de um roteador e de um ponto de acesso, consulte o *Glossário* na página 173.

3 Instale o McAfee Wireless Home Network Security em todos os computadores sem fio da sua rede. Não é necessário instalar esse software em computadores conectados com um cabo. Consulte *Instalação do Internet Security Suite-Wireless Network Edition* na página 15.

4 A partir de um dos computadores sem fio, proteja a sua rede. Consulte *Proteção de redes sem fio* na página 32.

5 Associe-se à rede a partir dos outros computadores sem fio. Consulte *Proteção de outros computadores* na página 31.

Compreensão do Wireless Home Network Security

Como muitas pessoas, você usa uma rede sem fio em casa por conveniência e facilidade. A conexão sem fio permite ter acesso à Internet de qualquer cômodo da casa ou mesmo em seu quintal, sem o custo e o trabalho de conectar cabos. A conexão em rede sem fio facilita o acesso de amigos e familiares à rede.

No entanto, essa comodidade acarreta uma vulnerabilidade de segurança. As redes sem fio utilizam ondas de rádio para transmitir dados e essas ondas de rádio se propagam além das paredes da sua casa. Com antenas especializadas, intrusos sem fio podem ter acesso à sua rede sem fio ou interceptar os seus dados a quilômetros de distância.

Para proteger os seus dados e a sua rede sem fio, é necessário restringir o acesso à sua rede sem fio e criptografar os seus dados. O seu roteador ou ponto de acesso sem fio vem com padrões de segurança incorporados, mas a dificuldade é ativar e gerenciar corretamente as suas configurações de segurança. Mais de sessenta por cento das redes sem fio não utilizam corretamente um alto nível de segurança, como a criptografia.

O Wireless Home Network Security torna isso fácil

O McAfee Wireless Home Network Security ativa a segurança na sua rede sem fio e protege o que é enviado através dela com um processo simples de apenas um clique que gera automaticamente uma chave de criptografia forte. A maioria das chaves que são fáceis de lembrar podem ser facilmente quebradas por hackers. Ao deixar que o computador lembre da chave para você, o Wireless Home Network Security pode utilizar chaves que sejam quase impossíveis de se quebrar.

Operando discretamente nos bastidores, esse software também cria e distribui uma nova chave de criptografia em intervalos de alguns minutos, frustrando até mesmo os hackers mais persistentes. Computadores legítimos, como os de seus amigos e familiares, que queiram ter acesso à sua rede sem fio, recebem a chave de criptografia forte e todas as distribuições de chaves.

Esse processo proporciona uma segurança forte, mas de implementação fácil para o proprietário de uma rede sem fio domiciliar. Com um único clique, é possível impedir que hackers roubem os seus dados transmitidos pelo ar. Os hackers não podem inserir cavalos de Tróia ou outros programas nocivos na sua rede. Eles não conseguem usar a sua rede sem fio como plataforma para lançar ataques de spam ou de vírus. Nem mesmo copiadores casuais de conteúdo protegido por copyright poderão usar a sua rede sem fio, portanto, você não será responsabilizado indevidamente por downloads ilegais de filmes ou músicas.

Nenhuma outra solução oferece a simplicidade ou a robustez da segurança oferecida pelo Wireless Home Network Security. A filtragem de endereços MAC ou desativação da difusão de SSID proporciona apenas uma proteção cosmética. Até mesmo hackers inexperientes podem contornar esses mecanismos fazendo download de ferramentas livremente disponíveis na Internet. Outros utilitários, como VPNs, não protegem a rede sem fio em si, portanto, você ainda fica vulnerável a uma infinidade de ataques.

O McAfee Wireless Home Network Security é o primeiro produto que verdadeiramente bloqueia a sua rede sem fio domiciliar.

Recursos

Esta versão do Wireless Home Network Security oferece os seguintes recursos:

- Proteção sempre ativada - detecta e protege automaticamente qualquer rede sem fio vulnerável à qual você se conecte.
- Interface intuitiva - proteja a sua rede sem a necessidade de tomar decisões difíceis ou conhecer termos técnicos complexos.
- Criptografia automática forte - permita que apenas os seus amigos e familiares tenham acesso à sua rede e proteja os seus dados durante o tráfego de informações.
- Uma solução inteiramente em software - o Wireless Home Network Security trabalha com o seu software de segurança e o seu roteador ou ponto de acesso sem fio padrão. Não é necessário adquirir hardware adicional.
- Rotação de chaves automática - mesmo os hackers mais determinados não conseguem capturar as suas informações porque a chave está sempre sendo alterada.
- Acréscimo de usuários de rede - você pode facilmente conceder acesso à sua rede para seus amigos e familiares.
- Ferramenta de conexão intuitiva - a ferramenta de conexão sem fio é intuitiva e informativa, com detalhes sobre a intensidade do sinal e as condições de segurança.

- Alertas e registro de eventos - alertas e relatórios de fácil interpretação oferecem aos usuários avançados mais informações sobre a sua rede sem fio.
- Modo de suspensão - suspenda temporariamente a rotação de chaves para que determinados aplicativos possam funcionar sem interrupção.
- Compatibilidade com outros equipamentos - o Wireless Home Network Security atualiza-se automaticamente com os mais recentes módulos de roteador ou ponto de acesso sem fio das marcas mais populares, como: Linksys®, NETGEAR®, D-Link®, Belkin® e outras.

Instalação a partir de um CD

1. Insira o CD do produto na unidade de CD-ROM. Se a instalação não for iniciada automaticamente, clique em **Iniciar** na área de trabalho do Windows e, em seguida, clique em **Executar**.
2. Na caixa de diálogo **Executar**, digite D:\SETUP.EXE (onde D é a letra da unidade de CD-ROM).
3. Clique em **OK**.
4. Vá para *Utilização do assistente de configuração* na página 23.

Instalação a partir do site

Ao instalar o Wireless Home Network Security a partir do site, você precisa salvar o arquivo de instalação. Esse arquivo é usado para instalar o Wireless Home Network Security em outros computadores.

1. Visite o site da McAfee e clique em **Minha conta**.
2. Se for solicitado, digite o endereço de e-mail e a senha para assinatura e clique em **Logon** para abrir a página **Informação da conta**.
3. Localize o seu produto na lista e clique em **Salvar destino como...** O arquivo de instalação será salvo no computador.

Instalação a partir do arquivo de instalação

Se você obteve o pacote de instalação através de um download (em vez de ter um CD), é necessário instalar o software em todos os computadores sem fio. Quando a rede estiver protegida, os computadores sem fio não poderão se conectar à rede sem inserir a chave. Escolha uma das opções seguintes:

- Antes de proteger a rede, faça download do pacote de instalação para cada computador sem fio.
- Copie o arquivo de instalação para uma "memory key" USB ou CD gravável e instale o software nos outros computadores sem fio.
- Se a rede já estiver protegida, conecte um cabo no roteador para fazer download do arquivo. Você também pode clicar em **Exibir chave de rede** para ver a chave atual e conectar-se à rede sem fio usando essa chave.

Após instalar o Wireless Home Network Security em todos os computadores sem fio, siga as instruções da tela. Quando você clicar em **Concluir**, o Assistente de configuração aparecerá. Vá para *Utilização do assistente de configuração* na página 23.

Utilização do assistente de configuração

O assistente de configuração é usado para:

- Proteger a sua rede a partir de um dos computadores sem fio. Para obter mais informações, consulte *Proteção de redes sem fio* na página 32.

  Se o Wireless Home Network Security não puder determinar o roteador ou ponto de acesso correto a ser protegido, você será solicitado a Repetir ou Cancelar. Experimente aproximar-se do roteador ou ponto de acesso a ser protegido e, em seguida, clique em **Repetir**.
- Associar-se a uma rede protegida (essa etapa não é necessária quando há apenas um computador sem fio).
- Conectar-se a uma rede. Para obter mais informações, consulte *Conexão a uma rede* na página 27.

Você será notificado se o seu adaptador sem fio não for detectado ou se o seu roteador ou ponto de acesso sem fio não estiver ligado.

Para visualizar o status da sua conexão, clique com o botão direito do mouse no ícone McAfee ( ), aponte para **Wireless Network Security** e selecione **Resumo**. A página **Resumo** aparece (Figura 2-1).

Figura 2-1. Página Resumo

Visualização da sua conexão

O painel Conexão mostra o status da sua conexão. Se quiser executar uma varredura da sua conexão sem fio, clique em **Varredura de segurança**.

- Status - se você está conectado ou desconectado. Se você estiver conectado, o nome da rede aparecerá.
- Segurança - o modo de segurança da rede.
- Velocidade - velocidade de conexão da sua placa de rede sem fio.
- Duração - por quanto tempo você esteve conectado a essa rede.
- Intensidade do sinal - nível de sinal da sua conexão sem fio.

Visualização da sua rede sem fio protegida

O painel Rede sem fio protegida oferece informações sobre a sua rede.

- Conexões feitas hoje - quantas vezes os usuários se conectaram a essa rede hoje.
- Rotações de chaves feitas hoje - quantas vezes a chave sofreu rotação hoje, incluindo o tempo decorrido desde a última rotação de chaves.
- Rotação de chaves suspensa - a rotação de chaves na sua rede está suspensa. Para retomar a rotação de chaves e assegurar que a sua rede fique totalmente protegida contra hackers, clique em **Continuar rotação de chaves**.
- Computadores protegidos neste mês - quantos computadores foram protegidos neste mês.
- Computadores - se você está conectado a uma rede protegida, mostra todos os computadores da rede e quando cada computador foi conectado pela última vez.

   - o computador está conectado.

   - o computador pode se reconectar sem se associar à rede.

   - o computador não está conectado. O computador precisa reassociar-se à rede porque a chave foi atualizada.

Clique em **Exibir eventos de rede** para ver eventos da rede. Consulte *Visualização de eventos* na página 28.

Clique em **Exibir chave atual** para ver a chave.

Se estiver conectando dispositivos sem fio para os quais o Wireless Home Network Security não oferece suporte (por exemplo, conectando um computador portátil sem fio à sua rede), siga estas etapas.

1. Na tela Resumo, clique em **Exibir chave atual**.
2. Anote a chave.
3. Clique em **Suspender rotação de chaves**. A suspensão da rotação de chaves evita que dispositivos que tenham sido conectados manualmente à rede sejam desconectados.
4. Insira a chave no dispositivo.

Ao terminar de usar tais dispositivos, clique em **Continuar rotação de chaves.** A McAfee recomenda retomar a rotação de chaves para garantir que a sua rede seja totalmente protegida contra hackers.

Para selecionar redes sem fio às quais se conectar ou se associar, clique com o botão direito do mouse no ícone McAfee ( ), aponte para **Wireless Network Security** e selecione **Redes sem fio disponíveis**. A página **Redes sem fio disponíveis** aparece (Figura 2-2).

Figura 2-2. Página Redes sem fio disponíveis

Quando você está conectado a uma rede sem fio protegida, as informações enviadas e recebidas são criptografadas. Hackers não podem interceptar os dados transmitidos através da rede protegida e não podem se conectar à sua rede.

- a rede está protegida.

- a rede está protegida com segurança WEP ou WPA-PSK.

- a rede não está protegida, mas você pode se conectar a ela mesmo assim (não recomendado).

Gerenciamento de redes sem fio

Esta seção fornece informações sobre o gerenciamento de redes sem fio.

Conexão a uma rede

Para se conectar a uma rede, selecione a rede à qual deseja se conectar e clique em **Conectar**. Se você configurou manualmente uma chave pré-compartilhada para o seu roteador ou ponto de acesso, também será necessário digitar a chave.

Se a rede está protegida, você precisa se associar a ela para poder conectá-la. Para se associar à rede, um usuário que já esteja conectado à rede precisa lhe dar permissão.

Quando você se associa a uma rede, é possível reconectar-se a ela sem a necessidade de se associar novamente. Você também pode conceder permissão para outros usuários se associarem a essa rede.

Desconexão de uma rede

Para se desconectar da rede à qual está conectado, clique em **Desconectar**.

Utilização de opções avançadas

Se quiser usar opções de conexão avançadas, clique em **Avançado**. A caixa de diálogo **Configurações avançadas** será exibida. A partir dessa caixa de diálogo, é possível fazer o seguinte.

- Alterar a ordem das redes às quais você se conecta automaticamente - a rede do início da lista é aquela à qual você se conectou por último e é a que o Wireless Home Network Security tenta conectar primeiro. Para mover uma rede, selecione-a e clique em **Mover para cima** ou **Mover para baixo**. Por exemplo, se você mudou de lugar e a última rede à qual se conectou está muito distante e não tem um sinal forte, é possível mover a rede que tem o sinal mais forte para o início da sua lista.
- Remover redes preferidas - você pode remover redes dessa lista. Por exemplo, se você se conectou por engano à rede do seu vizinho, ela foi incluída nessa lista. Para removê-la, selecione-a e clique em **Remover**.
- Modificar propriedades de rede - se estiver com problemas para se conectar a uma rede não protegida, é possível modificar suas propriedades. Observe que essa opção só se aplica a redes que não estão protegidas. Para modificar propriedades, selecione uma rede e clique em **Propriedades**.
- Adicionar redes que não divulgam SSID - por exemplo, se você estiver tentando se conectar à rede sem fio de um amigo, mas ela não aparecer na lista, clique em **Adicionar** e digite as informações apropriadas. Observe que a rede adicionada não pode ser protegida pelo Wireless Home Network Security.

Para configurar opções, clique com o botão direito do mouse no ícone McAfee ( ), aponte para **Wireless Network Security** e selecione **Opções**. A página **Opções** aparece (Figura 2-3).

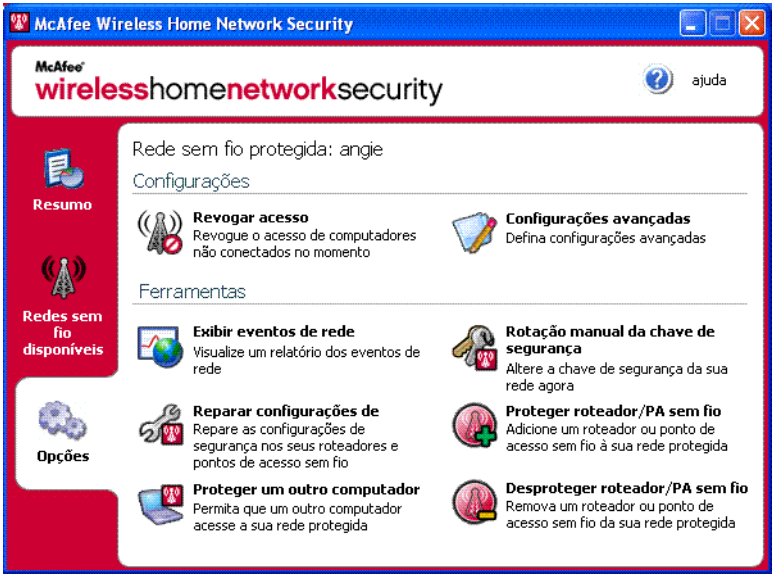


Figura 2-3. Página Opções

Visualização de eventos

As ações executadas pelo Wireless Home Network Security são armazenadas em registros de eventos. Para ver esses registros, clique em **Exibir eventos de rede**. As informações aparecem em ordem cronológica por padrão.

Na caixa **Eventos da rede**, é possível selecionar o tipo de evento exibido (todos os eventos continuam registrados) e é possível visualizar eventos de qualquer rede à qual você pertença (caso pertença a mais de uma rede).

Quando ocorre um evento, aparece um alerta com uma breve descrição.

Definição de configurações avançadas

Esta seção é para usuários avançados. Clique em **Configurações avançadas** para definir configurações de segurança, alerta e outras.

Quando alterar uma configuração, clique em **OK** para que as alterações tenham efeito. Observe que, após você clicar em **OK**, todos os computadores conectados perdem temporariamente a conectividade por alguns minutos.

Definição de configurações de segurança

Use a guia **Configurações de segurança** para alterar as suas configurações de segurança.

- Nome da rede sem fio protegida - nome da rede protegida atual. Quando você altera o nome de uma rede, ela aparece na lista **Redes sem fio disponíveis** e você precisa reconectar-se à rede.
- Modo de segurança - modo de segurança atual. Para alterar a segurança padrão (WEP), selecione WPA-PSK TKIP para uma criptografia mais forte. Verifique se os roteadores, pontos de acesso e adaptadores sem fio que se conectam à sua rede têm suporte para esse modo, caso contrário eles não poderão se conectar. Para obter mais informações sobre atualização do seu adaptador, consulte *Atualização do seu adaptador sem fio* na página 41.
- Ativar rotação de chaves automática - para suspender a rotação de chaves, desmarque essa opção. Para alterar a freqüência da rotação de chaves, mova o controle deslizante. Para obter mais informações sobre rotação de chaves, consulte *Visualização da sua rede sem fio protegida* na página 25.
- Alterar nome do usuário ou senha - por motivo de segurança, você pode alterar a senha ou o nome do usuário padrão para o roteador ou ponto de acesso sem fio selecionando-o e clicando em **Alterar nome do usuário ou senha**. A senha ou o nome do usuário padrão é aquele que você usou quando efetuou logon e configurou o seu roteador ou ponto de acesso.

Definição de configurações de alerta

Use a guia **Configurações de alerta** para alterar as suas configurações de alerta.

Selecione o tipo de evento sobre o qual você deseja ser alertado e clique em **OK**. Se não quiser ser alertado sobre determinados tipos de evento, desmarque a caixa apropriada.

Definição de outras configurações

Use a guia **Outras configurações** para alterar outras configurações.

- Exibir chaves em texto simples - para redes não protegidas pelo Wireless Home Network Security. As chaves para redes desprotegidas que aparecem na lista **Redes sem fio disponíveis** podem ser mostradas em texto simples em vez de asteriscos. Se você exibe chaves em texto simples, as suas chaves são descartadas por motivo de segurança.
- Descartar todas as chaves salvas - para redes não protegidas pelo Wireless Home Network Security. Exclui todas as chaves que foram salvas. Observe que, se excluir essas chaves, você terá de digitá-las novamente ao se conectar a redes WEP e WPA-PSK.

- Sair da rede - para redes protegidas pelo Wireless Home Network Security. Você pode cancelar os seus direitos de acesso a uma rede sem fio protegida. Por exemplo, se você deseja sair de uma rede e não planeja se conectar a ela novamente, selecione-a na lista e clique em **Sair da rede**.
- Exibir mensagem de notificação quando conectado a uma rede sem fio - quando uma conexão é feita, uma mensagem de notificação aparece.

Revogação do acesso à rede

Para evitar que computadores que se associaram à rede, mas que ainda não se conectaram a ela, tenham acesso à sua rede:

1. Clique em **Revogar acesso**. A caixa de diálogo **Revogar acesso** aparece.
2. Clique em **Revogar**.

A rotação de chaves para a rede está redefinida e os computadores atualmente conectados recebem a nova chave e permanecem conectados. Os computadores que não estão conectados no momento não recebem a chave atualizada, precisando reassociar-se à rede para poderem se conectar.

Quando você revoga o acesso de um computador, esse computador precisa se reassociar à rede para que possa se conectar à rede protegida novamente. Para isso, o computador precisa ter o Wireless Home Network Security instalado (consulte *Instalação do Internet Security Suite-Wireless Network Edition* na página 15), conectar-se à rede protegida e associar-se a ela (consulte *Conexão a uma rede* na página 27).

Reparo de configurações de segurança

Somente repare as configurações de segurança se estiver tendo problemas com a sua rede sem fio. Para obter mais informações, consulte *Não foi possível conectar* na página 41.

Para corrigir as configurações do seu roteador ou ponto de acesso na rede atual, siga estas etapas.

1. Clique em **Reparar configurações de segurança.** A caixa de diálogo **Reparar** aparece.
2. Clique em **Reparar**.
3. Clique em **Fechar** quando terminar.

Uma mensagem de erro aparece quando uma conexão não pode ser feita com os roteadores ou pontos de acesso da rede. Conecte-se à sua rede utilizando um cabo e, em seguida, tente reparar novamente. Se a senha para o roteador ou ponto de acesso tiver sido alterada, você será solicitado a informar a nova senha.

Proteção de outros computadores

Para obter mais informações sobre proteção de outros computadores e sobre como conceder acesso à sua rede protegida, clique em **Proteger um outro computador**.

Para proteger um outro computador:

1. Instale o McAfee Wireless Home Network Security no computador que você deseja proteger.
2. No computador sendo protegido, clique com o botão direito do mouse no ícone McAfee ( ), aponte para **Wireless Network Security** e selecione **Redes sem fio disponíveis**. A página **Redes sem fio disponíveis** aparece.
3. Selecione uma rede protegida para se associar e clique em **Conectar**. Observe que um usuário já conectado à rede precisa lhe dar permissão para que você possa se associar à rede.

   Quando você se associa a uma rede, é possível reconectar-se a ela sem a necessidade de se associar novamente. Você também pode conceder permissão para outros usuários se associarem a essa rede.
4. Clique em **OK** na caixa de diálogo de confirmação.

Se estiver conectando dispositivos sem fio para os quais o Wireless Home Network Security não oferece suporte (por exemplo, conectando um computador portátil sem fio à sua rede), siga estas etapas.

1. Na tela Resumo, clique em **Exibir chave atual**.
2. Anote a chave.
3. Clique em **Suspender rotação de chaves**. A suspensão da rotação de chaves evita que dispositivos que tenham sido conectados manualmente à rede sejam desconectados.
4. Insira a chave no dispositivo.

Ao terminar de usar tais dispositivos, clique em **Continuar rotação de chaves.** A McAfee recomenda retomar a rotação de chaves para garantir que a sua rede seja totalmente protegida contra hackers.

Rotação de chaves

Para fazer rotação da chave de segurança da sua rede, clique em **Rotação manual da chave de segurança**.

Proteção de redes sem fio

Para proteger um roteador ou ponto de acesso, siga estas etapas.

1. Clique em **Proteger roteador/PA sem fio**. A caixa de diálogo **Proteger rede sem fio** aparece. Se o roteador ou ponto de acesso não aparecer na lista, clique em **Atualizar**.
2. Selecione o roteador ou ponto de acesso a ser protegido e clique em **Proteger**.

Desproteção de redes sem fio

É necessário estar conectado ao roteador ou ponto de acesso sem fio que você está desprotegendo.

Para desproteger um roteador ou ponto de acesso, siga estas etapas.

1. Clique em **Desproteger roteador/PA sem fio**. A caixa de diálogo **Desproteger roteador/PA sem fio** aparece. Se o roteador ou ponto de acesso não aparecer na lista, clique em **Atualizar**.
2. Selecione o roteador ou ponto de acesso a ser desprotegido e clique em **Desproteger**.

Quando você está conectado à Internet, o Wireless Home Network Security verifica a cada quatro horas se há atualizações de software e faz download das atualizações e as instala toda semana, automaticamente, sem interromper o seu trabalho. Essas atualizações têm um impacto mínimo no desempenho do sistema durante o download.

Se ocorrer uma atualização de produto, um alerta será exibido. Quando alertado, você pode optar por atualizar o Wireless Home Network Security.

Verificação automática de atualizações

O McAfee SecurityCenter é configurado automaticamente para verificar se há atualizações para cada um dos seus serviços McAfee a cada quatro horas quando você está conectado à Internet, notificando-o com alertas e sons. Por padrão, o SecurityCenter faz download e instala automaticamente quaisquer atualizações disponíveis.

NOTA
Em alguns casos, pede-se que o computador seja reiniciado para concluir a atualização. Salve todo o seu trabalho e feche todos os aplicativos antes de reiniciar.

Verificação manual de atualizações

Além de verificar automaticamente se há atualizações quando se está conectado à Internet, também é possível verificar manualmente a qualquer momento.

Para verificar manualmente se há atualizações para o Wireless Home Network Security:

1. Verifique se o computador está conectado à Internet.
2. Clique com o botão direito do mouse no ícone McAfee e, em seguida, clique em **Atualizações**. A caixa de diálogo **Atualizações do SecurityCenter** aparece.
3. Clique em **Verificar agora**.

   Se houver uma atualização, a caixa de diálogo **McAfee SecurityCenter** será exibida. Clique em **Atualizar** para continuar.

   Se nenhuma atualização estiver disponível, uma caixa de diálogo informará que o Wireless Home Network Security está atualizado. Clique em **OK** para fechar a caixa de diálogo.
4. Se for solicitado, efetue logon no site. O **Assistente de atualização** instala automaticamente a atualização.
5. Clique em **Concluir** quando a instalação da atualização estiver concluída.

   NOTA
   Em alguns casos, pede-se que o computador seja reiniciado para concluir a atualização. Salve todo o seu trabalho e feche todos os aplicativos antes de reiniciar.

Os alertas aparecem quando ocorre um evento, notificando alterações na rede.

Acesso revogado

Um usuário atualizou a chave de rede. Para obter mais informações, consulte *Revogação do acesso à rede* na página 30.

Computador conectado

Um usuário conectou-se à rede. Para obter mais informações, consulte *Conexão a uma rede* na página 27.

Computador desconectado

Um usuário desconectou-se da rede. Para obter mais informações, consulte *Desconexão de uma rede* na página 27.

Computador protegido

Um usuário com acesso à rede protegida concedeu acesso a mais alguém. Por exemplo: 'Lance' deu acesso a 'Mercks' e agora eles podem usar a rede sem fio 'CoppiWAP'.

Falha na rotação de chaves

A rotação de chaves falhou porque:

- As informações de logon para o seu roteador ou ponto de acesso foram alteradas. Se você tem as informações de logon, consulte *Reparo de configurações de segurança* na página 30.
- A versão do firmware do seu roteador ou ponto de acesso foi alterada para uma versão não suportada. Para obter mais informações, consulte *Não foi possível conectar* na página 41.
- O seu roteador ou ponto de acesso não está disponível. Verifique se o roteador ou ponto de acesso está ligado e se está conectado à sua rede.
- Erro de administrador duplicado. Para obter mais informações, consulte *Erro de administrador duplicado* na página 38.

Se você está com problemas para se conectar a essa rede, consulte *Reparo de configurações de segurança* na página 30.

Rotação de chaves retomada

Um usuário retomou a rotação de chaves. A rotação de chaves impede que hackers acessem a sua rede.

Rotação de chaves suspensa

Um usuário suspendeu a rotação de chaves. A McAfee recomenda retomar a rotação de chaves para garantir que a sua rede seja totalmente protegida contra hackers.

Configuração de rede alterada

Um usuário alterou o modo de segurança da rede. Para obter mais informações, consulte *Definição de configurações de segurança* na página 29.

Rede renomeada

Um usuário renomeou a rede e você precisa se conectar novamente. Para obter mais informações, consulte *Conexão a uma rede* na página 27.

Rede reparada

Um usuário tentou reparar a rede porque teve problemas ao se conectar.

Configurações de rede alteradas

Um usuário está prestes a alterar configurações de segurança da rede. A sua conexão pode ser interrompida por alguns instantes enquanto isso ocorre. A configuração que está sendo alterada pode ser uma ou mais das seguintes:

- Nome da rede
- Modo de segurança
- Freqüência da rotação de chaves
- Status da rotação de chaves automatizada

Senha alterada

Um usuário alterou o nome do usuário ou senha em um roteador ou ponto de acesso na rede. Para obter mais informações, consulte *Definição de configurações de segurança* na página 29.

Chave de segurança trocada

A chave de segurança da rede sofreu rotação. O McAfee Wireless Home Network Security faz rotação da sua chave de criptografia de rede automaticamente, tornando mais difícil para os hackers interceptarem os seus dados ou se conectarem à sua rede.

Freqüência da rotação de chaves de segurança alterada

A freqüência da rotação de chaves de segurança da rede foi alterada. O McAfee Wireless Home Network Security faz rotação da sua chave de criptografia de rede automaticamente, tornando mais difícil para os hackers interceptarem os seus dados ou se conectarem à sua rede.

Roteador/PA sem fio protegido

Um roteador ou ponto de acesso sem fio foi protegido na sua rede. Para obter mais informações, consulte *Proteção de redes sem fio* na página 32.

Roteador/PA sem fio desprotegido

Um roteador ou ponto de acesso sem fio foi removido da rede. Para obter mais informações, consulte *Desproteção de redes sem fio* na página 32.

Solução de problemas

Este capítulo descreve procedimentos para solução de problemas com o McAfee Wireless Home Network Security e equipamentos de outros fabricantes.

Instalação

Esta seção explica como resolver problemas de instalação.

Em quais computadores instalar o software

Instale o McAfee Wireless Home Network Security em todos os computadores sem fio da sua rede (ao contrário de outros aplicativos da McAfee, esse software pode ser instalado em vários computadores).

É possível (mas não obrigatório) instalar em computadores que não tenham adaptadores sem fio, mas o software não estará ativo nesses computadores porque eles não precisam de proteção sem fio. Você precisa proteger o seu roteador ou ponto de acesso (consulte *Proteção de redes sem fio* na página 32) a partir de um dos computadores sem fio para tornar a sua rede segura.

Adaptador sem fio não detectado

Se o seu adaptador sem fio não é detectado ao ser instalado e ativado, reinicie o computador. Se o adaptador continuar não sendo detectado após o computador ser reiniciado, siga estas etapas.

1. Abra a caixa de diálogo **Propriedades de conexões de rede sem fio**.
2. Desmarque a caixa **Filtro do MWL** e, em seguida, selecione-a.
3. Clique em **OK**.

Se isso não funcionar, talvez o seu adaptador sem fio não seja suportado. Atualize o seu adaptador ou adquira um novo. Para ver uma lista de adaptadores suportados, visite http://www.mcafee.com/br/router. Para atualizar o seu adaptador, consulte *Atualização do seu adaptador sem fio* na página 41.

Múltiplos adaptadores sem fio

Se um erro informa que você tem múltiplos adaptadores sem fio instalados, você precisa desativar ou desconectar um deles. O Wireless Home Network Security funciona com apenas um adaptador sem fio.

Não foi possível fazer download em computadores sem fio porque a rede já está segura

Se você tem um CD, instale o McAfee Wireless Home Network Security a partir do CD em todos os seus computadores sem fio.

Caso tenha instalado o software em um computador sem fio e protegido a rede antes de instalar o software em todos os outros computadores sem fio, você tem as opções seguintes.

- Desproteja a rede (consulte *Desproteção de redes sem fio* na página 32). Em seguida, faça download do software e instale-o em todos os computadores sem fio. Proteja a rede novamente (consulte *Proteção de redes sem fio* na página 32).
- Visualize a chave de rede (consulte *Visualização da sua rede sem fio protegida* na página 25). Em seguida, digite a chave no seu computador sem fio para conectar-se à rede. Faça download do software, instale-o e associe-se à rede a partir do computador sem fio (consulte *Proteção de outros computadores* na página 31).
- Faça download do arquivo executável no computador que já está conectado à rede e salve-o em uma "memory key" USB ou grave-o em um CD para que você possa instalá-lo nos outros computadores.

Proteção ou configuração da sua rede

Esta seção explica como solucionar problemas que ocorrem ao proteger ou configurar a sua rede.

Roteador ou ponto de acesso não suportado

Se um erro informa que o seu roteador ou ponto de acesso sem fio talvez não seja suportado, o McAfee Wireless Home Network Security não pôde configurar o seu dispositivo porque não o reconheceu ou porque não o encontrou.

Verifique se você tem a versão mais recente do Wireless Home Network Security solicitando uma atualização (a McAfee está constantemente acrescentando suporte para novos roteadores e pontos de acesso). Se o seu roteador ou ponto de acesso aparece na lista de http://www.mcafee.com/br/router e esse erro ainda ocorre, você está com problemas de comunicação entre o computador e o roteador ou ponto de acesso. Consulte *Não foi possível conectar* na página 41 antes de proteger a sua rede novamente.

Atualização do firmware do roteador ou ponto de acesso

Se um erro informa que a revisão do firmware do seu roteador ou ponto de acesso sem fio não é suportada, isso significa que o seu dispositivo é suportado, mas a revisão do firmware do dispositivo não é. Verifique se você tem a versão mais recente do Wireless Home Network Security solicitando uma atualização (a McAfee está constantemente acrescentando suporte para novas revisões de firmware).

Se você tem a versão mais recente do Wireless Home Network Security, consulte o site ou organização de suporte do fabricante do seu roteador ou ponto de acesso e instale uma versão de firmware que esteja listada em http://www.mcafee.com/br/router.

Erro de administrador duplicado

Após configurar o seu roteador ou ponto de acesso, você precisa efetuar logoff na interface de administração. Em alguns casos, se você não efetuar logoff, o roteador ou ponto de acesso atuará como se um outro computador ainda o estivesse configurando e uma mensagem de erro aparecerá.

Se não puder efetuar logoff, desconecte a alimentação do roteador ou ponto de acesso e, em seguida, conecte-a novamente.

A rede aparece insegura

Se a sua rede aparece como insegura, ela não está protegida. É necessário proteger a rede (consulte *Proteção de redes sem fio* na página 32) para torná-la segura. Observe que o McAfee Wireless Home Network Security só trabalha com roteadores e pontos de acesso compatíveis (consulte http://www.mcafee.com/br/router).

Não foi possível reparar

Se o reparo falhar, tente o seguinte. Observe que cada procedimento é independente.

- Conecte-se à sua rede utilizando um cabo e, em seguida, tente reparar novamente.
- Desligue a alimentação do roteador ou ponto de acesso, ligue-a novamente e experimente conectar.
- Redefina o roteador ou ponto de acesso sem fio com sua configuração padrão e repare-o.
- Utilizando as opções avançadas, saia da rede em todos os computadores, redefina o roteador ou ponto de acesso sem fio com suas configurações padrão e, em seguida, proteja a rede.

Conexão de computadores à sua rede

Esta seção explica como solucionar problemas que ocorrem ao conectar computadores à sua rede.

Aguardando autorização

Se você tentar se associar a uma rede protegida e o seu computador permanecer aguardando autorização, verifique o seguinte.

- Se um computador sem fio que já tenha acesso à rede está ligado e conectado à rede.
- Se há alguém presente para conceder acesso nesse computador quando ele aparece.
- Se os computadores se encontram dentro do alcance um do outro.

Se **Conceder** não aparecer no computador que já tem acesso à rede, experimente conceder a partir de um outro computador.

Se não houver outros computadores disponíveis, desproteja a rede a partir do computador que já tem acesso e proteja a rede a partir do computador que não tinha acesso. Em seguida, associe-se à rede a partir do computador que protegeu a rede originalmente.

Concessão de acesso a um computador desconhecido

Quando você receber de um computador desconhecido uma solicitação para concessão de acesso, verifique se é familiar. Alguém pode estar tentando um acesso ilegítimo à sua rede.

Conexão a uma rede ou à Internet

Esta seção explica como solucionar problemas que ocorrem ao conectar a uma rede ou à Internet.

Conexão deficiente com a Internet

Se não conseguir se conectar, experimente acessar a sua rede utilizando um cabo e, em seguida, conecte-se à Internet. Se ainda assim não conseguir, verifique se:

- o modem está ligado
- as suas configurações PPPoE (consulte o *Glossário* na página 173) estão corretas
- a sua linha DSL ou de cabo está ativa

Problemas de conectividade, como velocidade e intensidade do sinal, também podem ser causados por interferência de equipamentos sem fio. Experimente mudar o canal do seu telefone sem fio, eliminar possíveis fontes de interferência ou mudar o seu ponto de acesso, roteador sem fio ou computador de lugar.

A conexão pára por alguns instantes

Quando a sua conexão pára por alguns instantes (por exemplo, durante um jogo on-line), a rotação de chaves pode estar causando breves atrasos na rede. Suspenda momentaneamente a rotação de chaves. A McAfee recomenda retomar a rotação de chaves assim que possível para garantir que a rede fique totalmente protegida contra hackers.

Dispositivos (que não o computador) perdendo a conexão

Se alguns dispositivos estão perdendo a conexão quando você usa o McAfee Wireless Home Network Security, suspenda a rotação de chaves.

Solicitado a digitar a chave WEP ou WPA

Se é necessário digitar uma chave WEP ou WPA para se conectar à sua rede, você provavelmente não instalou o software no seu computador. Para funcionar corretamente, o Wireless Home Network Security precisa estar instalado em todos os computadores sem fio da sua rede. Consulte *Proteção ou configuração da sua rede* na página 37.

Não foi possível conectar

Se não conseguir se conectar, experimente o seguinte. Observe que cada procedimento é independente.

- Se não estiver se conectando a uma rede protegida, verifique se você tem a chave correta e digite-a novamente.
- Desconecte o adaptador sem fio e conecte-o novamente ou desative-o e reative-o.
- Desligue o roteador ou ponto de acesso, ligue-o novamente e, em seguida, tente conectar.
- Verifique se o seu roteador ou ponto de acesso sem fio está conectado e repare as configurações de segurança (consulte *Reparo de configurações de segurança* na página 30).

  Se o reparo falhar, consulte *Não foi possível reparar* na página 38.
- Reinicie o computador.
- Atualize o adaptador sem fio ou compre um novo. Para atualizar o seu adaptador, consulte *Atualização do seu adaptador sem fio* na página 41. Por exemplo, a sua rede pode estar usando segurança WPA-PSK TKIP e talvez o seu adaptador sem fio não suporte o modo de segurança da rede (as redes mostram WEP, muito embora estejam definidas como WPA).
- Se não puder se conectar após atualizar o roteador ou ponto de acesso sem fio, talvez você o tenha atualizado para uma versão não suportada. Verifique se o roteador ou ponto de acesso é suportado. Se a versão não for suportada, remova a atualização para voltar a uma versão suportada ou espere até que uma atualização do Wireless Home Network Security esteja disponível.

Atualização do seu adaptador sem fio

Para atualizar o seu adaptador, siga estas etapas.

1. Na área de trabalho, clique em **Iniciar**, aponte para **Configurações** e, em seguida, selecione **Painel de controle**.
2. Clique duas vezes no ícone **Sistema**. A caixa de diálogo **Propriedades do sistema** aparece.
3. Selecione a guia **Hardware** e, em seguida, clique em **Gerenciador de dispositivos**.
4. Na lista **Gerenciador de dispositivos**, clique duas vezes no seu adaptador.
5. Selecione a guia **Driver** e anote o driver que você possui.

6 Visite o site do fabricante do adaptador e veja se há uma atualização disponível. Os drivers costumam ser encontrados na seção Suporte ou Downloads.

7 Se houver uma atualização de driver disponível, siga as instruções do site para fazer download.

8 Volte para a guia **Driver** e clique em **Atualizar driver**. Um assistente do Windows aparecerá.

9 Siga as instruções da tela.

Nível de sinal fraco

Se a sua conexão cai ou está lenta, o nível do sinal pode não estar suficientemente forte. Para melhorar o seu sinal, tente o seguinte.

- Verifique se os seus dispositivos sem fio não estão sendo bloqueados por objetos metálicos, como aquecedores, dutos ou aparelhos volumosos. Os sinais sem fio não se propagam bem através desses objetos.
- Se o seu sinal atravessa paredes, certifique-se de que ele não tenha de fazê-lo em um ângulo muito raso. Quanto maior o espaço percorrido pelo sinal dentro da parede, mais fraco ele fica.
- Se o seu roteador ou ponto de acesso sem fio possui mais de uma antena, experimente orientar ambas as antenas perpendicularmente entre si (por exemplo, uma na vertical e outra na horizontal, em um ângulo de 90 graus).
- Alguns fabricantes produzem antenas de alto ganho. Antenas direcionais proporcionam maior alcance, enquanto antenas onidirecionais oferecem maior versatilidade. Consulte as instruções de instalação do fabricante para instalar a antena.

Se essas etapas não forem bem-sucedidas, adicione à sua rede um ponto de acesso que esteja mais perto do computador ao qual você está tentando se conectar. Se você configurar o seu segundo ponto de acesso com o mesmo nome de rede (SSID) e um canal diferente, o seu adaptador encontrará automaticamente o sinal mais forte e fará a conexão através do ponto de acesso apropriado.

O Windows não pôde configurar a sua conexão sem fio

Ao receber uma mensagem informando que o Windows não pôde configurar a sua conexão sem fio, você pode ignorar isso. Use o Wireless Home Network Security para conectar e configurar redes sem fio. Na caixa de diálogo **Propriedades de conexões de rede sem fio** do Windows, sob a guia **Redes sem fio**, verifique se a caixa **Usar o Windows para definir minhas configurações de rede sem fio** está desmarcada.

Windows mostrando que não há conexão

Se você estiver conectado, mas o ícone de rede do Windows estiver mostrando um X (sem conexão), ignore isso. A sua conexão está boa.

Outros problemas

Esta seção explica como solucionar outros tipos de problemas.

Nome de rede diferente ao utilizar outros programas

Se o nome da rede for diferente ao ser visualizado através de outros programas (por exemplo, tendo _SafeAaf como parte do nome), isso é normal. O Wireless Home Network Security marca as redes com um código quando elas são protegidas.

Problemas ao configurar roteadores ou pontos de acesso sem fio

Se aparecer um erro ao configurar o seu roteador ou ponto de acesso ou ao adicionar múltiplos roteadores na rede, verifique se cada roteador e ponto de acesso possui um endereço IP distinto.

Se o nome do seu roteador ou ponto de acesso sem fio aparece na caixa de diálogo **Proteger roteador/PA sem fio**, mas ocorre um erro quando você o configura: Verifique se há suporte para o seu roteador ou ponto de acesso. Para ver uma lista de roteadores ou pontos de acesso suportados, visite http://www.mcafee.com/br/router.

Se o seu roteador ou ponto de acesso está configurado, mas não parece estar na rede correta (por exemplo, se não é possível ver os outros computadores ligados à LAN), verifique se você configurou o roteador ou ponto de acesso apropriado, e não o de seu vizinho. Desconecte a alimentação do roteador ou ponto de acesso e verifique se a conexão cai. Se o roteador ou ponto de acesso errado foi configurado, desproteja-o e, em seguida, proteja o roteador ou ponto de acesso certo.

Se você não consegue configurar ou adicionar o seu roteador ou ponto de acesso, havendo suporte para o mesmo, algumas alterações feitas por você podem estar impedindo-o de ser configurado corretamente.

- Siga as instruções do fabricante para configurar o seu roteador ou ponto de acesso sem fio para DHCP ou para configurar o endereço IP correto. Em alguns casos, o fabricante fornece uma ferramenta de configuração.
- Redefina o seu roteador ou ponto de acesso com os padrões de fábrica e tente reparar a sua rede novamente. Você pode ter alterado a porta de administração no roteador ou ponto de acesso ou desativado a administração sem fio. Verifique se você está usando a configuração padrão e se a configuração sem fio está ativada. Uma outra possibilidade é a administração http estar desativada. Nesse caso, verifique se a administração http está ativada.

- Se o seu roteador ou ponto de acesso sem fio não aparece na lista de roteadores ou pontos de acesso sem fio a serem protegidos ou conectados, ative a difusão de SSID e verifique se o roteador ou ponto de acesso está ativado.
- Se você for desconectado ou não puder estabelecer uma conexão, a filtragem de MAC pode estar ativada. Desative a filtragem de MAC.
- Caso não consiga executar operações de rede (por exemplo, compartilhar arquivos ou imprimir em impressoras compartilhadas) entre dois computadores com conexão sem fio à rede, verifique se você não ativou o "AP Isolation". Esse recurso impede que computadores sem fio se conectem uns aos outros através da rede.

Substituição de computadores

Se o computador que protegia a rede foi substituído e não há computador algum que tenha acesso (ou seja, se você não consegue acessar a rede), redefina o roteador ou ponto de acesso sem fio com seus padrões de fábrica e proteja a rede novamente.

Software não funcionando após atualização de sistema operacional

Se o Wireless Home Network Security não funcionar após uma atualização do sistema operacional, desinstale-o e, em seguida, reinstale-o.

McAfee VirusScan 3

Bem-vindo ao McAfee VirusScan.

O McAfee VirusScan é um serviço de assinatura antivírus que oferece uma proteção abrangente, confiável e atualizada contra vírus. Equipado com a premiada tecnologia de varredura da McAfee, o VirusScan protege o computador contra vírus, worms, cavalos de Tróia, scripts suspeitos, ataques híbridos e outras ameaças.

Ele oferece os seguintes recursos:

ActiveShield — Faz varredura dos arquivos quando estes são acessados por você ou pelo seu computador.

Fazer varredura — Procura vírus e outras ameaças em unidades de disco rígido, disquetes e em arquivos e pastas individuais.

Quarentena — Criptografa e isola temporariamente arquivos suspeitos na pasta de quarentena até que uma ação apropriada possa ser realizada.

Detecção de atividades hostis — Monitora o computador em busca de atividades semelhantes às de vírus causadas por scripts mal-intencionados e atividades semelhantes às de worms.

Novos recursos

Esta versão do VirusScan possui os seguintes novos recursos:

- **Detecção e remoção de spyware e adware**
  O VirusScan identifica e remove spyware, adware e outros programas que comprometem sua privacidade e reduzem o desempenho do seu computador.
- **Atualizações automáticas diárias**
  As atualizações automáticas diárias do VirusScan protegem contra as mais recentes ameaças ao computador, identificadas ou não.
- **Varredura rápida em segundo plano**
  Varreduras rápidas e discretas, que identificam e destroem vírus, cavalos de Tróia, worms, spyware, adware, discadores e outras ameaças sem interromper o seu trabalho.
- **Alertas de segurança em tempo real**
  Os alertas de segurança notificam emergências, como epidemias de vírus e ameaças à segurança, além de oferecerem opções de resposta para remover, neutralizar ou aprender mais sobre a ameaça.

- **Detecção e limpeza em vários pontos de entrada**
  O VirusScan monitora e limpa os principais pontos de entrada do computador: e-mails, anexos de mensagens instantâneas e downloads da Internet.
- **Monitoração de atividades semelhantes às de worms no e-mail**
  O WormStopper™ monitora comportamentos suspeitos de envio de mensagens em massa e impede a disseminação de vírus e worms para outros computadores por e-mail.
- **Monitoração de atividades semelhantes às de worms em scripts**
  O ScriptStopper™ monitora a execução de scripts suspeitos e impede a disseminação de vírus e worms para outros computadores por e-mail.
- **Suporte técnico gratuito por e-mail e mensagens instantâneas**
  O suporte técnico ao vivo fornece assistência imediata e fácil, usando mensagens instantâneas e e-mail.

Teste do VirusScan

Antes de começar a usar o VirusScan, deve-se testar a instalação. Siga as etapas abaixo para testar separadamente os recursos Fazer varredura e ActiveShield.

Teste do ActiveShield

NOTA
Para testar o ActiveShield a partir da guia VirusScan no SecurityCenter, clique em **Testar VirusScan** para ver uma seção de perguntas freqüentes do suporte on-line que contém essas etapas.

Para testar o ActiveShield:

1. Visite http://www.eicar.com/ com o seu navegador.
2. Clique no link **The AntiVirus testfile eicar.com** (O arquivo de teste de antivírus eicar.com).
3. Vá para o final da página. Em **Download**, você verá quatro links.
4. Clique em **eicar.com**.

Se o ActiveShield estiver funcionando adequadamente, ele detectará o arquivo eicar.com imediatamente após o clique no link. Você pode tentar excluir ou colocar em quarentena arquivos detectados para saber como o ActiveShield lida com possíveis ameaças. Consulte *Compreensão dos alertas de segurança* na página 60 para obter detalhes.

Teste do recurso Fazer varredura

Antes de testar o recurso Fazer varredura, é necessário desativar o ActiveShield para impedir que ele detecte os arquivos de teste antes da varredura. Após desativá-lo, faça o download dos arquivos de teste.

Para fazer download dos arquivos de teste:

1. Desative o ActiveShield: Clique com o botão direito do mouse no ícone da McAfee, aponte para **VirusScan** e clique em **Desativar**.
2. Faça o download de arquivos de teste EICAR no site da EICAR:
   a. Visite http://www.eicar.com/.
   b. Clique no link **The AntiVirus testfile eicar.com** (O arquivo de teste de antivírus eicar.com).
   c. Vá para o final da página. Em **Download**, você verá estes links:

      eicar.com contém uma linha de texto que o VirusScan detecta como vírus.

      eicar.com.txt (opcional) é o mesmo arquivo, mas com um outro nome, para os usuários que têm dificuldade em fazer o download do primeiro link. Basta renomear o arquivo como "eicar.com" após o download.

      eicar_com.zip é uma cópia do vírus de teste dentro de um arquivo compactado .ZIP (um arquivo do WinZip™).

      eicarcom2.zip é uma cópia do vírus de teste dentro de um arquivo compactado .ZIP que, por sua vez, está dentro de um arquivo compactado .ZIP.

   d. Clique em cada link para fazer o download do arquivo correspondente. Para cada arquivo, é exibida uma caixa de diálogo **Download de arquivo**.
   e. Clique em **Salvar**, clique no botão **Criar nova pasta** e renomeie a pasta como **Pasta de varredura do VSO**.
   f. Clique duas vezes em **Pasta de varredura do VSO** e, em seguida, clique novamente em **Salvar** em cada uma das caixas de diálogo **Salvar como**.
3. Quando terminar o download dos arquivos, feche o Internet Explorer.
4. Ative o ActiveShield: Clique com o botão direito do mouse no ícone da McAfee, aponte para **VirusScan** e clique em **Ativar**.

Para testar o recurso Fazer varredura:

1 Clique com o botão direito do mouse no ícone da McAfee, aponte para **VirusScan** e clique em **Fazer varredura**.

2 Utilizando a árvore de diretórios no painel esquerdo da caixa de diálogo, vá até a **Pasta de varredura do VSO** em que você salvou os arquivos:

   a Clique no sinal **+** ao lado do ícone da unidade C.

   b Clique em **Pasta de varredura do VSO** para selecioná-la (não clique no sinal **+** ao lado dessa opção).

   Isso indica que a opção Fazer varredura deve verificar somente essa pasta. Você também pode colocar os arquivos em locais aleatórios na unidade de disco rígido para obter uma demonstração mais convincente da capacidade do recurso Fazer varredura.

3 Na área **Opções de varredura** da caixa de diálogo **Fazer varredura**, verifique se todas as opções estão selecionadas.

4 Clique em **Fazer varredura** na parte inferior direita da caixa de diálogo.

   O VirusScan faz a varredura da **Pasta de varredura do VSO**. Os arquivos de teste EICAR que você salvou nessa pasta serão exibidos na **Lista de arquivos detectados**. Isso significa que o recurso Fazer varredura está funcionando adequadamente.

Experimente excluir ou colocar em quarentena os arquivos detectados para saber como o recurso Fazer varredura lida com possíveis ameaças. Consulte *Compreensão das detecções de ameaças* na página 69 para obter detalhes.

Utilização do ActiveShield

Quando o ActiveShield é iniciado (carregado na memória do computador) e ativado, ele passa a proteger constantemente o seu computador. O ActiveShield faz varredura dos arquivos quando estes são acessados por você ou pelo computador. Quando detecta um arquivo, o ActiveShield tenta limpá-lo automaticamente. Se o ActiveShield não puder limpar o vírus, coloque o arquivo em quarentena ou exclua-o.

Ativação ou desativação do ActiveShield

Por padrão, o ActiveShield é iniciado (carregado na memória do computador) e ativado (representado por um ícone vermelho na área de notificação do Windows) assim que você reinicia o computador após o processo de instalação.

Se o ActiveShield for interrompido (não carregado) ou desativado (indicado pelo ícone preto), você poderá executá-lo manualmente e configurá-lo para iniciar automaticamente com o Windows.

Ativação do ActiveShield

Para ativar o ActiveShield somente nesta sessão do Windows:

Clique com o botão direito do mouse no ícone da McAfee, aponte para **VirusScan** e clique em **Ativar**. O ícone da McAfee muda para vermelho  .

Se o ActiveShield ainda estiver configurado para ser iniciado junto com o Windows, uma mensagem informará que você está protegido contra ameaças. Caso contrário, será exibida uma caixa de diálogo em que você poderá configurar o ActiveShield para ser iniciado com o Windows (Figura 3-1 na página 50).

Desativação do ActiveShield

Para desativar o ActiveShield somente para a sessão atual do Windows:

1. Clique com o botão direito do mouse no ícone da McAfee, aponte para **VirusScan** e clique em **Desativar**.
2. Clique em **Sim** para confirmar.

   A cor do ícone da McAfee muda para preto  .

Se o ActiveShield ainda estiver configurado para iniciar com o Windows, o computador estará protegido contra ameaças novamente quando for reiniciado.

Configuração das opções do ActiveShield

É possível modificar as opções de execução e varredura do ActiveShield na guia **ActiveShield** da caixa de diálogo **Opções do VirusScan** (Figura 3-1), acessível por meio do ícone da McAfee na área de notificação do Windows.

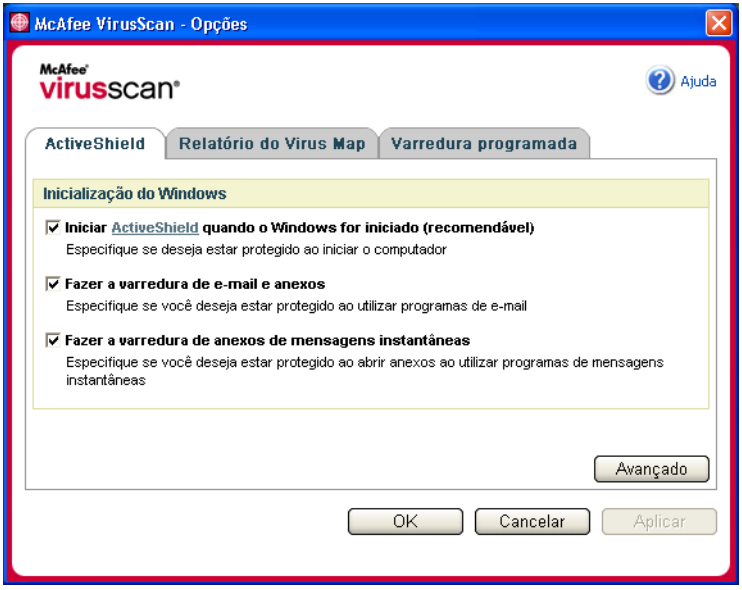


Figura 3-1. Opções do ActiveShield

Execução do ActiveShield

Por padrão, o ActiveShield é iniciado (carregado na memória do computador) e ativado (representado por um vermelho) assim que você reinicia o computador, após o processo de instalação.

Se o ActiveShield for interrompido (representado por um preto), você poderá configurá-lo para que seja iniciado automaticamente junto com o Windows (recomendável).

NOTA

Durante as atualizações do VirusScan, o **Assistente de atualização** pode interromper o ActiveShield temporariamente para instalar arquivos novos. Quando o **Assistente de atualização** solicitar que você clique em **Concluir**, o ActiveShield será iniciado novamente.

Para iniciar o ActiveShield automaticamente quando o Windows for iniciado:

1 Clique com o botão direito do mouse no ícone da McAfee, aponte para **VirusScan** e clique em **Opções**.

A caixa de diálogo **Opções do VirusScan** será aberta (Figura 3-1 na página 50).

2 Marque a caixa de seleção **Iniciar o ActiveShield ao iniciar o Windows (recomendável)** e clique em **Aplicar** para salvar as alterações.

3 Clique em **OK** para confirmar e, em seguida, clique em **OK**.

Interrupção do ActiveShield

AVISO
Se você interromper o ActiveShield, o seu computador não estará protegido contra ameaças. Se for necessário interromper o ActiveShield para outros fins que não seja a atualização do VirusScan, certifique-se de não estar conectado à Internet.

Para não executar o ActiveShield quando o Windows for iniciado:

1 Clique com o botão direito do mouse no ícone da McAfee, aponte para **VirusScan** e clique em **Opções**.

A caixa de diálogo **Opções do VirusScan** será aberta (Figura 3-1 na página 50).

2 Desmarque a caixa de seleção **Iniciar o ActiveShield ao iniciar o Windows (recomendável)** e clique em **Aplicar** para salvar as alterações.

3 Clique em **OK** para confirmar e, em seguida, clique em **OK**.

Varredura de e-mails e anexos

Por padrão, a varredura e a limpeza automática de e-mails são ativadas com a opção **Fazer a varredura de e-mail e anexos** (Figura 3-1 na página 50).

Quando essa opção está ativada, o ActiveShield faz varredura automaticamente e tenta limpar as mensagens e os anexos de e-mail detectados enviados (SMTP) e recebidos (POP3) pelos clientes de e-mail mais populares:

- Microsoft Outlook Express 4.0 ou posterior
- Microsoft Outlook 97 ou posterior
- Netscape Messenger 4.0 ou posterior
- Netscape Mail 6.0 ou posterior

- Eudora Light 3.0 ou posterior
- Eudora Pro 4.0 ou posterior
- Eudora 5.0 ou posterior
- Pegasus 4.0 ou posterior

NOTA
Não há suporte à varredura de e-mails nos seguintes clientes de e-mail: clientes baseados na Web, IMAP, AOL, POP3 SSL e Lotus Notes. No entanto, o ActiveShield faz varredura de anexos de e-mail quando estes são abertos.

Quando a opção **Fazer a varredura de e-mail e anexos** é desativada, as opções de varredura de e-mails e do WormStopper (Figura 3-2 na página 53) são desativadas automaticamente. Quando a varredura de e-mails enviados é desativada, as opções do WormStopper são desativadas automaticamente.

Se você alterar as opções de varredura de e-mails, reinicie o programa de e-mail para concluir essas alterações.

E-mails recebidos

Quando uma mensagem ou um anexo de e-mail recebido é detectado, o ActiveShield executa as seguintes etapas:

- Tenta limpar o e-mail detectado
- Tenta colocar em quarentena ou excluir o e-mail que não pode ser limpo
- Inclui um arquivo de alerta no e-mail recebido, contendo informações sobre as ações a serem executadas para remover a possível ameaça

E-mails enviados

Quando uma mensagem ou um anexo de e-mail enviado é detectado, o ActiveShield executa as seguintes etapas:

- Tenta limpar o e-mail detectado
- Tenta colocar em quarentena ou excluir o e-mail que não pode ser limpo

NOTA
Para obter detalhes sobre os erros da varredura de e-mails enviados, consulte a ajuda on-line.

Desativação da varredura de e-mails

Por padrão, o ActiveShield faz varredura de e-mails recebidos e enviados. Porém, para melhor controle, é possível configurar o ActiveShield para fazer a varredura somente de e-mails recebidos ou enviados.

Para desativar a varredura de e-mails recebidos ou enviados:

1. Clique com o botão direito do mouse no ícone da McAfee, aponte para **VirusScan** e clique em **Opções**.
2. Clique em **Avançado** e, em seguida, clique na guia **Varredura de e-mail** (Figura 3-2).
3. Desmarque **Mensagens de e-mail recebidas** ou **Mensagens de e-mail enviadas** e clique em **OK**.

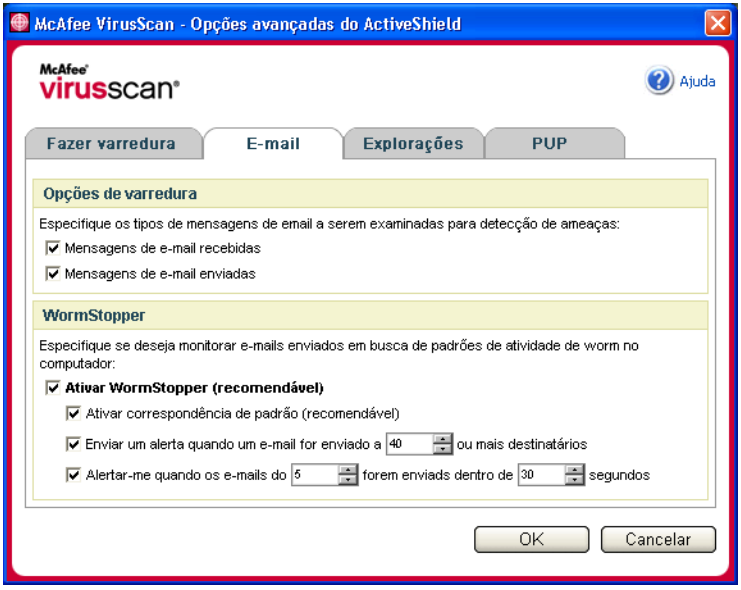


Figura 3-2. Opções avançadas do ActiveShield - guia E-mail

Varredura de worms

O VirusScan monitora o computador verificando atividades suspeitas que podem indicar a presença de ameaças no computador. Enquanto o VirusScan limpa vírus e outras ameaças, o WormStopper™ evita que vírus e worms se espalhem ainda mais.

Um "worm" de computador é um vírus que se replica automaticamente e que reside na memória, podendo enviar cópias de si mesmo por e-mail. Sem o WormStopper, os worms são percebidos apenas quando sua replicação descontrolada consome recursos do sistema, diminuindo o desempenho ou interrompendo tarefas.

O mecanismo de proteção do WormStopper detecta, alerta e bloqueia atividades suspeitas. As atividades suspeitas podem executar as seguintes ações no computador:

- Tentativas de encaminhar e-mails a muitos contatos da lista de endereços
- Tentativas de encaminhar várias mensagens de e-mail em uma seqüência rápida

Quando o ActiveShield está configurado para usar a opção padrão **Ativar WormStopper (recomendável)** da caixa de diálogo **Opções avançadas**, o WormStopper monitora a atividade de e-mail em busca de padrões de atividades suspeitas e envia um alerta caso um número especificado de e-mails ou destinatários seja excedido em um determinado intervalo de tempo.

Para configurar o ActiveShield para fazer varredura de mensagens de e-mail enviadas quanto a atividades semelhantes às de worms:

1. Clique com o botão direito do mouse no ícone da McAfee, aponte para **VirusScan** e clique em **Opções**.
2. Clique em **Avançado** e, em seguida, clique na guia **E-mail**.
3. Clique em **Ativar WormStopper (recomendável)** (Figura 3-3).

   Por padrão, as seguintes opções detalhadas estão ativadas:

   - Correspondência de padrões para detectar atividades suspeitas
   - Envio de alertas quando um e-mail é enviado a 40 ou mais destinatários
   - Envio de alertas quando 5 ou mais e-mails são enviados em 30 segundos

   NOTA
   Se você alterar o número de destinatários ou de segundos para a monitoração de e-mails enviados, poderão ocorrer detecções inválidas. A McAfee recomenda clicar em **Não** para manter as configurações padrão. Se preferir, clique em **Sim** para alterar as configurações padrão.

Essa opção pode ser ativada automaticamente após a detecção de um possível worm pela primeira vez (consulte detalhes em *Gerenciamento de possíveis worms* na página 61):

- Bloqueio automático de e-mails suspeitos enviados

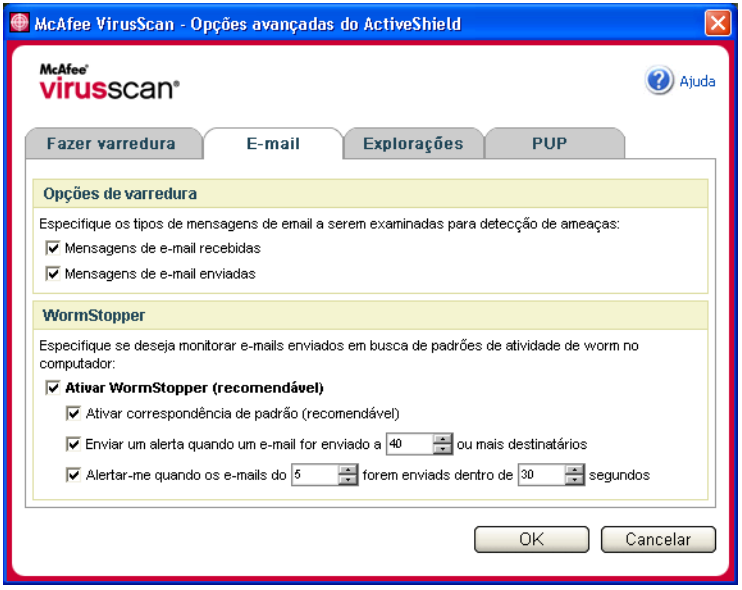


Figura 3-3. Opções avançadas do ActiveShield - guia E-mail

Varredura de anexos de mensagens instantâneas recebidas

Por padrão, a varredura de anexos de mensagens instantâneas é ativada com a opção **Fazer a varredura de anexos de mensagens instantâneas** (Figura 3-1 na página 50).

Quando essa opção está ativada, o VirusScan faz varredura automaticamente e tenta limpar os anexos detectados de mensagens instantâneas recebidas dos programas de mensagens instantâneas mais populares, incluindo os seguintes:

- MSN Messenger 6.0 ou superior
- Yahoo Messenger 4.1 ou superior
- AOL Instant Messenger 2.1 ou superior

NOTA

Para sua proteção, não é possível desativar a limpeza automática dos anexos de mensagens instantâneas.

Quando um anexo de mensagem instantânea recebida é detectado, o VirusScan executa as seguintes etapas:

- Tenta limpar a mensagem detectada
- Pergunta se deve colocar em quarentena ou excluir a mensagem que não pode ser limpa

Varredura de todos os arquivos

Quando o ActiveShield é configurado para usar a opção padrão **Todos os arquivos (recomendável)**, ele faz varredura de todos os tipos de arquivos existentes no computador à medida que este tenta utilizá-los. Utilize essa opção para obter a varredura mais completa possível.

Para configurar o ActiveShield para fazer varredura de todos os tipos de arquivos:

1. Clique com o botão direito do mouse no ícone da McAfee, aponte para **VirusScan** e clique em **Opções**.
2. Clique em **Avançado** e, em seguida, clique na guia **Fazer varredura** (Figura 3-4 na página 56).
3. Clique em **Todos os arquivos (recomendável)** e, em seguida, clique em **OK**.

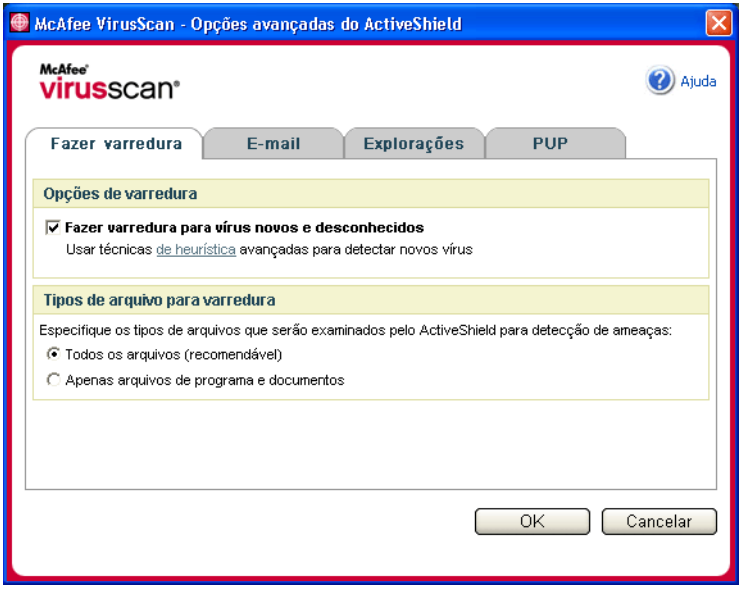


Figura 3-4. Opções avançadas do ActiveShield - guia Fazer varredura

Varredura somente de arquivos de programa e documentos

Quando o ActiveShield é configurado para usar a opção **Apenas arquivos de programas e documentos**, ele faz varredura somente de documentos e arquivos de programas. O arquivo de assinatura de vírus mais recente (arquivo DAT) determina os tipos de arquivos a serem examinados pelo ActiveShield. Para configurar o ActiveShield para fazer varredura apenas de arquivos de programas e documentos:

1. Clique com o botão direito do mouse no ícone da McAfee, aponte para **VirusScan** e clique em **Opções**.
2. Clique em **Avançado** e, em seguida, clique na guia **Fazer varredura** (Figura 3-4).
3. Clique em **Apenas arquivos de programa e documentos** e, em seguida, clique em **OK**.

Varredura de vírus novos e desconhecidos

Quando você configura o ActiveShield para utilizar a opção padrão **Fazer varredura para vírus novos e desconhecidos (recomendável)**, ele utiliza técnicas avançadas de heurística que tentam fazer uma correspondência entre os arquivos e as assinaturas dos vírus conhecidos, ao mesmo tempo que procura indícios de vírus desconhecidos nos arquivos.

Para configurar o ActiveShield para fazer varredura de vírus novos e desconhecidos:

1. Clique com o botão direito do mouse no ícone da McAfee, aponte para **VirusScan** e clique em **Opções**.
2. Clique em **Avançado** e, em seguida, clique na guia **Fazer varredura** (Figura 3-4).
3. Clique em **Fazer varredura para vírus novos e desconhecidos (recomendável)** e, em seguida, clique em **OK**.

Varredura de scripts

O VirusScan monitora o computador verificando atividades suspeitas que podem indicar a presença de ameaças no computador. Enquanto o VirusScan limpa vírus e outras ameaças, o ScriptStopper™ evita que cavalos de Tróia executem scripts que disseminem ainda mais os vírus.

Um "cavalo de Tróia" é um programa suspeito que se faz passar por um aplicativo benigno. Os cavalos de Tróia não são vírus porque não se replicam, mas podem ser tão destruidores quanto os vírus.

O mecanismo de proteção do ScriptStopper detecta, alerta e bloqueia atividades suspeitas. As atividades suspeitas podem incluir as seguintes ações no computador:

- Execução de um scripts que resulte na criação, cópia ou exclusão de arquivos, ou na abertura do Registro do Windows

Quando o ActiveShield está configurado para usar a opção padrão **Ativar ScriptStopper (recomendável)** da caixa de diálogo **Opções avançadas**, o ScriptStopper monitora a execução de scripts em busca de padrões de atividades suspeitas e envia um alerta caso um número especificado de e-mails ou destinatários seja excedido em um determinado intervalo de tempo.

Para configurar o ActiveShield para fazer varredura de scripts em execução em busca de atividades semelhantes às de worms:

1. Clique com o botão direito do mouse no ícone da McAfee, aponte para **VirusScan** e clique em **Opções**.
2. Clique em **Avançado** e, em seguida, clique na guia **Explorações** (Figura 3-5).
3. Clique em **Ativar ScriptStopper (recomendável)** e, em seguida, clique em **OK**.

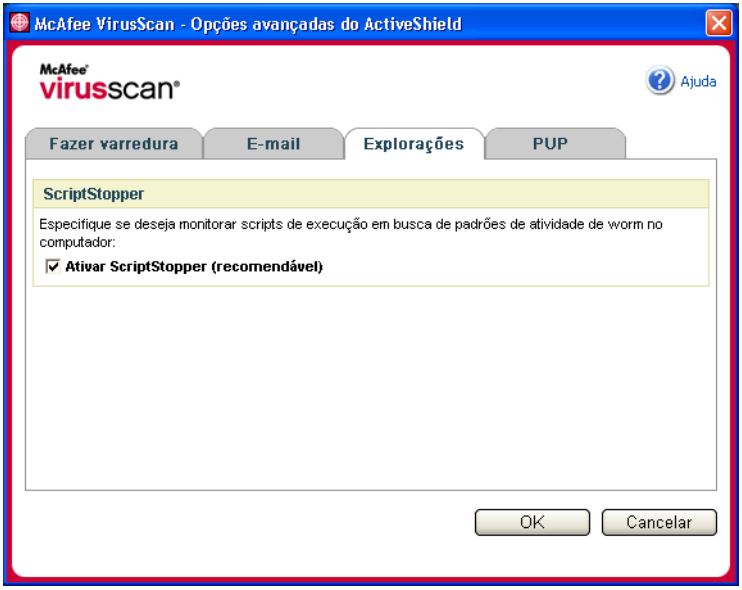


Figura 3-5. Opções avançadas do ActiveShield - guia Explorações

Varredura de programas potencialmente indesejados (PUPs)

NOTA
Após ser instalado no computador, o McAfee AntiSpyware gerencia todas as atividades de programas potencialmente indesejados (PUPs). Abra o McAfee AntiSpyware para configurar as opções.

Quando você configura o ActiveShield para utilizar a opção padrão **Fazer a varredura de programas potencialmente indesejados (recomendável)** na caixa de diálogo **Opções Avançadas**, a proteção contra programas potencialmente indesejados (PUPs) detecta, bloqueia e remove rapidamente spyware, adware e outros programas que coletam e transmitem os seus dados privados sem a sua permissão.

Para configurar o ActiveShield para fazer varredura de PUPs:

1. Clique com o botão direito do mouse no ícone da McAfee, aponte para **VirusScan** e clique em **Opções**.
2. Clique em **Avançado** e, em seguida, clique na guia **PUP** (Figura 3-6).
3. Clique em **Fazer a varredura de programas potencialmente indesejados (recomendável)** e, em seguida, clique em **OK**.

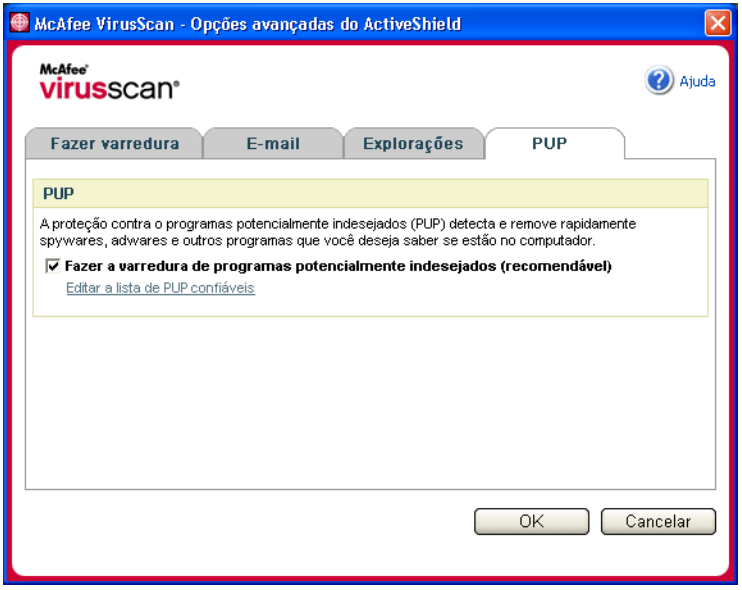


Figura 3-6. Opções avançadas do ActiveShield - guia PUP

Compreensão dos alertas de segurança

Quando o ActiveShield encontra um vírus, é exibido um alerta semelhante a Figura 3-7. Com a maioria dos vírus, cavalos de Tróia e worms, o ActiveShield tenta limpar automaticamente o arquivo e envia um alerta a você. Com programas potencialmente indesejados (PUPs), o ActiveShield detecta o arquivo, bloqueia-o automaticamente e envia um alerta a você.

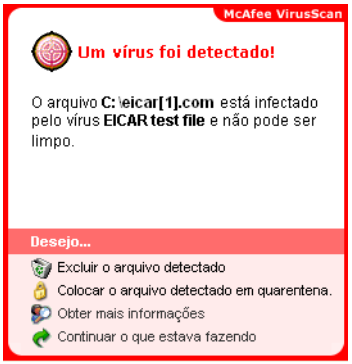


Figura 3-7. Alerta de vírus

Você pode escolher como gerenciar arquivos detectados, e-mails detectados, scripts suspeitos, worms potenciais ou PUPs, bem como se deseja enviar os arquivos detectados para os laboratórios AVERT da McAfee para que sejam pesquisados.

Para maior proteção, sempre que o ActiveShield detecta um arquivo suspeito, é solicitada a realização imediata de uma varredura em todo o computador. A menos que escolha ocultar o aviso da varredura, você receberá lembretes periódicos até executá-la.

Gerenciamento de arquivos detectados

1 Se o ActiveShield puder limpar o arquivo, você poderá obter mais informações ou ignorar o alerta:

- Clique em **Obter mais informações** para exibir o nome, local e nome de vírus associado ao arquivo detectado.
- Clique em **Continuar o que eu estava fazendo** para ignorar o alerta e fechá-lo.

2 Se o ActiveShield não puder limpar o arquivo, clique em **Colocar o arquivo detectado em quarentena** para criptografar e isolar temporariamente os arquivos suspeitos no diretório de quarentena até que uma ação apropriada possa ser executada.

   Uma mensagem de confirmação é exibida, solicitando que seja verificada a existência de ameaças no computador. Clique em **Fazer varredura** para concluir o processo de quarentena.

3 Se o ActiveShield não puder colocar o arquivo em quarentena, clique em **Excluir o arquivo detectado** para tentar remover o arquivo.

Gerenciamento de e-mails detectados

Por padrão, a varredura de e-mails tenta limpar automaticamente o e-mail detectado. Um arquivo de alerta incluído na mensagem recebida informa se o e-mail foi limpo, colocado em quarentena ou excluído.

Gerenciamento de scripts suspeitos

Quando o ActiveShield detecta um script suspeito, você pode obter mais informações e interromper o script, caso não tenha pretendido iniciá-lo:

- Clique em **Obter mais informações** para exibir o nome, o local e a descrição da atividade associada ao script suspeito.
- Clique em **Interromper este script** para impedir a execução do script suspeito.

Se tiver certeza de que o script é confiável, você pode permitir que ele seja executado:

- Clique em **Permitir este script desta vez** para permitir que todos os scripts contidos em um único arquivo sejam executados uma vez.
- Clique em **Continuar o que eu estava fazendo** para ignorar o alerta e deixar o script ser executado.

Gerenciamento de possíveis worms

Quando o ActiveShield detecta um possível worm, você pode obter mais informações e interromper a atividade de e-mail, caso não tenha pretendido iniciá-la:

- Clique em **Obter mais informações** para exibir a lista de destinatários, a linha de assunto, o corpo da mensagem e uma descrição da atividade suspeita associada à mensagem de e-mail detectada.
- Clique em **Interromper este e-mail** para impedir o envio do e-mail suspeito e excluí-lo da fila de mensagens.

Se tiver certeza de que o e-mail é confiável, clique em **Continuar o que eu estava fazendo** para ignorar o alerta e permitir o envio do e-mail.

Gerenciamento de PUPs

Se o ActiveShield detectar e bloquear um programa potencialmente indesejado (PUP), você poderá obter mais informações e remover o programa, caso não pretenda instalá-lo:

- Clique em **Obter mais informações** para exibir o nome, o local e a ação recomendada associada ao PUP.
- Clique em **Remover este PUP** para remover o programa, caso não pretenda instalá-lo.

  Uma mensagem de confirmação é exibida.

  - Se (a) você não reconhecer o PUP ou (b) não tiver instalado o PUP como parte de um pacote ou aceitado um contrato de licença associado a esses programas, clique em **OK** para remover o programa usando o método da McAfee.

  - Caso contrário, clique em **Cancelar** para sair do processo de remoção automática. Caso mude de idéia posteriormente, você poderá remover o programa manualmente, usando o programa de desinstalação do fornecedor.
- Clique em **Continuar o que eu estava fazendo** para ignorar o alerta e bloquear o programa desta vez.

Se você (a) reconhecer o PUP ou (b) tiver instalado o PUP como parte de um pacote ou aceitado um contrato de licença associado a esses programas, poderá permitir sua execução:

- Clique em **Confiar neste PUP** para incluir o programa na lista branca e sempre permitir sua execução no futuro.

  Consulte "*Gerenciamento de PUPs confiáveis*" para obter detalhes.

Gerenciamento de PUPs confiáveis

Os programas adicionados à lista **PUPs confiáveis** não são detectados pelo McAfee VirusScan.

Se um PUP for detectado e adicionado à lista **PUPs confiáveis**, ele poderá ser removido posteriormente, se necessário.

Se a lista **PUPs confiáveis** estiver cheia, será necessário remover alguns de seus itens para poder confiar em outro PUP.

Para remover um programa da lista **PUPs confiáveis**:

1. Clique com o botão direito do mouse no ícone da McAfee, aponte para **VirusScan** e clique em **Opções**.
2. Clique em **Avançado** e, em seguida, clique na guia **PUP**.

3 Clique em **Editar a lista de PUPs confiáveis**, marque a caixa de seleção ao lado do nome do arquivo e clique em **Remover**. Clique em **OK** quando terminar de remover os itens.

Varredura manual do computador

O recurso Fazer varredura permite procurar seletivamente vírus e outras ameaças em unidades de disco rígido, disquetes e arquivos e pastas individuais. Ao encontrar um arquivo suspeito, ele tenta limpá-lo automaticamente, a não ser que seja um programa potencialmente indesejado. Se o recurso Fazer varredura não conseguir limpar o arquivo, você poderá colocar o arquivo em quarentena ou excluí-lo.

Varredura manual de vírus e outras ameaças

Para fazer varredura do computador:

1 Clique com o botão direito do mouse no ícone da McAfee, aponte para **VirusScan** e clique em **Fazer varredura**.

A caixa de diálogo **Fazer varredura** será aberta (Figura 3-8).

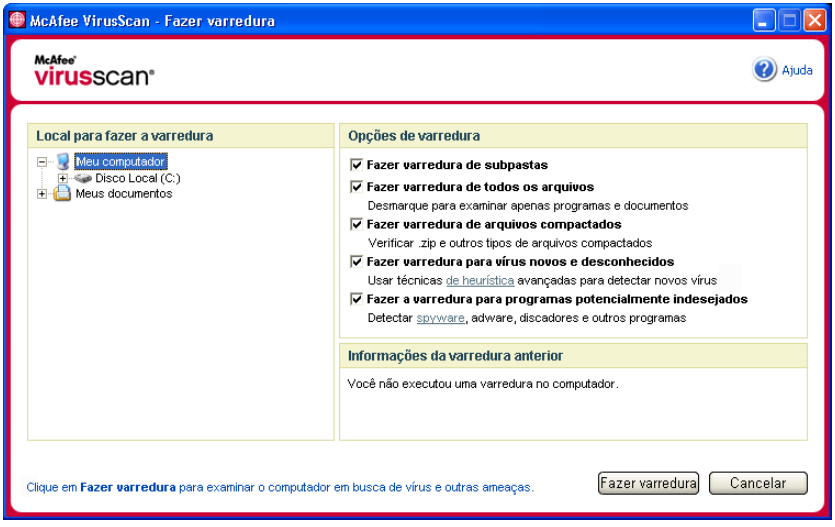


Figura 3-8. Caixa de diálogo Fazer varredura

2 Clique na unidade, pasta ou arquivo em que será feita a varredura.

3 Selecione **Opções de varredura**. Por padrão, todas as **Opções de varredura** são previamente selecionadas para fornecer a varredura mais completa possível (Figura 3-8):

- **Fazer varredura de subpastas** — Use essa opção para fazer varredura de arquivos contidos nas suas subpastas. Desmarque essa caixa de seleção para permitir a verificação somente dos arquivos que podem ser vistos quando uma pasta ou unidade é aberta.

  Exemplo: Os arquivos da Figura 3-9 serão os únicos examinados se você desmarcar a caixa **Fazer varredura de subpastas**. As pastas e seu conteúdo não serão examinados. Para fazer varredura das pastas e de seu conteúdo, é necessário deixar essa caixa de seleção marcada.

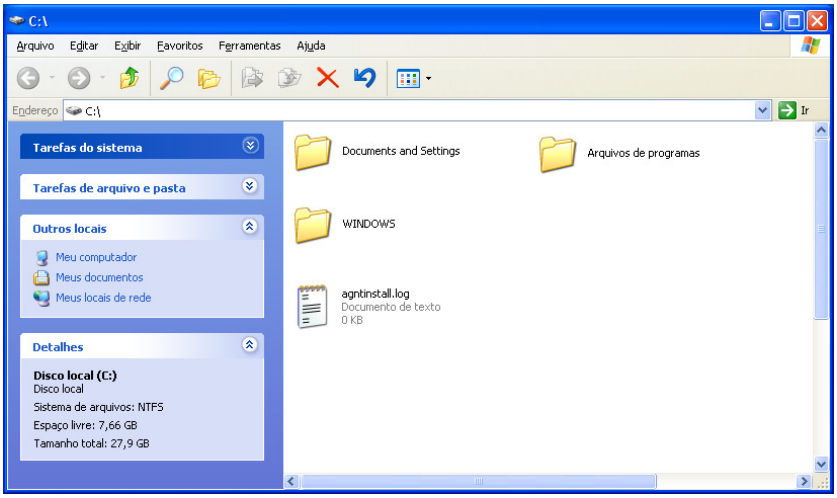


Figura 3-9. Conteúdo do disco local

- **Fazer varredura de todos os arquivos** — Use essa opção para permitir a varredura completa de todos os tipos de arquivo. Desmarque essa caixa de seleção para diminuir o tempo da varredura e permitir a verificação apenas de documentos e arquivos de programas.

- **Fazer varredura de arquivos compactados** — Use essa opção para revelar arquivos ocultos dentro de arquivos .ZIP e outros arquivos compactados. Desmarque essa caixa de seleção para evitar a varredura de arquivos ou arquivos compactados que se encontram em outros arquivos compactados.

Às vezes, os autores inserem vírus em um arquivo .ZIP e, em seguida, inserem esse arquivo .ZIP dentro de um outro arquivo .ZIP, visando burlar os mecanismos antivírus. O recurso Fazer varredura pode detectar esses vírus desde que essa opção esteja selecionada.

- **Fazer varredura para vírus novos e desconhecidos** — Utilize essa opção para encontrar os vírus mais recentes, para os quais podem não existir "vacinas". Essa opção usa técnicas heurísticas avançadas que tentam fazer a correspondência dos arquivos com as assinaturas de vírus conhecidos e, ao mesmo tempo, procura indícios de vírus não identificados nos arquivos.

  Esse método de varredura também examina o arquivo em busca de características que geralmente indicam que ele contém vírus. Isso minimiza a possibilidade de a varredura fornecer indicações falsas. Porém, se uma varredura heurística detectar um vírus, trate-o com o mesmo cuidado destinado a arquivos que você sabe que contêm vírus.

  Essa opção proporciona a varredura mais completa, mas geralmente é mais lenta do que a varredura normal.

- **Fazer varredura para programas potencialmente indesejados** — Utilize essa opção para detectar spyware, adware e outros programas que coletam e transmitem os seus dados privados sem a sua permissão.

  NOTA
  Mantenha todas as opções padrão selecionadas para obter a varredura mais completa possível. Esse procedimento fará a varredura de todos os arquivos da unidade ou da pasta selecionada. Portanto, reserve tempo suficiente para que a varredura seja concluída. Quanto maior a unidade de disco rígido e o número de arquivos existentes, mais demorada será a varredura.

4 Clique em **Fazer varredura** para iniciar a varredura de arquivos.

Quando a varredura for concluída, um resumo informará o número de arquivos examinados e de arquivos detectados, além do número de programas potencialmente indesejados e arquivos detectados que foram limpos automaticamente.

5 Clique em **OK** para fechar o resumo e exibir a lista de todos os arquivos detectados na caixa de diálogo **Fazer varredura** (Figura 3-10).

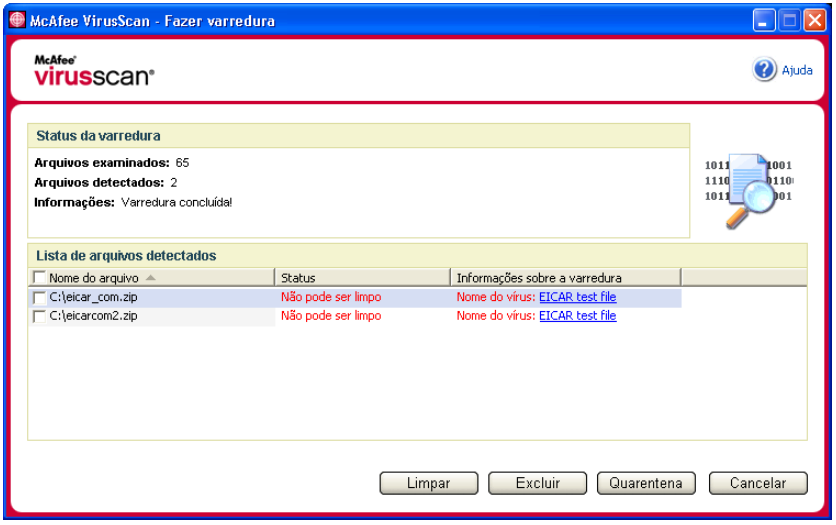


Figura 3-10. Resultados da varredura

NOTA
O recurso Fazer varredura considera um arquivo compactado (.ZIP, .CAB, etc.) como um único arquivo na contagem de **Arquivos examinados**. Além disso, o número de arquivos examinados pode variar se você tiver excluído os arquivos temporários da Internet após a última varredura.

6 Se a varredura não encontrar vírus ou outras ameaças, clique em **Voltar** para selecionar outra pasta ou unidade para a varredura, ou clique em **Fechar** para fechar a caixa de diálogo. Caso contrário, consulte *Compreensão das detecções de ameaças* na página 69.

Varredura pelo Windows Explorer

O VirusScan fornece um menu de atalho que permite fazer varredura de arquivos, pastas ou unidades selecionadas a partir do Windows Explorer, em busca de vírus e outras ameaças.

Para fazer a varredura de arquivos no Windows Explorer:

1 Abra o Windows Explorer.

2 Clique com o botão direito do mouse na unidade, na pasta ou no arquivo em que a varredura será feita e clique em **Fazer varredura**.

A caixa de diálogo **Fazer varredura** será aberta e iniciará a varredura dos arquivos. Todas as **Opções de varredura** padrão são previamente selecionadas para oferecer a varredura mais completa possível (Figura 3-8 na página 63).

Varredura pelo Microsoft Outlook

O VirusScan fornece um ícone de barra de ferramentas para o Microsoft Outlook 97 ou posterior que permite verificar a existência de vírus e outras ameaças nos locais selecionados de armazenamento de mensagens e respectivas subpastas, pastas de caixa de correio ou mensagens de e-mail com anexos.

Para fazer varredura de e-mails no Microsoft Outlook:

1 Abra o Microsoft Outlook.

2 Clique no local de armazenamento de mensagens, pasta ou mensagem de e-mail que contém o anexo a ser examinado e clique no ícone de varredura de e-mails  da barra de ferramentas.

O mecanismo de varredura de e-mails é aberto e inicia a varredura dos arquivos. Todas as **Opções de varredura** padrão são previamente selecionadas para oferecer a varredura mais completa possível (Figura 3-8 na página 63).

Varredura automática de vírus e outras ameaças

Embora o VirusScan faça varredura dos arquivos quando eles são acessados por você ou por seu computador, você pode programar a varredura automática no Agendador do Windows para fazer a varredura completa de vírus e outras ameaças no computador em intervalos específicos.

Para programar uma varredura:

1 Clique com o botão direito do mouse no ícone da McAfee, aponte para **VirusScan** e clique em **Opções**.

A caixa de diálogo **Opções do VirusScan** será aberta.

2 Clique na guia **Varredura programada** (Figura 3-11 na página 68).

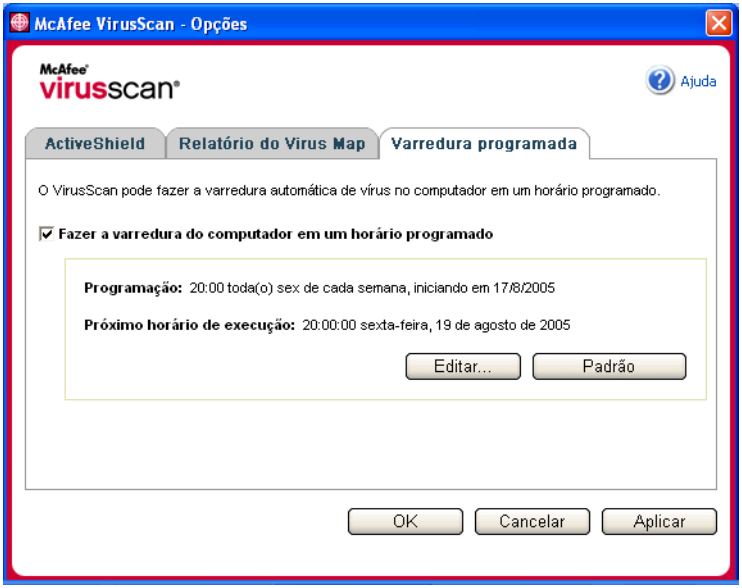


Figura 3-11. Opções de Varredura programada

3 Marque a caixa de seleção **Fazer a varredura do computador em um horário programado** para ativar a varredura automática.

4 Especifique uma programação para a varredura automática:

- Para aceitar a programação padrão (toda sexta-feira, às 20h), clique em **OK**.
- Para editar a programação:

  a. Clique em **Editar**.

  b. Selecione a freqüência para fazer a varredura de computador na lista **Programar tarefa** e, em seguida, selecione opções adicionais na área dinâmica abaixo dela:

  Diariamente - Especifique o número de dias entre varreduras.

  Semanalmente (padrão) - Especifique o número de semanas entre varreduras, bem como os dias da semana.

  Mensalmente - Especifique em qual dia do mês será feita a varredura. Clique em **Selecionar meses** para especificar os meses em que a varredura será feita e clique em **OK**.

Uma vez - Especifique em qual data a varredura será feita.

NOTA
Não há suporte para as seguintes opções do Agendador do Windows:
Ao inicializar o sistema, **Quando ocioso** e **Mostrar vários agendamentos**. A última programação com suporte permanecerá ativada até você selecionar uma das opções válidas.

c. Na caixa **Hora de início**, selecione a hora do dia em que a varredura do computador será feita.

d. Para selecionar opções avançadas, clique em **Avançado**.

A caixa de diálogo **Opções avançadas de agendamento** será aberta.

i. Especifique a data inicial, a data final, a duração, a hora final e se deseja interromper a tarefa em um horário específico se a varredura ainda estiver sendo executada.

ii. Clique em **OK** para salvar as alterações e fechar a caixa de diálogo. Caso contrário, clique em **Cancelar**.

5 Clique em **OK** para salvar as alterações e fechar a caixa de diálogo. Caso contrário, clique em **Cancelar**.

6 Para retornar à programação padrão, clique em **Padrão**. Caso contrário, clique em **OK**.

Compreensão das detecções de ameaças

Com a maioria dos vírus, cavalos de Tróia e worms, o recurso de varredura tenta limpar o arquivo automaticamente. Você pode especificar como gerenciar os arquivos detectados, inclusive se deseja enviá-los aos laboratórios AVERT da McAfee para serem pesquisados. Se a varredura detectar um programa potencialmente indesejado, tente limpá-lo manualmente, colocá-lo em quarentena ou excluí-lo (o envio para a AVERT não está disponível).

Para gerenciar um vírus ou programa potencialmente indesejado:

1 Se um arquivo for exibido na **Lista de arquivos detectados**, clique na caixa de seleção ao lado do arquivo para selecioná-lo.

NOTA
Se aparecer mais de um arquivo na lista, você poderá marcar a caixa de seleção ao lado da lista **Nome do arquivo** para executar a mesma ação em todos os arquivos. Também é possível clicar no nome do arquivo na lista **Informações sobre a varredura** para exibir detalhes da Biblioteca de informações sobre vírus.

2 Se o arquivo for um programa potencialmente indesejado, clique em **Limpar** para tentar limpá-lo.

3 Se o recurso Fazer varredura não conseguir limpar o arquivo, clique em **Quarentena** para criptografar e isolar temporariamente os arquivos suspeitos no diretório de quarentena até que uma ação apropriada possa ser realizada. (Consulte *Gerenciamento de arquivos em quarentena* na página 70 para obter detalhes).

4 Se o recurso Fazer varredura não conseguir limpar o arquivo ou colocá-lo em quarentena, execute uma destas ações:

- Clique em **Excluir** para remover o arquivo.
- Clique em **Cancelar** para fechar a caixa de diálogo sem realizar nenhuma ação.

Se o recurso Fazer varredura não conseguir limpar ou excluir o arquivo detectado, consulte a Biblioteca de informações sobre vírus em http://br.mcafee.com/virusInfo/default.asp para obter instruções sobre exclusão manual do arquivo.

Se o arquivo detectado não permitir que você utilize a conexão com a Internet ou o computador em geral, tente utilizar um Disco de resgate para iniciar o computador. Em muitos casos, o Disco de resgate pode iniciar um computador incapacitado por um arquivo detectado. Consulte *Criação de um Disco de resgate* na página 72 para obter detalhes.

Para obter mais ajuda, consulte o Atendimento ao cliente da McAfee em http://www.mcafeeajuda.com/.

Gerenciamento de arquivos em quarentena

O recurso Quarentena criptografa e isola temporariamente arquivos suspeitos no diretório de quarentena até que uma ação apropriada possa ser executada. Após ser limpo, o arquivo em quarentena pode ser restaurado para o local original.

Para gerenciar um arquivo em quarentena:

1 Clique com o botão direito do mouse no ícone da McAfee, aponte para **VirusScan** e clique em **Gerenciar arquivos em quarentena**.

Uma lista de arquivos em quarentena é exibida (Figura 3-12).

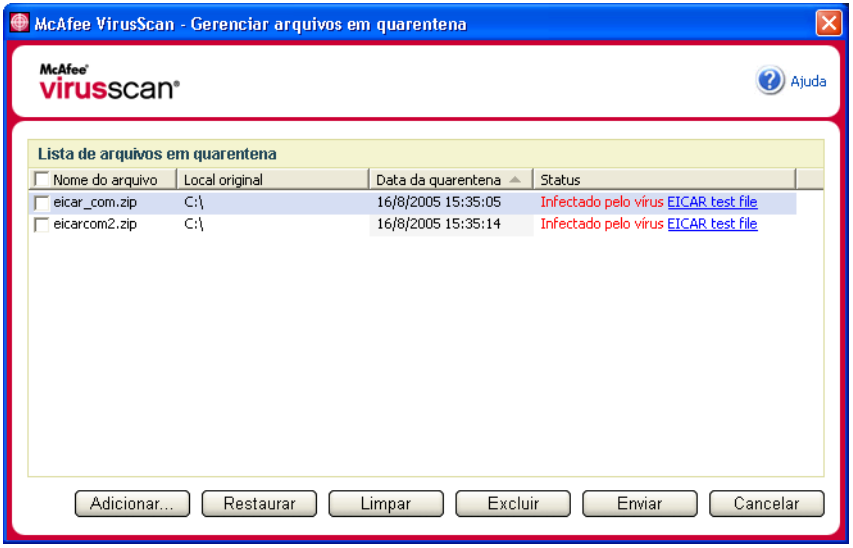


Figura 3-12. Caixa de diálogo Gerenciar arquivos em quarentena

2 Marque as caixas de seleção correspondentes aos arquivos a serem limpos.

> **NOTA**
> Se aparecer mais de um arquivo na lista, você poderá marcar a caixa de seleção ao lado da lista **Nome do arquivo** para executar a mesma ação em todos os arquivos. Você também pode clicar no nome do vírus na lista **Status** para exibir detalhes da Biblioteca de informações sobre vírus.
>
> Uma alternativa é clicar em **Adicionar**, selecionar um arquivo suspeito para adicionar à lista de quarentena, clicar em **Abrir** e, em seguida, selecioná-lo na lista de quarentena.

3 Clique em **Limpar**.

4 Se o arquivo estiver limpo, clique em **Restaurar** para devolvê-lo para o local original.

5 Se o VirusScan não conseguir limpar o vírus, clique em **Excluir** para remover o arquivo.

6 Se o VirusScan não conseguir limpar ou excluir o arquivo e se o arquivo não for um programa potencialmente indesejado, você poderá enviá-lo à McAfee AntiVirus Emergency Response Team (AVERT™) para que seja pesquisado:

   a Atualize os arquivos de assinatura de vírus, caso tenham sido recebidos há mais de duas semanas.

   b Verifique a sua assinatura.

   c Selecione o arquivo e clique em **Enviar** para enviar o arquivo à AVERT.

      O VirusScan envia o arquivo em quarentena como um anexo de mensagem de e-mail contendo o seu endereço de e-mail, país, versão de software, sistema operacional, nome do arquivo e local original do mesmo. O tamanho máximo para envio é um único arquivo de 1,5 MB por dia.

7 Clique em **Cancelar** para fechar a caixa de diálogo sem realizar nenhuma ação.

Criação de um Disco de resgate

O Disco de resgate é um utilitário que cria um disquete inicializável a ser utilizado para iniciar o computador e fazer varredura de vírus quando um vírus impede a inicialização normal.

> **NOTA**
> É necessário estar conectado à Internet para fazer o download da imagem do Disco de resgate. Além disso, o Disco de resgate está disponível somente para computadores com partições de unidade de disco rígido FAT (FAT 16 e FAT 32). Ele é desnecessário para partições NTFS.

Para criar um Disco de resgate:

1 Em um computador não infectado, insira um disquete não infectado na unidade A. Convém utilizar o recurso Fazer varredura para verificar se o computador e o disquete estão sem vírus. (Consulte *Varredura manual de vírus e outras ameaças* na página 63 para obter detalhes).

2 Clique com o botão direito do mouse no ícone da McAfee, aponte para **VirusScan** e clique em **Criar Disco de resgate**.

A caixa de diálogo **Criar um Disco de resgate** será aberta (Figura 3-13).

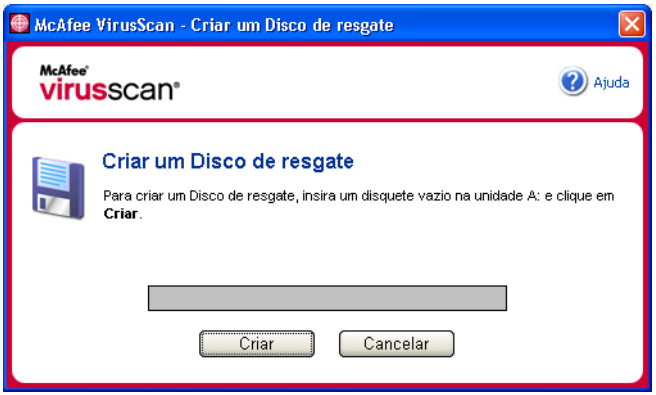


Figura 3-13. Caixa de diálogo Criar um Disco de resgate

3 Clique em **Criar** para criar o Disco de resgate.

Ao criar um Disco de resgate pela primeira vez, uma mensagem informa que é preciso fazer download do arquivo de imagem do Disco de resgate. Clique em **OK** para fazer o download do componente agora ou clique em **Cancelar** para fazê-lo mais tarde.

Uma mensagem de aviso informa que o conteúdo do disquete será perdido.

4 Clique em **Sim** para continuar a criação do Disco de resgate.

O status da criação é exibido na caixa de diálogo **Criar Disco de resgate**.

5 Quando a mensagem "Disco de resgate criado com êxito" for exibida, clique em **OK** e feche a caixa de diálogo **Criar Disco de resgate**.

6 Remova o Disco de resgate da unidade, proteja-o contra gravação e armazene-o em um local seguro.

Proteção de um Disco de resgate contra gravação

Para proteger um Disco de resgate contra gravação:

1 Coloque o disquete com o lado do rótulo para baixo (o círculo de metal deve estar visível).

2 Localize a lingüeta de proteção contra gravação. Deslize a lingüeta para que o orifício fique visível.

Utilização de um Disco de resgate

Para usar um Disco de resgate:

1. Desligue o computador infectado.
2. Insira o Disco de resgate na unidade.
3. Ligue o computador.

   Uma janela cinza com várias opções é exibida.
4. Escolha a opção que melhor atende às suas necessidades pressionando as teclas de função (por exemplo, F2, F3).

   NOTA
   Se você não pressionar nenhuma tecla, o Disco de resgate será inicializado automaticamente em 60 segundos.

Atualização de um Disco de resgate

O Disco de resgate deve ser atualizado regularmente. Para atualizar o Disco de resgate, siga as mesmas instruções de criação de um novo Disco de resgate.

Relato automático de vírus

Agora é possível enviar, de forma anônima, informações de controle de vírus para serem incluídas no World Virus Map. Ative automaticamente esse recurso seguro e gratuito durante a instalação do VirusScan (na caixa de diálogo **Relatório do Virus Map**) ou a qualquer momento na guia **Relatório do Virus Map** da caixa de diálogo **Opções do VirusScan**.

Relato ao World Virus Map

Para relatar automaticamente informações sobre vírus ao World Virus Map:

1 Clique com o botão direito do mouse no ícone da McAfee, aponte para **VirusScan** e clique em **Opções**.

A caixa de diálogo **Opções do VirusScan** será aberta.

2 Clique na guia **Relatório do Virus Map** (Figura 3-14).

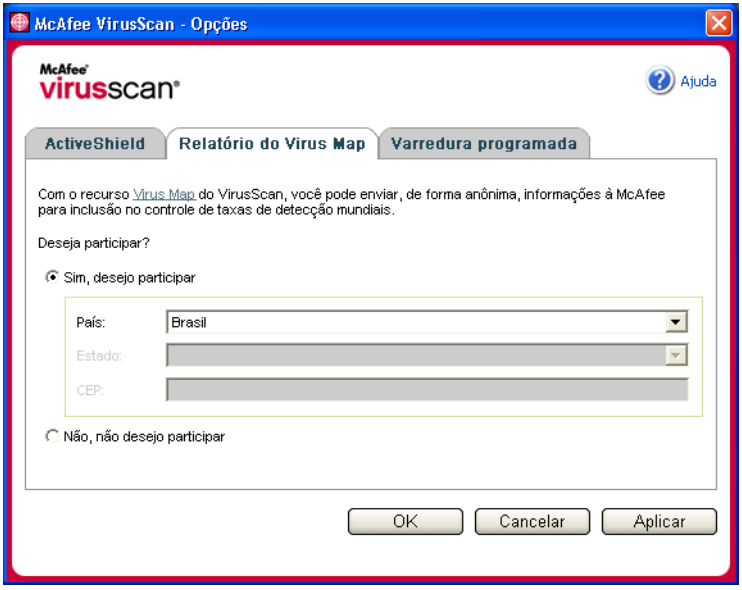


Figura 3-14. Opções de Relatório do Virus Map

3 Aceite a opção padrão **Sim, desejo participar** para enviar anonimamente as informações de vírus para a McAfee, de modo que sejam incluídas no World Virus Map de taxas de detecção mundiais. Caso contrário, selecione **Não, não desejo participar** para impedir o envio de informações.

4 Se estiver nos Estados Unidos, selecione o estado e informe o código de endereçamento postal correspondente ao local onde o seu computador se encontra. Caso contrário, o VirusScan tenta selecionar automaticamente o país em que o seu computador está localizado.

5 Clique em **OK**.

Exibição do World Virus Map

Sendo ou não participante do World Virus Map, você pode visualizar as taxas de detecções mundiais mais recentes através do ícone da McAfee na área de notificação do Windows.

Para exibir o World Virus Map:

- Clique com o botão direito do mouse no ícone da McAfee, aponte para **VirusScan** e, em seguida, clique em **World Virus Map**.

  A página da Web do **World Virus Map** é exibida (Figura 3-15).

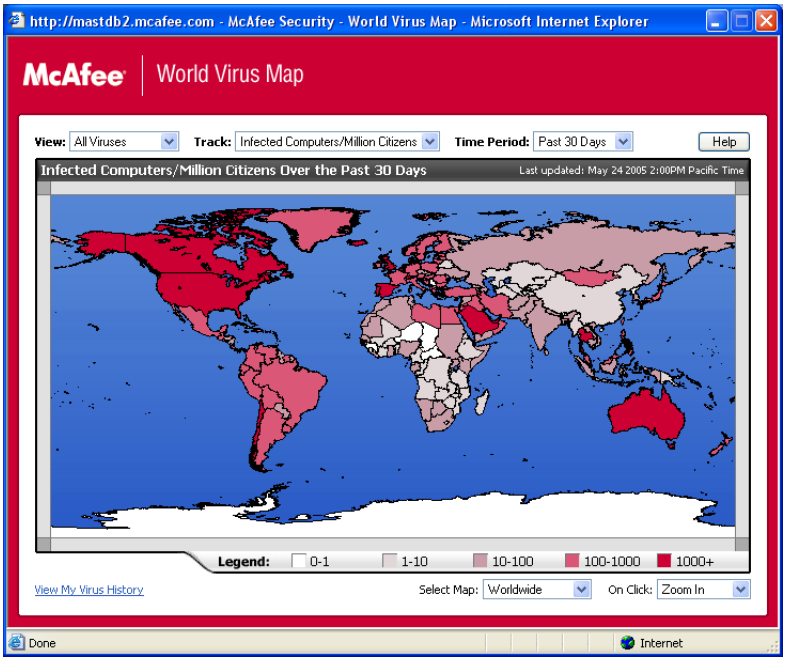


Figura 3-15. World Virus Map

Por padrão, o World Virus Map exibe o número de computadores detectados mundialmente nos últimos 30 dias, além de indicar quando os dados de relatórios foram atualizados pela última vez. É possível alterar o modo de visualização do mapa para exibir o número de arquivos detectados ou alterar o período de tempo, exibindo somente os resultados dos últimos 7 dias ou das últimas 24 horas.

A seção de rastreamento de vírus lista totais acumulados do número de arquivos examinados, arquivos detectados e computadores detectados que foram relatados desde a data exibida.

Atualização do VirusScan

Quando você está conectado à Internet, o VirusScan procura atualizações automaticamente a cada quatro horas. Semanalmente, ele faz download automático das atualizações de definições de vírus, instalando-as sem interromper o seu trabalho.

Os arquivos de definições de vírus possuem aproximadamente 100 KB e, portanto, causam impacto mínimo no desempenho do sistema durante o processo de download.

Se ocorrer uma atualização de produto ou epidemia de vírus, um alerta será exibido. Ao receber o alerta, faça a atualização do VirusScan para remover a ameaça de epidemia de vírus.

Verificação automática de atualizações

O McAfee SecurityCenter é configurado automaticamente para verificar se há atualizações para cada um dos seus serviços McAfee a cada quatro horas quando você está conectado à Internet, notificando-o com alertas e sons. Por padrão, o SecurityCenter faz download e instala automaticamente quaisquer atualizações disponíveis.

NOTA
Em alguns casos, é solicitado o reinício do computador para concluir a atualização. Verifique se salvou todo o seu trabalho e fechou todos os aplicativos antes de reiniciar o computador.

Verificação manual de atualizações

Além de verificar as atualizações automaticamente a cada quatro horas quando se está conectado à Internet, também é possível verificar manualmente as atualizações a qualquer momento.

Para verificar as atualizações do VirusScan manualmente:

1. Verifique se o computador está conectado à Internet.
2. Clique com o botão direito do mouse no ícone McAfee e, em seguida, clique em **Atualizações**.

   A caixa de diálogo **Atualizações do SecurityCenter** será aberta.

3 Clique em **Verificar agora**.

Se houver uma atualização, a caixa de diálogo **Atualizações do VirusScan** será aberta (Figura 3-16 na página 78). Clique em **Atualizar** para continuar.

Se nenhuma atualização estiver disponível, será aberta uma caixa de diálogo informando que o VirusScan está atualizado. Clique em **OK** para fechar a caixa de diálogo.

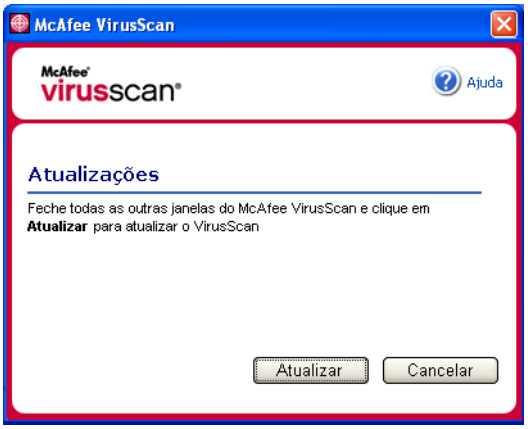


Figura 3-16. Caixa de diálogo Atualizações

4 Se solicitado, efetue logon no site da Web. O **Assistente de atualização** instala automaticamente a atualização.

5 Clique em **Concluir** quando a instalação da atualização estiver concluída.

NOTA
Em alguns casos, é solicitado o reinício do computador para concluir a atualização. Verifique se salvou todo o seu trabalho e fechou todos os aplicativos antes de reiniciar o computador.

McAfee Personal Firewall Plus 4

Bem-vindo ao McAfee Personal Firewall Plus.

O software McAfee Personal Firewall Plus oferece proteção avançada para o seu computador e os seus dados pessoais. O Personal Firewall estabelece uma barreira entre o seu computador e a Internet, monitorando de forma silenciosa o tráfego da Internet em busca de atividades suspeitas.

Ele oferece os seguintes recursos:

- Defesa contra possíveis sondagens e ataques de hackers
- Defesas antivírus adicionais
- Monitoramento da atividade da rede e da Internet
- Alerta sobre eventos potencialmente hostis
- Fornece informações detalhadas sobre tráfego suspeito na Internet
- Integra a funcionalidade Hackerwatch.org, que inclui geração de relatórios de eventos, ferramentas de autoteste e o recurso de envio de eventos relatados por e-mail para outras autoridades on-line
- Fornece recursos de rastreamento detalhado e pesquisa de eventos

Novos recursos

- **Suporte avançado a jogos**
  O McAfee Personal Firewall Plus protege o computador contra tentativas de invasão e atividades suspeitas durante jogos de tela cheia, mas pode ocultar os alertas se detectar tentativas de invasão ou atividades suspeitas. Os alertas vermelhos são exibidos depois que você sai do jogo.

- **Manipulação aprimorada de acesso**
  O McAfee Personal Firewall Plus permite que os usuários concedam, dinamicamente, acesso temporário à Internet para os aplicativos. O acesso é restrito ao tempo decorrido entre a execução e o fechamento do aplicativo. Quando o Personal Firewall detecta um programa desconhecido tentando comunicação com a Internet, um alerta vermelho oferece a opção de conceder ao aplicativo acesso temporário à Internet.

- **Controle de segurança aprimorado**
  A execução do modo Bloqueado do McAfee Personal Firewall Plus permite bloquear instantaneamente todo o tráfego de entrada e saída da Internet entre um determinado computador e a Internet. Os usuários podem ativar e desativar o modo Bloqueado em três locais do Personal Firewall.

- **Opções aprimoradas de recuperação**
  As Opções de redefinição permitem restaurar automaticamente as configurações padrão do Personal Firewall. Se o Personal Firewall exibir um comportamento insatisfatório que não possa ser corrigido, é possível desfazer as configurações atuais e retornar às configurações padrão do produto.

- **Proteção à conectividade com a Internet**
  Para evitar que um usuário desative inadvertidamente sua conexão à Internet, a opção de proibir um endereço da Internet é omitida em um alerta azul quando o Personal Firewall detecta uma conexão à Internet originária de um servidor DHCP ou DNS. Se o tráfego de entrada não for proveniente de um servidor DHCP ou DNS, a opção será exibida.

- **Integração aprimorada ao HackerWatch.org**
  Relatar hackers em potencial é mais fácil do que nunca. O McAfee Personal Firewall Plus aprimora a funcionalidade do HackerWatch.org, que inclui o envio de eventos potencialmente mal-intencionados para o banco de dados.

- **Manipulação estendida inteligente de aplicativos**
  Quando um aplicativo busca acesso à Internet, o Personal Firewall primeiro verifica se reconhece o aplicativo como sendo confiável ou mal-intencionado. Se o aplicativo for reconhecido como confiável, o Personal Firewall permitirá automaticamente o acesso à Internet para que você não precise fazê-lo.

- **Detecção avançada de cavalos de Tróia**
  O McAfee Personal Firewall Plus combina o gerenciamento de conexões de aplicativos com um banco de dados avançado para detectar e impedir que aplicativos potencialmente mal-intencionados, como cavalos de Tróia, acessem a Internet e transmitam os seus dados pessoais.

- **Rastreamento visual aprimorado**
  O rastreamento visual (Visual Trace) inclui mapas gráficos de fácil leitura, que mostram a origem de tráfego e de ataques hostis em todo o mundo, inclusive informações detalhadas sobre contatos/proprietários de endereços IP de origem.

- **Mais fácil de usar**
  O McAfee Personal Firewall Plus inclui um Assistente de configuração e um Tutorial do usuário para conduzir os usuários durante a configuração e o uso do firewall. Embora o produto tenha sido criado para ser usado sem intervenção, a McAfee oferece aos usuários vários recursos para que eles entendam e avaliem o que o firewall tem a oferecer.

- **Detecção aprimorada de invasões**
  O sistema de detecção de invasão (IDS) do Personal Firewall detecta padrões de ataques comuns e outras atividades suspeitas. A detecção de invasões monitora todos os pacotes de dados em busca de transferências de dados ou métodos de transferência suspeitos e os inclui no registro de eventos.

- **Análise avançada de tráfego**
  O McAfee Personal Firewall Plus oferece aos usuários uma exibição dos dados que entram e saem de seus computadores, bem como uma exibição das conexões de aplicativos, inclusive aqueles que estão "escutando" de forma ativa em busca de conexões abertas. Isso permite que os usuários vejam e tomem providências em relação a aplicativos que possam estar abertos a invasões.

Remoção de outros firewalls

Antes de o software do McAfee Personal Firewall Plus ser instalado, é necessário desinstalar todos os demais programas de firewall do computador. Siga as instruções de desinstalação do programa de firewall para executar esse procedimento.

NOTA
Se você usa o Windows XP, não é necessário desativar o recurso incorporado de firewall antes de instalar o McAfee Personal Firewall Plus. Mas, mesmo assim, recomendamos que você o desative. Caso contrário, você não receberá eventos no registro de **Eventos de entrada** do McAfee Personal Firewall Plus.

Definição do firewall padrão

O McAfee Personal Firewall é capaz de gerenciar as permissões e o tráfego dos aplicativos da Internet em seu computador, mesmo que o firewall do Windows esteja sendo executado.

Quando instalado, o McAfee Personal Firewall desativa automaticamente o firewall do Windows e define a si próprio como firewall padrão. Portanto, você dispõe apenas da funcionalidade e das mensagens do McAfee Personal Firewall. Se, depois disso, você ativar o firewall do Windows no Windows Security Center ou no painel de controle do Windows, permitindo que os dois firewalls sejam executados no computador, isso poderá resultar em perda parcial de dados no registro do McAfee Firewall, bem como em mensagens duplicadas de status e de alerta.

NOTA

Se os dois firewalls estiverem ativados, o McAfee Personal Firewall não mostrará todos os endereços IP bloqueados na guia **Eventos de entrada**. O firewall do Windows intercepta e bloqueia a maioria desses eventos, evitando que o McAfee Personal Firewall os detecte ou registre. No entanto, o McAfee Personal Firewall pode bloquear tráfego adicional com base em outros fatores de segurança e esse tráfego será registrado.

Por padrão, o registro é desativado no firewall do Windows. Para manter os dois firewalls ativados, é possível ativar o registro do firewall do Windows. O registro padrão do firewall do Windows é C:\Windows\pfirewall.log

Para assegurar que o computador estará protegido por pelo menos um firewall, o firewall do Windows é reativado automaticamente quando o McAfee Personal Firewall é desinstalado.

Se você desativar o McAfee Personal Firewall ou definir seu nível de segurança como **Aberto** sem ativar manualmente o firewall do Windows, toda a proteção do firewall será removida, com exceção dos aplicativos bloqueados anteriormente.

Definição do nível de segurança

Você pode configurar opções de segurança para indicar como o Personal Firewall reagirá quando detectar tráfego indesejado. Por padrão, o nível de segurança **Padrão** é ativado. No nível de segurança **Padrão**, quando um aplicativo solicita acesso à Internet e você o concede, está fornecendo acesso total ao aplicativo. O acesso total permite que o aplicativo envie e receba dados não solicitados em portas que não sejam do sistema.

Para definir as configurações de segurança:

1. Clique com o botão direito do mouse no ícone da McAfee na área de notificação do Windows, aponte para **Personal Firewall** e, em seguida, selecione **Opções**.
2. Clique no ícone **Configurações de segurança**.

3 Defina o nível de segurança movendo o botão deslizante para o nível desejado.

O nível de segurança varia de Bloqueado a Aberto:

- **Bloqueado —** Todas as conexões à Internet do computador são fechadas. Você pode usar essa configuração para bloquear portas que foram configuradas para serem abertas na página **Serviços do sistema**.
- **Segurança rígida —** Quando um aplicativo solicita um tipo específico de acesso à Internet (por exemplo, Somente acesso de saída), é possível permitir ou não que o aplicativo se conecte à Internet. Se o aplicativo solicitar posteriormente Acesso total, você poderá conceder Acesso total ou limitá-lo a Somente acesso de saída.
- **Segurança padrão (recomendada) —** Quando um aplicativo solicita e recebe acesso à Internet, ele recebe acesso total à Internet para manipular o tráfego de entrada e de saída.
- **Segurança confiável —** Todos os aplicativos são automaticamente considerados confiáveis quando tentam acessar a Internet pela primeira vez. No entanto, é possível configurar o Personal Firewall para usar alertas que notifiquem sobre novos aplicativos no computador. Use essa configuração caso alguns jogos ou arquivos de fluxo de mídia não estejam funcionando.
- **Aberto —** O firewall é efetivamente desativado. Essa configuração permite que todo o tráfego passe pelo Personal Firewall sem ser filtrado.

  NOTA
  Os aplicativos bloqueados anteriormente continuarão bloqueados se o firewall estiver definido como **Aberto** ou **Bloqueado**. Para evitar que isso ocorra, altere as permissões do aplicativo para **Permitir acesso total** ou exclua a regra de permissão **Bloqueado** da lista **Aplicativos da Internet**.

4 Selecione configurações adicionais de segurança:

  NOTA
  Se o computador for executado no Windows XP e vários usuários do XP tiverem sido adicionados, essas opções estarão disponíveis somente se você tiver efetuado logon como administrador.

- **Gravar os eventos da detecção de invasão (IDS) no registro de eventos de entrada —** Se você selecionar essa opção, os eventos detectados pelo IDS serão exibidos no registro de **Eventos de entrada**. O Sistema de detecção de invasão (IDS) detecta tipos comuns de ataques e outras atividades suspeitas. A detecção de invasão monitora todos os pacotes de dados de entrada e de saída em busca de métodos de transferência ou transferências de dados suspeitos. Ela os compara com um banco de dados de "assinaturas" e rejeita automaticamente os pacotes vindos de computadores ofensivos.

A detecção procura padrões de tráfego específicos usados pelos invasores. Ela também verifica todos os pacotes recebidos pelo computador para detectar o tráfego de ataques suspeitos ou conhecidos. Por exemplo, quando encontra pacotes ICMP, o Personal Firewall os analisa em busca de padrões de tráfego suspeito, comparando o tráfego ICMP com padrões de ataques conhecidos.

- **Aceitar pedidos de ping ICMP** — O tráfego ICMP é usado principalmente para executar rastreamentos e pings. O recurso de ping normalmente é usado para executar um teste rápido antes de estabelecer comunicações. Se você estiver usando ou já tiver usado um programa de compartilhamento de arquivos ponto a ponto, talvez receba muitas solicitações de ping. Se essa opção for selecionada, o Personal Firewall permitirá todas as solicitações de ping sem incluí-las no registro de **Eventos de entrada**. Se você não selecionar essa opção, o Personal Firewall bloqueará todas as solicitações de ping e as incluirá no registro de **Eventos de entrada**.
- **Permitir que usuários restritos alterem as configurações do firewall** — Se o computador estiver executando o Windows XP ou o Windows 2000 Professional com vários usuários, selecione essa opção para permitir que usuários restritos do XP modifiquem as configurações do Personal Firewall.

5 Clique em **OK** ao terminar de fazer as alterações.

Teste do McAfee Personal Firewall Plus

É possível testar a instalação do Personal Firewall para verificar possíveis vulnerabilidades a atividades suspeitas e invasões.

Para testar a instalação do Personal Firewall usando o ícone da McAfee na área de notificação:

- Clique com o botão direito do mouse no ícone da McAfee na área de notificação do Windows e selecione **Testar o firewall**.

O Personal Firewall abre o Internet Explorer e acessa http://www.hackerwatch.org/, um site da Web mantido pela McAfee. Siga as instruções da página de sondagem do Hackerwatch.org para testar o Personal Firewall.

Sobre a página Resumo

O Resumo do Personal Firewall contém quatro páginas:

- Resumo principal
- Resumo dos aplicativos
- Resumo de eventos
- Resumo do HackerWatch

As páginas **Resumo** contêm vários relatórios sobre eventos de entrada recentes, status de aplicativos e a atividade de invasão mundial relatada pelo HackerWatch.org. Também é possível encontrar links para tarefas comuns executadas no Personal Firewall.

Para abrir a página **Resumo principal** no Personal Firewall:

- Clique com o botão direito do mouse no ícone da McAfee na área de notificação do Windows, aponte para **Personal Firewall** e, em seguida, selecione **Exibir resumo** (Figura 4-1).

Figura 4-1. Página Resumo principal

Clique nestas opções para navegar para outras páginas **Resumo**:

Item	Descrição
Alterar exibição	Clique em **Alterar exibição** para abrir uma lista das páginas Resumo. Na lista, selecione uma página Resumo para ser exibida.
Seta para a direita	Clique no ícone de seta para a direita para exibir a próxima página Resumo.
Seta para a esquerda	Clique no ícone de seta para a esquerda a fim de exibir a página Resumo anterior.
Início	Clique nesse ícone para retornar à página **Resumo principal**.

A página **Resumo principal** fornece as seguintes informações:

Item	Descrição
Configuração de segurança	O status da configuração de segurança indica o nível de segurança para o qual o firewall está definido. Clique no link para alterar o nível de segurança.
Eventos bloqueados	O status dos eventos bloqueados exibe o número de eventos que foram bloqueados no dia. Clique no link para exibir detalhes do evento na página **Eventos de entrada**.
Alterações nas regras de aplicativo	O status das regras de aplicativo mostra o número de regras de aplicativo que foram alteradas recentemente. Clique no link para exibir a lista de aplicativos permitidos e bloqueados e para modificar permissões de aplicativos.
O que há de novo?	**O que há de novo?** mostra o último aplicativo que recebeu acesso total à Internet.
Último evento	**Último evento** mostra os eventos de entrada mais recentes. Clique em um link para rastrear um evento ou para confiar no endereço IP. A confiança em um endereço IP permite que todo o tráfego proveniente desse endereço chegue ao seu computador.
Relatório diário	**Relatório diário** exibe o número de eventos de entrada que o Personal Firewall bloqueou no dia, na semana e no mês. Clique no link para exibir detalhes do evento na página **Eventos de entrada**.
Aplicativos ativos	**Aplicativos ativos** exibe os aplicativos que estão em execução no computador e acessando a Internet. Clique em um aplicativo para exibir os endereços IP aos quais ele está se conectando.
Tarefas comuns	Clique em um link em **Tarefas comuns** para passar às páginas do Personal Firewall, nas quais é possível exibir a atividade do firewall e executar tarefas.

Para exibir a página **Resumo dos aplicativos**:

1 Clique com o botão direito do mouse no ícone da McAfee na área de notificação do Windows, aponte para **Personal Firewall** e, em seguida, selecione **Exibir resumo**.

2 Clique em **Alterar exibição** e selecione **Resumo dos aplicativos**.

A página **Resumo dos aplicativos** fornece as seguintes informações:

Item	Descrição
Monitor de tráfego	A opção **Monitor de tráfego** mostra as conexões de entrada e saída da Internet nos últimos quinze minutos. Clique no gráfico para exibir os detalhes da monitoração do tráfego.
Aplicativos ativos	**Aplicativos ativos** mostra o uso de largura de banda dos aplicativos mais ativos do computador nas últimas 24 horas. **Aplicativo** — O aplicativo que está acessando a Internet. **%** — A porcentagem de largura de banda usada pelo aplicativo. **Permissão** — O tipo de acesso à Internet permitido ao aplicativo. **Regra criada** — Quando a regra de aplicativo foi criada.
O que há de novo?	**O que há de novo?** mostra o último aplicativo que recebeu acesso total à Internet.
Aplicativos ativos	**Aplicativos ativos** exibe os aplicativos que estão em execução no computador e acessando a Internet. Clique em um aplicativo para exibir os endereços IP aos quais ele está se conectando.
Tarefas comuns	Clique em um link em **Tarefas comuns** para passar às páginas do Personal Firewall, nas quais é possível exibir o status do aplicativo e executar as tarefas relacionadas ao aplicativo.

Para exibir a página **Resumo de eventos**:

1 Clique com o botão direito do mouse no ícone da McAfee na área de notificação do Windows, aponte para **Personal Firewall** e, em seguida, selecione **Exibir resumo**.

2 Clique em **Alterar exibição** e selecione **Resumo de eventos**.

A página **Resumo de eventos** oferece as seguintes informações:

Item	Descrição
Comparação de portas	**Comparação de portas** mostra um gráfico de torta das portas mais solicitadas do computador nos últimos 30 dias. Clique em um nome de porta para exibir os detalhes da página **Eventos de entrada**. Também é possível posicionar o ponteiro do mouse sobre o número da porta para exibir a descrição.
Principais infratores	**Principais infratores** mostra os endereços IP bloqueados com mais freqüência, quando o último evento de entrada ocorreu para cada endereço e o número total de eventos de entrada nos últimos trinta dias para cada endereço. Clique em um evento para exibir os detalhes na página **Eventos de entrada**.
Relatório diário	**Relatório diário** exibe o número de eventos de entrada que o Personal Firewall bloqueou no dia, na semana e no mês. Clique em um número para exibir os detalhes do evento no registro de **Eventos de entrada**.
Último evento	**Último evento** mostra os eventos de entrada mais recentes. Clique em um link para rastrear um evento ou para confiar no endereço IP. A confiança em um endereço IP permite que todo o tráfego proveniente desse endereço chegue ao seu computador.
Tarefas comuns	Clique em um link em **Tarefas comuns** para passar às páginas do Personal Firewall, nas quais é possível exibir os detalhes dos eventos e executar as tarefas a eles relacionadas.

Para exibir a página **Resumo do HackerWatch**:

1. Clique com o botão direito do mouse no ícone da McAfee na área de notificação do Windows, aponte para **Personal Firewall** e, em seguida, selecione **Exibir resumo.**
2. Clique em **Alterar exibição** e selecione **Resumo do HackerWatch**.

A página **Resumo do HackerWatch** fornece as informações seguintes**.**

Item	Descrição
Atividade mundial	**Atividade mundial** mostra um mapa-múndi que identifica atividades recentemente bloqueadas, monitoradas pelo HackerWatch.org. Clique no mapa para abrir o mapa de análise de ameaças globais no HackerWatch.org.
Rastreamento de eventos	**Rastreamento de eventos** mostra o número de eventos de entrada enviados para o HackerWatch.org.

Item	Descrição
Atividade global de porta	**Atividade global de porta** mostra as principais portas que, nos últimos 5 dias, aparentaram estar sob ameaça. Clique em uma porta para exibir seu número e sua descrição.
Tarefas comuns	Clique em um link em **Tarefas comuns** para passar às páginas do HackerWatch.org nas quais é possível obter mais informações sobre a atividade de hackers no mundo todo.

Sobre a página Aplicativos da Internet

Use a página **Aplicativos da Internet** para exibir a lista de aplicativos permitidos e bloqueados.

Para iniciar a página **Aplicativos da Internet**:

- Clique com o botão direito do mouse no ícone da McAfee na área de notificação do Windows, aponte para **Personal Firewall** e, em seguida, selecione **Aplicativos** (Figura 4-2).

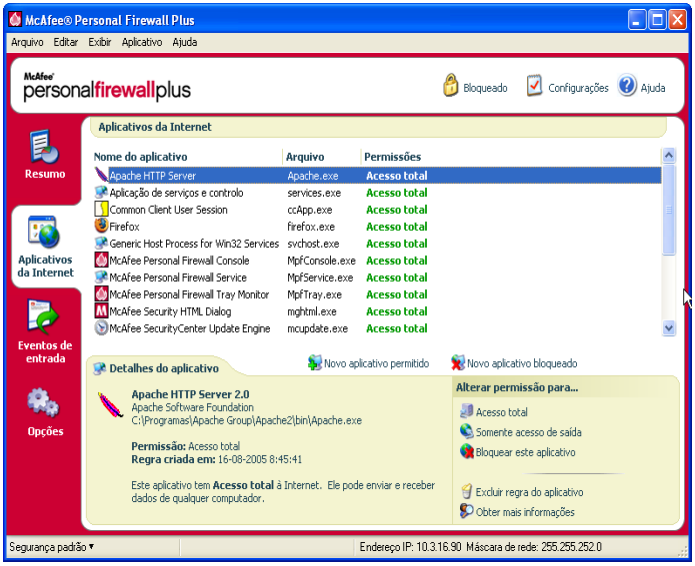


Figura 4-2. Página Aplicativos da Internet

A página **Aplicativos da Internet** oferece as seguintes informações:

- Nomes dos aplicativos
- Nomes dos arquivos
- Níveis de permissão atuais
- Detalhes do aplicativo: nome e versão do aplicativo, nome da empresa, nome do caminho, permissão, marcas de data e hora e explicações dos tipos de permissão

Alteração de regras de aplicativo

O Personal Firewall permite alterar as regras de acesso dos aplicativos.

Para alterar uma regra de aplicativo:

1. Clique com o botão direito do mouse no ícone da McAfee, aponte para **Personal Firewall** e selecione **Aplicativos da Internet**.
2. Na lista **Aplicativos da Internet**, clique com o botão direito do mouse na regra de um aplicativo e selecione um nível diferente:
   - **Permitir acesso total —** Permite que o aplicativo estabeleça conexões de entrada e saída da Internet.
   - **Somente acesso de saída —** Permite que o aplicativo estabeleça apenas uma conexão de saída da Internet.
   - **Bloquear este aplicativo —** Não permite ao aplicativo o acesso à Internet.

     NOTA
     Os aplicativos bloqueados anteriormente continuarão bloqueados se o firewall estiver definido como **Aberto** ou **Bloqueado**. Para evitar que isso ocorra, altere a regra de acesso do aplicativo para **Permitir acesso total** ou exclua a regra de permissão **Bloqueado** da lista **Aplicativos da Internet**.

Para excluir uma regra de aplicativo:

1. Clique com o botão direito do mouse no ícone da McAfee na área de notificação do Windows, aponte para **Personal Firewall** e selecione **Aplicativos da Internet**.
2. Na lista **Aplicativos da Internet**, clique com o botão direito do mouse na regra de aplicativo e selecione **Excluir regra do aplicativo**.

Na próxima vez que o aplicativo solicitar acesso à Internet, defina seu nível de permissão para adicioná-lo à lista novamente.

Permissão e bloqueio de aplicativos da Internet

Para alterar a lista de aplicativos da Internet permitidos e bloqueados:

1. Clique com o botão direito do mouse no ícone da McAfee na área de notificação do Windows, aponte para **Personal Firewall** e selecione **Aplicativos da Internet**.
2. Na página **Aplicativos da Internet**, clique em uma das seguintes opções:
   - **Novo aplicativo permitido** — Permite ao aplicativo acesso total à Internet.
   - **Novo aplicativo bloqueado** — Não permite o acesso de um aplicativo à Internet.
   - **Excluir regra do aplicativo** — Remove uma regra de aplicativo.

Sobre a página Eventos de entrada

Use a página **Eventos de entrada** para exibir o registro de **Eventos de entrada** gerado quando o Personal Firewall bloqueia conexões à Internet não solicitadas.

Para iniciar a página **Eventos de entrada**:

- Clique com o botão direito do mouse no ícone da McAfee na área de notificação do Windows, aponte para **Personal Firewall** e, em seguida, selecione **Eventos de entrada** (Figura 4-3).

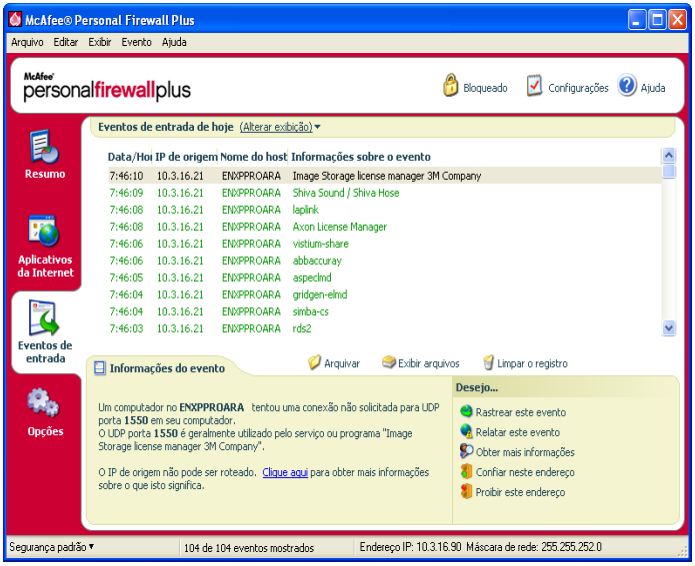


Figura 4-3. Página Eventos de entrada

A página **Eventos de entrada** oferece as seguintes informações:

- Marcas de data e hora
- IPs de origem
- Nomes de host
- Nomes de serviços ou de aplicativos
- Detalhes do evento: tipos de conexão, portas de conexão, IP ou nome do host e explicações de eventos de porta

Compreensão dos eventos

Sobre endereços IP

Os endereços IP são números: quatro números, cada um entre 0 e 255. Esses números identificam um local específico para onde o tráfego pode ser direcionado na Internet.

Tipos de endereço IP

Diversos endereços IP são incomuns por vários motivos:

Endereços IP não roteáveis — Também conhecidos como "espaço IP privado". Esses endereços IP não podem ser usados na Internet. Os blocos de endereços IP privados são 10.x.x.x, 172.16.x.x - 172.31.x.x e 192.168.x.x.

Endereços IP de loopback — Os endereços de loopback são usados para fins de teste. O tráfego enviado a esse bloco de endereços IP volta para o dispositivo que gerou o pacote. Ele nunca sai do dispositivo, sendo usado principalmente para testes de hardware e software. O bloco de endereços IP de loopback é 127.x.x.x.

Endereço IP nulo — Trata-se de um endereço inválido. Quando detectado, o Personal Firewall indica que o tráfego utilizou um endereço IP em branco. Geralmente isso indica que o remetente está deliberadamente ocultando a origem do tráfego. O remetente não poderá receber nenhuma resposta para esse tráfego, a não ser que o pacote seja recebido por um aplicativo que reconheça seu conteúdo e que o pacote contenha instruções específicas para esse aplicativo. Qualquer endereço iniciado com 0 (0.x.x.x) é um endereço nulo. Por exemplo, 0.0.0.0 é um endereço IP nulo.

Eventos de 0.0.0.0

Quando são exibidos eventos do endereço IP 0.0.0.0, existem duas causas prováveis. A primeira, e mais comum, é que o computador recebeu um pacote mal formatado. A Internet nem sempre é 100% confiável e é comum haver pacotes com problemas. Como o Personal Firewall vê os pacotes antes que o TCP/IP possa validá-los, ele pode relatar esses pacotes como um evento.

A outra situação ocorre quando o IP de origem é fraudado ou falso. Os pacotes fraudados podem ser um sinal de que alguém está em busca de cavalos de Tróia no seu computador. O Personal Firewall bloqueia esse tipo de atividade, portanto o computador está seguro.

Eventos de 127.0.0.1

Às vezes, os eventos indicam o IP de origem como 127.0.0.1. Isso é o que se chama de endereço de loopback ou localhost.

Muitos programas legítimos usam o endereço de loopback para comunicação entre componentes. Por exemplo, é possível configurar muitos servidores de e-mail pessoal ou servidores Web por meio de uma interface da Web. Para acessar a interface, digite "http://localhost/" no seu navegador.

O Personal Firewall permite o tráfego desses programas; portanto, se você receber eventos de 127.0.0.1, é provável que o endereço IP de origem esteja fraudado ou seja falso. Os pacotes fraudados geralmente indicam que outro computador está em busca de cavalos de Tróia no seu computador. O Personal Firewall bloqueia essas tentativas de invasão; portanto, o computador está seguro.

Alguns programas, particularmente o Netscape 6.2 e posterior, exigem que o endereço 127.0.0.1 seja adicionado à lista **Endereços IP confiáveis**. Os componentes desses programas se comunicam entre si de uma maneira que o Personal Firewall não consegue determinar se o tráfego é local ou não.

No exemplo do Netscape 6.2, se você não confiar no 127.0.0.1, não poderá usar a sua lista de amigos. Portanto, se você receber tráfego de 127.0.0.1 e todos os aplicativos do computador funcionarem normalmente, é sinal de que esse tráfego pode ser bloqueado sem problemas. Porém, se ocorrerem problemas com algum programa (como o Netscape), adicione o 127.0.0.1 à lista **Endereços IP confiáveis** do Personal Firewall.

Se isso resolver o problema, será necessário tomar uma decisão: se confiar no 127.0.0.1, o programa funcionará, mas você estará mais vulnerável a ataques de fraude. Se não confiar no endereço, o programa não funcionará, mas você continuará protegido contra determinado tráfego mal-intencionado.

Eventos de computadores na LAN

Os eventos podem ser gerados por computadores da rede local (LAN). Para indicar que esses eventos são gerados pela sua rede, o Personal Firewall os exibe em verde.

Na maioria das configurações de LAN corporativas, selecione **Tornar todos os computadores da sua LAN confiáveis** nas opções de Endereços IP confiáveis.

Em algumas situações a rede "local" pode ser tão perigosa quanto a Internet, especialmente se o computador estiver em uma rede de banda larga DSL ou de modem a cabo. Nesse caso, não selecione **Tornar todos os computadores da sua LAN confiáveis**. Em vez disso, adicione os endereços IP dos computadores locais à lista **Endereços IP confiáveis**.

Eventos de endereços IP privados

Os endereços IP de formato 192.168.xxx.xxx, 10.xxx.xxx.xxx e 172.16.0.0 - 172.31.255.255 são chamados de não-roteáveis ou privados. Esses endereços IP nunca devem sair da sua rede e, na maioria das vezes, são confiáveis.

O bloco 192.168 xxx.xxx é usado com o Microsoft Internet Connection Sharing (ICS). Se estiver usando ICS e receber eventos desse bloco de endereços IP, você poderá adicionar o endereço IP 192.168.255.255 à lista **Endereços IP confiáveis**. Isso tornará todo o bloco 192.168.xxx.xxx confiável.

Se você não estiver em uma rede privada e receber eventos desses intervalos de endereços IP, talvez o endereço IP de origem seja fraudado ou falso. Os pacotes fraudados geralmente são um sinal de que alguém está fazendo uma varredura em busca de cavalos de Tróia. É importante lembrar que o Personal Firewall bloqueou essa tentativa e que, portanto, o seu computador está seguro.

Como os endereços IP privados se referem a computadores diferentes dependendo da rede em que você está, o relato desses eventos não traz nenhum benefício e, por isso, não é necessário fazê-lo.

Exibição de eventos no registro de Eventos de entrada

O registro de **Eventos de entrada** exibe os eventos de várias formas. A exibição padrão se limita aos eventos que ocorreram no dia atual. Você também pode exibir eventos que ocorreram na semana passada ou exibir o registro completo.

O Personal Firewall também permite exibir eventos de entrada de dias específicos, de endereços da Internet específicos (endereços IP) ou eventos que contenham as mesmas informações de eventos.

Para obter informações sobre um evento, clique nele para exibir as informações no painel **Informações do evento**.

Exibição dos eventos de hoje

Use essa opção para analisar os eventos do dia.

Para mostrar os eventos de hoje:

1. Clique com o botão direito do mouse no ícone da McAfee na área de notificação do Windows, aponte para **Personal Firewall** e, em seguida, selecione **Eventos de entrada**.
2. No registro de **Eventos de entrada**, clique com o botão direito do mouse em uma entrada, e, em seguida, clique em **Mostrar eventos de hoje**.

Exibição dos eventos desta semana

Use essa opção para analisar os eventos da semana.

Para mostrar os eventos da semana:

1. Clique com o botão direito do mouse no ícone da McAfee na área de notificação do Windows, aponte para **Personal Firewall** e, em seguida, selecione **Eventos de entrada**.
2. No registro de **Eventos de entrada**, clique com o botão direito do mouse em uma entrada e, em seguida, clique em **Mostrar eventos desta semana**.

Exibição do registro de Eventos de entrada completo

Use essa opção para analisar todos os eventos.

Para mostrar todos os eventos do registro de **Eventos de entrada**:

1. Clique com o botão direito do mouse no ícone da McAfee, aponte para **Personal Firewall** e clique em **Eventos de entrada**.
2. No registro de **Eventos de entrada**, clique com o botão direito do mouse em uma entrada e, em seguida, clique em **Mostrar registro completo**.

   O registro de **Eventos de entrada** exibe todos os eventos do registro de **Eventos de entrada**.

Exibição de eventos de um dia específico

Use essa opção para analisar os eventos de um dia específico.

Para mostrar os eventos de um dia:

1. Clique com o botão direito do mouse no ícone da McAfee na área de notificação do Windows, aponte para **Personal Firewall** e, em seguida, selecione **Eventos de entrada**.
2. No registro de **Eventos de entrada**, clique com o botão direito do mouse em uma entrada e clique em **Mostrar somente eventos a partir deste dia**.

Exibição de eventos de um endereço da Internet específico

Use essa opção para examinar outros eventos que se originam de um endereço da Internet específico.

Para mostrar eventos de um endereço da Internet:

1. Clique com o botão direito do mouse no ícone da McAfee na área de notificação do Windows, aponte para **Personal Firewall** e clique em **Eventos de entrada**.
2. No registro de **Eventos de entrada**, clique com o botão direito do mouse em uma entrada e, em seguida, clique em **Mostrar somente eventos do endereço da Internet selecionado**.

Exibição de eventos que compartilham informações de evento idênticas

Use essa opção para examinar outros eventos no registro de **Eventos de entrada** que tenham as mesmas informações do evento selecionado na coluna **Informações sobre o evento**. Você pode descobrir quantas vezes esse evento ocorreu e se ele é da mesma origem. A coluna **Informações sobre o evento** oferece uma descrição do evento e, se for conhecido, o programa ou serviço comum que utiliza essa porta.

Para mostrar eventos que compartilham informações idênticas:

1. Clique com o botão direito do mouse no ícone da McAfee na área de notificação do Windows, aponte para **Personal Firewall** e clique em **Eventos de entrada**.
2. No registro de **Eventos de entrada**, clique com o botão direito do mouse em uma entrada e, em seguida, clique em **Mostrar somente eventos com as mesmas informações de evento**.

Resposta a eventos de entrada

Além de examinar detalhes sobre eventos no registro de **Eventos de entrada**, é possível executar um rastreamento visual dos endereços IP de um evento no registro de **Eventos de entrada** ou obter detalhes no site HackerWatch.org da comunidade on-line anti-hackers.

Rastreamento do evento selecionado

Você pode tentar executar um rastreamento visual dos endereços IP de um evento contido no registro de **Eventos de entrada**.

Para rastrear um evento selecionado:

1. Clique com o botão direito do mouse no ícone da McAfee na área de notificação do Windows, aponte para **Personal Firewall** e selecione **Eventos de entrada**.
2. No registro de **Eventos de entrada**, clique com o botão direito do mouse no evento que deseja rastrear e, em seguida, clique em **Rastrear o evento selecionado**. Você também pode clicar duas vezes em um evento para rastreá-lo.

Por padrão, o Personal Firewall inicia um rastreamento visual usando o programa Visual Trace integrado ao Personal Firewall.

Obtenção de informações do HackerWatch.org

Para obter informações do HackerWatch.org:

1. Clique com o botão direito do mouse no ícone da McAfee, aponte para **Personal Firewall** e selecione **Eventos de entrada**.
2. Selecione a entrada do evento na página **Eventos de entrada** e clique em **Obter mais informações** no painel **Desejo**.

O seu navegador padrão da Web é iniciado e abre o site HackerWatch.org para obter informações sobre o tipo de evento e saber se ele deve ser relatado.

Relato de um evento

Para relatar um evento que parece ser um ataque ao seu computador:

1. Clique com o botão direito do mouse no ícone da McAfee na área de notificação do Windows, aponte para **Personal Firewall** e selecione **Eventos de entrada**.
2. Clique no evento que deseja relatar e, em seguida, clique em **Relatar este evento** no painel **Desejo**.

O Personal Firewall relata o evento para o site HackerWatch.org usando a sua ID exclusiva.

Inscrição no HackerWatch.org

Quando você abre a página **Resumo** pela primeira vez, o Personal Firewall contacta o site HackerWatch.org para gerar a sua ID de usuário exclusiva. Se você for um usuário existente, a inscrição será validada automaticamente. Se for um novo usuário, você deverá inserir um apelido e um endereço de e-mail e, em seguida, clicar no link de validação no e-mail de confirmação do site HackerWatch.org para poder usar os recursos de filtragem de eventos/envio de eventos por e-mail desse site.

É possível relatar eventos para o site HackerWatch.org sem validar a ID de usuário. No entanto, para filtrar eventos e enviá-los por e-mail para um amigo, é necessário inscrever-se nesse serviço.

A inscrição no serviço permite que os envios sejam rastreados e que você seja notificado se o HackerWatch.org precisar de mais informações ou da sua intervenção. A inscrição também é necessária porque precisamos confirmar todas as informações recebidas para que elas sejam úteis.

Todos os endereços de e-mail fornecidos ao site HackerWatch.org são mantidos como confidenciais. Se um provedor de Internet solicitar informações adicionais, essa solicitação será roteada pelo site HackerWatch.org. Seu endereço de e-mail nunca será revelado.

Confiança em um endereço

É possível usar a página **Eventos de entrada** para adicionar um endereço IP à lista **Endereços IP confiáveis**, permitindo, assim, a conexão permanente.

Se, na página **Eventos de entrada**, houver um evento contendo um endereço IP que você precise permitir, determine que o Personal Firewall sempre permita conexões desse endereço.

Para adicionar um endereço IP à lista **Endereços IP confiáveis**:

1. Clique com o botão direito do mouse no ícone da McAfee na área de notificação do Windows, aponte para **Personal Firewall** e selecione **Eventos de entrada**.
2. Clique com o botão direito do mouse no evento cujo endereço IP deve ser confiável e clique em **Confiar no endereço IP de origem**.

Verifique se o endereço IP exibido na caixa de diálogo **Confiar neste endereço** está correto e clique em **OK**. O endereço IP é adicionado à lista **Endereços IP confiáveis**.

Para verificar se o endereço IP foi adicionado:

1. Clique com o botão direito do mouse no ícone da McAfee na área de notificação do Windows, aponte para **Personal Firewall** e selecione **Opções**.
2. Clique no ícone **IPs confiáveis e proibidos** e, em seguida, na guia **Endereços IP confiáveis**.

O endereço IP aparece marcado na lista **Endereços IP confiáveis**.

Proibição de um endereço

Um endereço IP que aparece no registro de **Eventos de entrada** indica que o tráfego desse endereço foi bloqueado. Portanto, proibir um endereço não garante proteção adicional, a menos que as portas do computador sejam abertas deliberadamente pelo recurso Serviços do sistema ou que o computador possua um aplicativo com permissão para receber tráfego.

Adicione um endereço IP à lista de endereços proibidos somente se houver uma ou mais portas deliberadamente abertas e se houver necessidade de bloquear o acesso desse endereço às portas abertas.

Se houver algum evento na página **Eventos de entrada** que contenha um endereço IP a ser proibido, é possível configurar o Personal Firewall para impedir sempre as conexões desse endereço.

É possível usar a página **Eventos de entrada**, que lista os endereços IP de todo o tráfego de entrada da Internet, para proibir um endereço IP suspeito de ser a origem de atividade suspeita ou indesejada na Internet.

Para adicionar um endereço IP à lista **Endereços IP proibidos**:

1. Clique com o botão direito do mouse no ícone da McAfee na área de notificação do Windows, aponte para **Personal Firewall** e, em seguida, selecione **Eventos de entrada**.
2. A página **Eventos de entrada** lista os endereços IP de todo o tráfego de entrada da Internet. Selecione um endereço IP e execute um dos seguintes procedimentos:
   - Clique com o botão direito do mouse no endereço IP e selecione **Proibir o endereço IP de origem**.
   - No menu **Desejo**, clique em **Proibir este endereço**.

3 Na caixa de diálogo Adicionar regra de endereço IP proibido, use uma ou mais das configurações a seguir para configurar a regra de endereço IP proibido:

- **Um endereço IP único**: O endereço IP a ser proibido. A entrada padrão é o endereço IP selecionado na página **Eventos de entrada**.
- **Um intervalo de endereços IP**: Os endereços IP entre o endereço especificado em Do endereço IP e o endereço IP especificado em Para o endereço IP.
- **Fazer com que esta regra expire em**: Data e hora de expiração da regra do endereço IP proibido. Selecione os menus suspensos apropriados para selecionar a data e a hora.
- **Descrição**: Opcionalmente, descreva a nova regra.
- Clique em **OK**.

4 Na caixa de diálogo, clique em **Sim** para confirmar a configuração. Clique em **Não** para voltar à caixa de diálogo Adicionar regra de endereço IP proibido.

Quando detecta um evento proveniente de uma conexão proibida com a Internet, o Personal Firewall emite um alerta de acordo com o método especificado na página **Configurações de alerta**.

Para verificar se o endereço IP foi adicionado:

1 Clique na guia **Opções**.

2 Clique no ícone **IPs confiáveis e proibidos** e, em seguida, clique na guia **Endereços IP proibidos**.

O endereço IP aparece marcado na lista **Endereços IP proibidos**.

Gerenciamento do registro de Eventos de entrada

A página **Eventos de entrada** permite gerenciar os eventos do registro de **Eventos de entrada** gerados quando o Personal Firewall bloqueia tráfego de Internet não solicitado.

Arquivamento do registro de Eventos de entrada

É possível arquivar o registro de **Eventos de entrada** atual para salvar todos os eventos de entrada registrados, incluindo datas e horas, IPs de origem, nomes de host, portas e informações sobre eventos. O registro de **Eventos de entrada** deve ser arquivado periodicamente para que não fique grande demais.

Para arquivar o registro de **Eventos de entrada**:

1. Clique com o botão direito do mouse no ícone da McAfee na área de notificação do Windows, aponte para **Personal Firewall** e, em seguida, selecione **Eventos de entrada**.
2. Na página **Eventos de entrada**, clique em **Arquivar**.
3. Na caixa de diálogo **Arquivar registro**, clique em **Sim** para continuar com a operação.
4. Clique em **Salvar** para salvar o arquivo no local padrão ou navegue até o local onde deseja salvá-lo.

> **NOTA**
> Por padrão, o Personal Firewall arquiva automaticamente o registro de **Eventos de entrada**. Marque ou desmarque **Arquivar automaticamente os eventos registrados** na página **Configurações do registro de eventos** para ativar ou desativar a opção.

Exibição de um registro de Eventos de entrada arquivado

Você pode exibir qualquer registro de **Eventos de entrada** que tenha sido arquivado anteriormente. O arquivo salvo inclui datas e horários, IPs de origem, nomes de host, portas e informações sobre eventos relacionados aos eventos.

Para exibir um registro de **Eventos de entrada** arquivado:

1. Clique com o botão direito do mouse no ícone da McAfee na área de notificação do Windows, aponte para **Personal Firewall** e, em seguida, selecione **Eventos de entrada**.
2. Na página **Eventos de entrada**, clique em **Exibir arquivos**.
3. Selecione ou procure o nome de arquivo e clique em **Abrir**.

Limpeza do registro de Eventos de entrada

É possível limpar todas as informações do registro de **Eventos de entrada**.

> **AVISO**
> Se você limpar o registro de Eventos de entrada, ele não poderá ser recuperado. Se você acha que precisará do registro de eventos no futuro, arquive-o.

Para limpar o registro de **Eventos de entrada**:

1. Clique com o botão direito do mouse no ícone da McAfee, aponte para **Personal Firewall** e selecione **Eventos de entrada**.
2. Na página **Eventos de entrada**, clique em **Limpar o registro**.
3. Clique em **Sim** na caixa de diálogo para limpar o registro.

Cópia de um evento para a área de transferência

É possível copiar um evento para a área de transferência para poder colá-lo em um arquivo de texto usando o Bloco de notas.

Para copiar eventos para a área de transferência:

1. Clique com o botão direito do mouse no ícone da McAfee, aponte para **Personal Firewall** e selecione **Eventos de entrada**.
2. Clique com o botão direito do mouse no evento do registro de **Eventos de entrada**.
3. Clique em **Copiar evento selecionado para a área de transferência**.
4. Inicie o Bloco de notas.
   - Digite `notepad` na linha de comando ou clique no botão **Iniciar** do Windows, aponte para **Programas** e, em seguida, para **Acessórios**. Selecione **Bloco de notas**.
5. Clique em **Editar** e, em seguida, em **Colar**. O texto do evento será exibido no Bloco de notas. Repita esta etapa para todos os eventos necessários.
6. Salve o arquivo do Bloco de notas em um local seguro.

Exclusão do evento selecionado

É possível excluir eventos do registro de **Eventos de entrada**.

Para excluir eventos do registro de **Eventos de entrada**:

1. Clique com o botão direito do mouse no ícone da McAfee na área de notificação do Windows, aponte para **Personal Firewall** e, em seguida, selecione **Eventos de entrada**.
2. Clique na entrada do evento a ser excluído na página **Eventos de entrada**.
3. No menu **Editar**, clique em **Excluir o evento selecionado**. O evento é excluído do registro de **Eventos de entrada**.

Sobre alertas

Recomendamos que você se familiarize com os tipos de alerta que encontrará ao usar o Personal Firewall. Observe a seguir os tipos de alerta que podem ser exibidos e as possíveis respostas a serem escolhidas para reagir com segurança a um alerta.

NOTA
As recomendações sobre alertas ajudam a decidir como lidar com cada alerta. Para exibir recomendações nos alertas, clique na guia **Opções**, clique no ícone **Configurações de alerta** e selecione **Usar recomendações inteligentes** (o padrão) ou **Exibir somente as recomendações inteligentes** na lista **Recomendações inteligentes**.

Alertas vermelhos

Os alertas vermelhos contêm informações importantes que exigem atenção imediata:

- **Aplicativo da Internet bloqueado** — Esse alerta será exibido se o Personal Firewall impedir o acesso de um aplicativo à Internet. Por exemplo, se for exibido um alerta de programa cavalo de Tróia, a McAfee impedirá automaticamente que esse programa acesse a Internet e recomendará que se faça uma varredura de vírus no computador.
- **O aplicativo deseja acessar a Internet —** Esse alerta aparece quando o Personal Firewall detecta tráfego de Internet ou de rede para novos aplicativos.
- **O aplicativo foi modificado —** Esse alerta é exibido quando o Personal Firewall detecta alteração de um aplicativo ao qual havia sido concedido acesso à Internet anteriormente. Se você não tiver atualizado o aplicativo recentemente, tome cuidado ao permitir que o aplicativo modificado acesse a Internet.

- **O aplicativo solicita acesso como servidor —** Esse alerta aparece quando o Personal Firewall detecta que um aplicativo ao qual você concedeu acesso à Internet anteriormente solicitou acesso como servidor.

NOTA
A configuração padrão das Atualizações automáticas do Windows XP SP2 faz o download e instala as atualizações do sistema operacional Windows e de outros programas da Microsoft em execução no computador sem avisar o usuário. Quando um aplicativo é modificado em uma atualização silenciosa do Windows, um alerta do McAfee Personal Firewall é exibido na primeira vez que o aplicativo Microsoft é usado após a atualização.

IMPORTANTE
Você deve conceder acesso aos aplicativos que precisam acessar a Internet para executar atualizações de produtos on-line (como os serviços da McAfee) a fim de mantê-los atualizados.

Alerta Aplicativo da Internet bloqueado

Quando é exibido um alerta de cavalo de Tróia (Figura 4-4), o Personal Firewall nega automaticamente o acesso à Internet a esse programa e recomenda que seja feita a varredura no computador em busca de vírus. Se o McAfee VirusScan não estiver instalado, inicie o McAfee SecurityCenter.

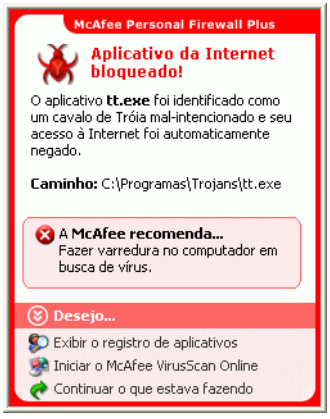


Figura 4-4. Alerta Aplicativo da Internet bloqueado

Veja uma breve descrição do evento e escolha uma das opções a seguir:

- Clique em **Obter mais informações** para obter detalhes sobre o evento com o registro de **Eventos de entrada** (consulte *Sobre a página Eventos de entrada* na página 91 para obter detalhes).
- Clique em **Iniciar o McAfee VirusScan** para fazer uma varredura de vírus no computador.
- Clique em **Continuar o que eu estava fazendo** se não desejar executar nenhuma ação além do que o Personal Firewall já tenha feito.
- Clique em **Conceder acesso de saída** para permitir uma conexão de saída (segurança **Rígida**).

Alerta O aplicativo deseja acessar a Internet

Se você tiver selecionado segurança **Padrão** ou **Rígida** nas opções de Configurações de segurança, o Personal Firewall exibirá um alerta (Figura 4-5) quando detectar conexões de Internet ou de rede para aplicativos novos ou modificados.

Figura 4-5. Alerta O aplicativo deseja acessar a Internet

Se for exibido um alerta recomendando cuidado ao permitir que o aplicativo acesse a Internet, clique em **Clique aqui para obter mais informações** para obter mais informações sobre o aplicativo. Essa opção só aparecerá no alerta se o Personal Firewall estiver configurado para usar recomendações inteligentes.

A McAfee talvez não reconheça o aplicativo que está tentando obter acesso à Internet (Figura 4-6).

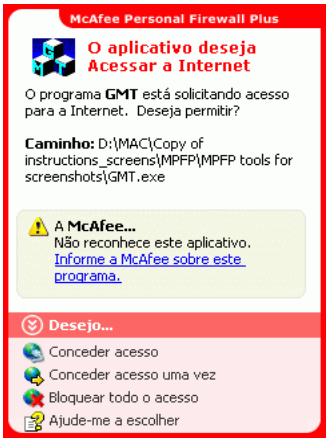


Figura 4-6. Alerta de aplicativo não reconhecido

Portanto, a McAfee não pode fornecer nenhuma recomendação sobre como lidar com o aplicativo. Você pode relatar o aplicativo para a McAfee clicando em **Informe à McAfee sobre este programa**. Uma página da Web é exibida e solicita informações relacionadas ao aplicativo. Forneça o máximo de informações que puder.

As informações enviadas são usadas juntamente com outras ferramentas de pesquisa pelos operadores do HackerWatch para determinar se um aplicativo merece estar relacionado em nosso banco de dados de aplicativos conhecidos e, em caso afirmativo, como ele deve ser tratado pelo Personal Firewall.

Veja uma breve descrição do evento e escolha uma das opções a seguir:

- Clique em **Conceder acesso** para permitir ao aplicativo uma conexão de entrada e saída da Internet.
- Clique em **Conceder acesso uma vez** para conceder ao aplicativo uma conexão temporária à Internet. O acesso é limitado ao tempo decorrido entre a inicialização e o encerramento do aplicativo.
- Clique em **Bloquear todo o acesso** para proibir uma conexão à Internet.
- Clique em **Conceder acesso de saída** para permitir uma conexão de saída (segurança **Rígida**).
- Clique em **Ajude-me a escolher** para exibir a Ajuda on-line sobre as permissões de acesso do aplicativo.

Alerta O aplicativo foi modificado

Se o nível de segurança **Confiável**, **Padrão** ou **Rígida** tiver sido selecionado nas opções Configurações de segurança, o Personal Firewall exibirá um alerta (Figura 4-7) quando detectar alteração de um aplicativo ao qual o acesso à Internet foi permitido anteriormente. Se você não tiver atualizado esse aplicativo recentemente, tome cuidado ao permitir o acesso do aplicativo modificado à Internet.

Figura 4-7. Alerta O aplicativo foi modificado

Veja uma breve descrição do evento e escolha uma das opções a seguir:

- Clique em **Conceder acesso** para permitir ao aplicativo uma conexão de entrada e saída da Internet.
- Clique em **Conceder acesso uma vez** para conceder ao aplicativo uma conexão temporária à Internet. O acesso é limitado ao tempo decorrido entre a inicialização e o encerramento do aplicativo.
- Clique em **Bloquear todo o acesso** para proibir uma conexão à Internet.
- Clique em **Conceder acesso de saída** para permitir uma conexão de saída (segurança **Rígida**).
- Clique em **Ajude-me a escolher** para exibir a Ajuda on-line sobre as permissões de acesso do aplicativo.

Alerta O aplicativo solicita acesso como servidor

Se você tiver selecionado segurança **Rígida** nas opções de Configurações de segurança, o Personal Firewall exibirá um alerta (Figura 4-8) quando detectar que um aplicativo ao qual você concedeu acesso à Internet anteriormente solicitou acesso como servidor.

Figura 4-8. Alerta O aplicativo solicita acesso como servidor

Por exemplo, um alerta é exibido quando o MSN Messenger solicita acesso como servidor para enviar um arquivo durante um bate-papo.

Veja uma breve descrição do evento e escolha uma das opções a seguir:

- Clique em **Conceder acesso uma vez** para permitir ao aplicativo um acesso temporário à Internet. O acesso é limitado ao tempo decorrido entre a inicialização e o encerramento do aplicativo.
- Clique em **Conceder acesso como servidor** para permitir ao aplicativo uma conexão de entrada e saída da Internet.
- Clique em **Restringir ao acesso de saída** para proibir uma conexão de entrada da Internet.
- Clique em **Bloquear todo o acesso** para proibir uma conexão à Internet.
- Clique em **Ajude-me a escolher** para exibir a Ajuda on-line sobre permissões de acesso do aplicativo.

Alertas verdes

Os alertas verdes notificam sobre eventos no Personal Firewall, como aplicativos que receberam acesso à Internet automaticamente.

Programa com permissão para acessar a Internet — Esse alerta é exibido quando o Personal Firewall concede acesso à Internet automaticamente a todos os aplicativos novos e, em seguida, o notifica (segurança **Confiável**). Um exemplo de aplicativo modificado é um aplicativo com regras modificadas para permitir automaticamente o acesso do aplicativo à Internet.

Alerta Aplicativo com permissão para acessar a Internet

Se você tiver selecionado segurança **Confiável** nas opções de Configurações de segurança, o Personal Firewall concederá automaticamente acesso à Internet para todos os aplicativos novos e o notificará com um alerta (Figura 4-9).

Figura 4-9. Programa com permissão para acessar a Internet

Veja uma breve descrição do evento e escolha uma das opções a seguir:

- Clique em **Exibir o registro de aplicativos** para obter detalhes sobre o evento com o registro de aplicativos da Internet (consulte *Sobre a página Aplicativos da Internet* na página 89 para obter detalhes).
- Clique em **Desativar este tipo de alerta** para impedir que esse tipo de alerta seja exibido.
- Clique em **Continuar o que eu estava fazendo** se não desejar executar nenhuma ação além do que o Personal Firewall já tenha feito.
- Clique em **Bloquear todo o acesso** para proibir uma conexão à Internet.

Alerta O aplicativo foi modificado

Se você tiver selecionado segurança **Confiável** nas opções de Configurações de segurança, o Personal Firewall concederá automaticamente acesso à Internet a todos os aplicativos modificados. Veja uma breve descrição do evento e escolha uma das opções a seguir:

- Clique em **Exibir o registro de aplicativos** para obter detalhes sobre o evento com o registro de **Aplicativos da Internet** (consulte *Sobre a página Aplicativos da Internet* na página 89 para obter detalhes).
- Clique em **Desativar este tipo de alerta** para impedir que esse tipo de alerta seja exibido.
- Clique em **Continuar o que eu estava fazendo** se não desejar executar nenhuma ação além do que o Personal Firewall já tenha feito.
- Clique em **Bloquear todo o acesso** para proibir uma conexão à Internet.

Alertas azuis

Os alertas azuis contêm informações que não exigem respostas.

- **Tentativa de conexão bloqueada —** Esse alerta é exibido quando o Personal Firewall bloqueia tráfego de rede ou de Internet não desejado. (Segurança Confiável, Padrão ou Rígida)

Alerta Tentativa de conexão bloqueada

Se você tiver selecionado segurança **Confiável**, **Padrão** ou **Rígida**, o Personal Firewall exibirá um alerta (Figura 4-10) quando bloquear tráfego não desejado de rede ou de Internet.

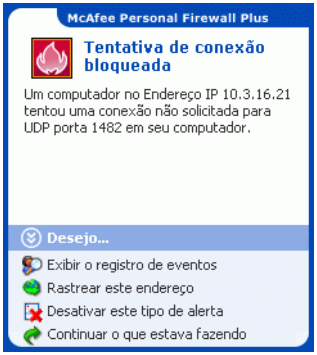


Figura 4-10. Alerta Tentativa de conexão bloqueada

Veja uma breve descrição do evento e escolha uma das opções a seguir:

- Clique em **Exibir o registro de eventos** para obter detalhes sobre o evento com o registro de **Eventos de entrada** do Personal Firewall (consulte *Sobre a página Eventos de entrada* na página 91 para obter detalhes).
- Clique em **Rastrear este endereço** para executar um rastreamento visual dos endereços IP desse evento.
- Clique em **Proibir este endereço** para impedir que o endereço acesse o seu computador. O endereço é adicionado à lista **Endereços IP proibidos**.
- Clique em **Confiar neste endereço** para permitir que o endereço IP acesse o seu computador.
- Clique em **Continuar o que eu estava fazendo** se não desejar executar nenhuma ação além do que o Personal Firewall já tenha feito.

McAfee Privacy Service 5

Bem-vindo ao McAfee® Privacy Service™. O software McAfee Privacy Service oferece proteção avançada para você, sua família, seus dados pessoais e seu computador.

Recursos

Esta versão do McAfee Privacy Service oferece os seguintes recursos:

- Regras de utilização do horário na Internet — Permitem especificar os dias e os horários em que os usuários podem acessar a Internet.
- Filtragem personalizada por palavras-chave — Permite criar regras de palavra-chave para permitir ou bloquear o acesso dos usuários a determinados sites.
- Backup e restauração do Privacy Service — Permite salvar e restaurar as configurações do Privacy Service a qualquer momento.
- Bloqueador de Web bugs — Bloqueia Web bugs (objetos obtidos em um site potencialmente mal-intencionado) para que eles não sejam carregados em páginas navegadas na Web.
- Bloqueador de pop-ups — Evita a exibição de janelas pop-up enquanto você navega na Internet.
- Shredder — O McAfee Shredder protege a sua privacidade eliminando com segurança e rapidez arquivos indesejados.

O administrador

O administrador especifica quais usuários podem acessar a Internet, quando eles podem utilizá-la e o que eles podem fazer na Internet.

NOTA
O administrador é considerado adulto e, portanto, pode acessar todos os sites da Web, mas é solicitado a permitir ou proibir a transmissão de informações identificáveis como pessoais (PII) adicionais.

Configuração do Privacy Service

O Assistente de configuração permite que você crie o administrador, gerencie configurações globais, digite informações pessoais e adicione usuários.

Memorize a sua senha de administrador e a resposta à pergunta de segurança para que possa efetuar logon no Privacy Service. Se você não conseguir fazer logon, não poderá utilizar o Privacy Service e a Internet. Mantenha a sua senha em segredo para que somente você possa alterar as configurações do Privacy Service. Para que alguns sites da Web funcionem adequadamente, é necessário que os cookies estejam ativados. O Privacy Service sempre aceita cookies da McAfee.com.

Recuperação da senha de administrador

Se esquecer a senha de administrador, você poderá acessá-la utilizando as informações de segurança digitadas durante a criação do perfil de administrador.

Para recuperar a senha de administrador:

1. Clique com o botão direito do mouse no ícone da McAfee na área de notificação do Windows, aponte para **McAfee Privacy Service** e selecione **Conectar-se**.
2. Selecione **Administrador** no menu suspenso **Nome do usuário**.
3. Clique em **Esqueceu a senha?**
4. Digite a resposta à pergunta de segurança exibida e clique em **Obter senha**. Uma mensagem é exibida informando a sua senha. Se você esquecer a resposta à pergunta de segurança, desinstale o McAfee Privacy Service no modo de segurança (somente para Windows 2000 e Windows XP).

Remoção do Privacy Service no modo de segurança

Para remover o Privacy Service no modo de segurança:

1. Clique em **Iniciar** e aponte para **Desligar**. A caixa de diálogo **Desligar o Windows** é exibida.
2. Selecione **Desligar** no menu e clique em **OK**.
3. Aguarde até que a mensagem **O computador já pode ser desligado com segurança** seja exibida e desligue o computador.
4. Ligue o computador novamente.
5. Comece imediatamente a pressionar repetidas vezes a tecla **F8** até que o **menu de inicialização do Windows** seja exibido.
6. Selecione **Modo de segurança** e pressione **Enter**.

7 Quando o Windows for iniciado, uma mensagem será exibida, explicando o modo de segurança. Clique em **OK**.

8 Vá para **Adicionar ou remover programas**, encontrado no Painel de controle do Windows. Quando tiver terminado, reinicialize o computador.

9 Reinstale o McAfee Privacy Service e especifique a senha de administrador. Anote a senha especificada.

NOTA
Só é possível remover o Privacy Service no modo de segurança no Windows 2000 ou no Windows XP.

O usuário de inicialização

O usuário de inicialização é automaticamente conectado ao Privacy Service quando o computador é iniciado.

Por exemplo, se um usuário utilizar o computador ou a Internet com mais freqüência do que os outros, você poderá torná-lo o usuário de inicialização. Quando o usuário de inicialização utiliza o computador, ele não precisa se conectar ao Privacy Service.

Se você tiver crianças, também poderá definir o mais novo como usuário de inicialização. Dessa forma, quando um usuário mais velho utilizar o computador, ele poderá efetuar logoff da conta do usuário mais novo e efetuar logon novamente utilizando seu próprio nome de usuário e senha. Isso protege os usuários mais novos contra sites da Web inadequados.

Configuração do administrador como usuário de inicialização

Para configurar o administrador como usuário de inicialização:

1 Na caixa de diálogo **Conecte-se**, selecione o seu nome de usuário no menu suspenso **Nome do usuário**.

2 Digite a sua senha no campo **Senha**.

3 Selecione **Fazer deste o usuário de inicialização** e, em seguida, conecte-se.

Execução do McAfee Privacy Service

Após a instalação do McAfee Privacy Service, o ícone da McAfee é exibido na área de notificação do Windows, que fica localizada próximo ao relógio do sistema. O ícone da McAfee permite acessar o McAfee Privacy Service, o McAfee SecurityCenter e outros produtos McAfee instalados no computador.

Execução e conexão ao Privacy Service

1. Clique com o botão direito do mouse no ícone da McAfee na área de notificação do Windows, aponte para **McAfee Privacy Service** e selecione **Conectar-se**.
2. Selecione o seu nome de usuário no menu suspenso **Nome do usuário**.
3. Digite a senha no campo **Senha**.
4. Clique em **Conectar-se**.

Desativação do Privacy Service

Você deve efetuar logon no Privacy Service como administrador para desativá-lo.

Para desativar o Privacy Service:

- Clique com o botão direito do mouse no ícone da McAfee  , aponte para **McAfee Privacy Service** e selecione **Desconectar-se**.

NOTA
Se **Conectar-se** aparecer no lugar de **Desconectar-se**, é sinal de que você já está desconectado.

Atualização do McAfee Privacy Service

O McAfee SecurityCenter verifica regularmente se há atualizações para o Privacy Service enquanto o computador está em execução e conectado à Internet. Se houver uma atualização disponível, o McAfee SecurityCenter solicitará que você atualize o Privacy Service.

Para verificar manualmente se existem atualizações:

- Clique no ícone **Atualizações**  localizado no painel superior.

Remoção e reinstalação do Privacy Service

Você precisa estar conectado ao Privacy Service como administrador para desinstalar o produto.

NOTA
A remoção do Privacy Service apaga todos os dados do Privacy Service.

Remoção do Privacy Service

Para remover o Privacy Service:

1. Salve todo o seu trabalho e feche todos os aplicativos abertos.
2. Abra o Painel de controle:

- Usuários do Windows 98, Windows Me e Windows 2000 - Selecione **Iniciar**, aponte para **Configurações** e clique em **Painel de controle**.
- Usuários do Windows XP - Na barra de tarefas do Windows, selecione **Iniciar** e clique em **Painel de controle**.

3. Abra a caixa de diálogo **Adicionar ou remover programas**:

- Usuários do Windows 98, Windows Me e Windows 2000 - Clique duas vezes em **Adicionar ou remover programas**.
- Usuários do Windows XP - Clique em **Adicionar ou remover programas**.

4. Selecione McAfee Privacy Service na lista de programas e clique em **Alterar/remover**.
5. Quando for solicitado, clique em **Sim** para confirmar a operação.
6. Ao ser solicitado a reiniciar o sistema, clique em **Fechar**. O computador será reiniciado para concluir o processo de desinstalação.

Instalação do Privacy Service

Para instalar o Privacy Service:

1. Vá até o site da McAfee e navegue até a página do **Privacy Service**.
2. Clique no link **Download** na página do **Privacy Service**.
3. Clique em **Sim** em todas as mensagens que perguntarem se você deseja fazer download de arquivos do site da McAfee.
4. Clique em **Iniciar instalação** na janela de instalação do Privacy Service.
5. Quando o download estiver concluído, clique em **Reiniciar** para reiniciar o computador. Uma alternativa é clicar em **Fechar** se desejar salvar algum trabalho ou fechar algum programa e, em seguida, reiniciar o computador normalmente. É preciso reiniciar o computador para que o Privacy Service funcione adequadamente.

Após o computador ser reiniciado, será necessário criar o administrador novamente.

Para adicionar usuários, você deve conectar-se ao Privacy Service como administrador.

1. Clique com o botão direito do mouse no ícone da McAfee na área de notificação do Windows.
2. Aponte para **McAfee Privacy Service** e selecione **Gerenciar usuários**. A caixa de diálogo **Selecionar usuário** será exibida.
3. Clique em **Adicionar** e digite o nome do novo usuário no campo **Nome do usuário**.

Definição da senha

1. Digite uma senha no campo **Senha**. A senha pode conter até 50 caracteres, entre números e letras maiúsculas e minúsculas.
2. Digite a senha novamente no campo **Confirme a senha**.
3. Selecione **Fazer deste o usuário de inicialização** para que esse seja o usuário de inicialização.
4. Clique em **Avançar**.

Ao atribuir senhas, considere a faixa etária do usuário. Por exemplo, ao atribuir uma senha a uma criança pequena, crie uma senha simples. Ao atribuir uma senha a um adolescente ou adulto, crie senhas mais complexas.

Definição da faixa etária

Selecione a configuração de faixa etária apropriada e clique em **Avançar**.

Definição do bloqueador de cookies

Selecione a opção apropriada e clique em **Avançar**.

- **Rejeitar todos os cookies** — Torna os cookies ilegíveis para os sites da Web que os enviaram. Para que alguns sites da Web funcionem adequadamente, é necessário ativar os cookies.
- **Perguntar ao usuário se ele aceitará cookies** — Permite decidir se aceitará ou rejeitará cookies de acordo com cada caso. O Privacy Service informará quando o site da Web a ser exibido deseja enviar um cookie ao seu computador. Depois que você se decidir, não será mais perguntado sobre esse cookie novamente.

- **Aceitar todos os cookies** — Permite que os sites da Web leiam os cookies que enviam ao seu computador.

  NOTA
  Para que alguns sites da Web funcionem adequadamente, é necessário que os cookies estejam ativados.

  O Privacy Service sempre aceita cookies da McAfee.

Definição dos limites de horário para uso da Internet

Para conceder uso irrestrito da Internet:

1. Selecione **Usar a Internet em qualquer horário**.
2. Clique em **Criar**. O novo usuário é exibido na lista **Selecionar usuário**.

Para conceder uso limitado da Internet:

1. Selecione **Restringir uso da Internet** e clique em **Editar**.
2. Na página **Limites de horário na Internet**, percorra a grade de horários para selecionar o horário e o dia em que os usuários podem acessar a Internet. Você pode especificar os limites de horários em intervalos de trinta minutos. As partes verdes da grade são os períodos em que o usuário pode acessar a Internet. As partes vermelhas indicam quando o usuário não pode acessar a Internet. Se um usuário tentar utilizar a Internet quando não for permitido, o Privacy Service exibirá uma mensagem informando que o usuário não tem permissão para utilizar a Internet nesse horário. Para modificar os períodos em que o usuário pode acessar a Internet, percorra as partes verdes da grade.
3. Clique em **Concluído**.
4. Clique em **Criar**. O novo usuário é exibido na lista **Selecionar usuário**. Se um usuário tentar utilizar a Internet quando não for permitido, o Privacy Service exibirá uma mensagem informando que o usuário não tem permissão para utilizar a Internet nesse horário.

Para proibir o uso da Internet:

Selecione **Restringir uso da Internet** e clique em **Criar**. Quando o usuário utiliza o computador, ele é solicitado a conectar-se ao Privacy Service. Ele poderá utilizar o computador, mas não a Internet.

Criação de permissões para sites com palavras-chave

O Privacy Service mantém uma lista padrão de palavras-chave e regras correspondentes, que determina se um usuário de uma determinada faixa etária pode ou não visitar um site que contenha essa palavra-chave.

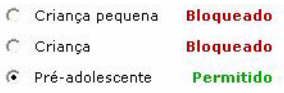
O administrador pode adicionar suas próprias palavras-chave permitidas ao banco de dados do Privacy Service e associá-las a determinadas faixas etárias. As regras de palavras-chave adicionadas pelo administrador substituem as regras associadas a qualquer palavra-chave correspondente no banco de dados padrão do Privacy Service. Um administrador pode usar palavras-chave existentes ou especificar novas palavras-chave para associar a determinadas faixas etárias.

Para criar permissões para sites com palavras-chave:

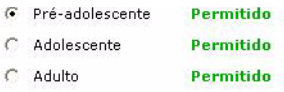
1. Clique com o botão direito do mouse no ícone da McAfee na área de notificação do Windows, aponte para **Privacy Service** e selecione **Opções**.
2. Clique na guia **Palavras-chave**.
3. No campo **Pesquisa de palavra**, digite uma palavra para uma faixa etária.
4. No painel **Permissões**, selecione a faixa etária a ser associada à palavra. As faixas etárias são:
   - Criança pequena
   - Criança
   - Pré-adolescente
   - Adolescente
   - Adulto

   A palavra-chave e sua faixa etária selecionada aparecem na **Lista de palavras**.

   As faixas etárias que aparecem acima da faixa associada têm bloqueado seu acesso a sites que contenham a palavra.



   A faixa etária à qual a palavra foi atribuída e as faixas que aparecem abaixo dela podem acessar sites que contenham a palavra.



Para modificar permissões de sites existentes:

1. Clique com o botão direito do mouse no ícone da McAfee na área de notificação do Windows, aponte para **Privacy Service** e selecione **Opções**.
2. Clique na guia **Palavras-chave**.
3. No campo **Pesquisa de palavra**, digite uma palavra que você queira modificar e clique em **Pesquisar**. A palavra aparecerá se já existir no banco de dados do Privacy Service.

Para editar usuários, você deve conectar-se ao Privacy Service como administrador.

Alteração de senhas

1. Selecione o usuário cujas informações serão alteradas e clique em **Editar**.
2. Selecione **Senha** e digite a nova senha do usuário no campo **Nova senha**. A senha pode conter até 50 caracteres, entre números e letras maiúsculas e minúsculas.
3. Digite a mesma senha no campo **Confirme a senha** e clique em **Aplicar**.
4. Clique em **OK** na caixa de diálogo de confirmação.

> **NOTA**
> O administrador pode alterar a senha de um usuário sem saber a senha atual.

Alteração das informações de um usuário

1. Selecione o usuário cujas informações serão alteradas e clique em **Editar**.
2. Selecione **Informações do usuário**.
3. Digite o novo nome de usuário no campo **Novo nome de usuário**.
4. Clique em **Aplicar** e, em seguida, clique em **OK** na caixa de diálogo de confirmação.
5. Para restringir o acesso de um usuário aos sites da lista **Sites da Web permitidos**, selecione **Restringir o acesso deste usuário aos sites da Web que constam na lista "Sites da Web permitidos"**.

Alteração da configuração do bloqueador de cookies

1. Selecione o usuário cujas informações serão alteradas e clique em **Editar**.
2. Selecione **Cookies** e escolha a opção apropriada.
   - **Rejeitar todos os cookies** — Torna os cookies ilegíveis para os sites da Web que os enviaram. Para que alguns sites da Web funcionem adequadamente, é necessário ativar os cookies.
   - **Perguntar ao usuário se ele aceitará cookies** — Permite decidir se aceitará ou rejeitará cookies de acordo com cada caso. O Privacy Service informará quando o site da Web a ser exibido deseja enviar um cookie ao seu computador. Depois que você se decidir, não será mais perguntado sobre esse cookie novamente.
   - **Aceitar todos os cookies** — Permite que os sites da Web leiam os cookies que enviam ao seu computador.
3. Clique em **Aplicar** e, em seguida, clique em **OK** na caixa de diálogo de confirmação.

Edição da lista de cookies aceitos e rejeitados

1. Selecione **Perguntar ao usuário se ele aceitará cookies** e clique em **Editar** para especificar quais sites da Web têm permissão para ler cookies.
2. Especifique a lista que será modificada selecionando **Sites da Web que podem definir cookies** ou **Sites da Web que não podem definir cookies**.
3. No campo **http://**, digite o endereço do site da Web cujos cookies serão aceitos ou rejeitados.
4. Clique em **Adicionar**. O site da Web será exibido na lista de sites da Web.
5. Clique em **Concluído** ao terminar de fazer as alterações.

NOTA
Para que alguns sites da Web funcionem adequadamente, é necessário que os cookies estejam ativados.

O Privacy Service sempre aceita cookies da McAfee.

Alteração da faixa etária

1. Selecione o usuário cujas informações serão alteradas e clique em **Editar**.
2. Selecione **Faixa etária**.
3. Selecione uma nova faixa etária para o usuário e clique em **Aplicar**.
4. Clique em **OK** na caixa de diálogo de confirmação.

Alteração dos limites de horário para uso da Internet

1. Selecione o usuário cujas informações serão alteradas e clique em **Editar**.
2. Selecione **Limites de horário** e faça o seguinte:

Para permitir acesso ilimitado à Internet:

1. Selecione **Usar a Internet em qualquer horário** e clique em **Aplicar**.
2. Clique em **OK** na caixa de diálogo de confirmação.

Para restringir o acesso à Internet:

1. Selecione **Restringir uso da Internet** e clique em **Editar**.
2. Na página **Limites de horário na Internet**, selecione um quadrado verde ou vermelho e, em seguida, percorra a grade de horários para alterar os horários e os dias em que os usuários podem acessar a Internet.
   Você pode especificar os limites de horários em intervalos de trinta minutos. As partes verdes da grade são os períodos em que o usuário pode acessar a Internet. As partes vermelhas indicam quando o usuário não pode acessar a Internet. Se um usuário tentar utilizar a Internet quando não for permitido, o Privacy Service exibirá uma mensagem informando que o usuário não tem permissão para utilizar a Internet nesse horário.
3. Clique em **Aplicar**.
4. Na página **Limites de horários**, clique em **OK**.
5. Na caixa de diálogo de confirmação do McAfee Privacy Service, clique em **OK**.

Alteração do usuário de inicialização

O administrador pode alterar o usuário de inicialização a qualquer momento. Se já existir um usuário de inicialização, não será necessário desmarcá-lo.

1. Selecione o usuário que você deseja designar como usuário de inicialização e clique em **Editar**.
2. Selecione **Informações do usuário**.
3. Selecione **Fazer deste o usuário de inicialização**.
4. Clique em **Aplicar** e, em seguida, clique em **OK** na caixa de diálogo de confirmação.

NOTA
Também é possível atribuir um usuário de inicialização a partir da caixa de diálogo **Conecte-se**. Para obter mais informações, consulte *O usuário de inicialização* na página 115

Remoção de usuários

1. Selecione o usuário a ser removido e clique em **Remover**.
2. Clique em **Sim** na caixa de diálogo de confirmação.
3. Feche a janela Privacy Service ao concluir as alterações.

Para configurar as opções do Privacy Service, é necessário conectar-se ao Privacy Service como administrador.

Bloqueio de sites da Web

1. Clique em **Opções** e selecione **Lista de bloqueados**.
2. No campo **http://**, digite o URL do site da Web a ser bloqueado e clique em **Adicionar**. O site da Web será exibido na lista **Sites da Web bloqueados**.

NOTA
Os usuários (incluindo os administradores) que pertencem ao nível Adulto podem acessar todos os sites da Web, mesmo que estes constem na lista **Sites da Web bloqueados**. Para testar os sites da Web bloqueados, os administradores devem efetuar logon como usuários não-adultos.

Permissão de sites da Web

O administrador pode permitir que todos os usuários acessem determinados sites da Web. Isso prevalece sobre as configurações padrão do Privacy Service e os sites adicionados à lista de sites bloqueados.

1. Clique em **Opções** e selecione **Lista de permitidos**.
2. No campo **http://**, digite o URL do site da Web a ser permitido e clique em **Adicionar**. O site da Web será exibido na lista **Sites da Web permitidos**.

Bloqueio de informações

O administrador pode impedir que outros usuários enviem informações pessoais específicas pela Internet (mas o administrador pode enviar essas informações).

Quando o Privacy Service detecta informações de identificação pessoal (PII) em algo prestes a ser enviado, acontece o seguinte:

- Se você for um administrador, será avisado e poderá decidir se enviará ou não as informações.
- Se o usuário conectado não for o administrador, as informações bloqueadas serão substituídas por *MFEMFEMFE*. Por exemplo, se você enviar o e-mail *Lance Armstrong ganha viagem* e Armstrong estiver definido como uma informação pessoal a ser bloqueada, o e-mail enviado será *Lance MFEMFEMFE ganha viagem*.

Acréscimo de informações

1. Clique em **Opções** e selecione **Bloquear informações**.
2. Clique em **Adicionar**. O menu suspenso **Selecionar tipo** será exibido.
3. Selecione o tipo de informações a serem bloqueadas.
4. Digite as informações nos campos apropriados e clique em **OK**. As informações digitadas são exibidas na lista.

Edição de informações

1. Clique em **Opções** e selecione **Bloquear informações**.
2. Selecione as informações a serem editadas e clique em **Editar**.
3. Faça as alterações apropriadas e clique em **OK**. Se não for necessário alterar as informações, clique em **Cancelar**.

Remoção de informações pessoais

1. Clique em **Opções** e selecione **Bloquear informações**.
2. Selecione as informações a serem removidas e clique em **Remover**.
3. Clique em **Sim** na caixa de diálogo de confirmação.

Bloqueio de Web bugs

Os Web bugs são pequenos arquivos gráficos que podem enviar mensagens a terceiros, incluindo o rastreamento de seus hábitos de navegação na Internet ou a transmissão de informações pessoais a um banco de dados externo. As pessoas que recebem mensagens dos Web bugs podem usar essas informações para criar perfis de usuário.

Para evitar que os Web bugs sejam carregados em páginas navegadas na Web, selecione **Bloquear Web Bugs neste computador**.

Bloqueio de anúncios

Geralmente, os anúncios são gráficos transmitidos por um domínio de terceiros a uma página da Web ou janela pop-up. O Privacy Service não bloqueia os anúncios fornecidos pelo mesmo domínio da página da Web do host.

Pop-ups são janelas secundárias do navegador que apresentam anúncios indesejados, exibidos automaticamente quando você visita um site da Web. O Privacy Service bloqueia somente os pop-ups exibidos automaticamente quando uma página da Web é carregada. O Privacy Service não bloqueia pop-ups iniciados com um clique em um link. Para exibir um pop-up bloqueado, mantenha a tecla CTRL pressionada e atualize a página da Web.

Configure o Privacy Service para bloquear anúncios e pop-ups quando você estiver utilizando a Internet.

1. Clique em **Opções** e selecione **Bloquear anúncios**.
2. Selecione a opção apropriada.
   - **Bloquear anúncios neste computador** — Bloqueia anúncios enquanto você estiver utilizando a Internet.
   - **Bloquear pop-ups neste computador** — Bloqueia pop-ups enquanto você estiver utilizando a Internet.
3. Clique em **Aplicar** e, em seguida, clique em **OK** na caixa de diálogo de confirmação.

Para desativar o bloqueio de pop-ups, clique com o botão direito do mouse na página da Web, aponte para **Bloqueador de pop-ups da McAfee** e desmarque **Ativar bloqueador de pop-ups**.

Permissão para cookies de sites da Web específicos

Se você bloquear cookies ou pedir para ser avisado antes que eles sejam aceitos e perceber que determinados sites da Web não funcionam adequadamente, configure o Privacy Service para permitir que o site leia cookies.

1. Clique em **Opções** e selecione **Cookies**.
2. No campo **http://**, digite o endereço do site da Web que precisa ler os cookies e clique em **Adicionar**. O endereço será exibido na lista **Aceitar cookies de sites da Web**.

Para exibir o registro de eventos, é necessário conectar-se ao Privacy Service como administrador. Em seguida, selecione **Registro de eventos** e clique em qualquer entrada do registro para exibir seus detalhes. Para salvar ou exibir um registro salvo, selecione a guia **Registros salvos**.

Data e hora

Por padrão, o registro de eventos exibe as informações em ordem cronológica, com os eventos mais recentes na parte superior. Se as entradas do registro de eventos não estiverem em ordem cronológica, clique no título Data e hora.

A data é exibida no formato mês/dia/ano e a hora no formato 6:00/18:00, por exemplo.

Usuário

O usuário é a pessoa que estava conectada e usando a Internet quando o Privacy Service registrou o evento.

Resumo

Os resumos exibem uma descrição concisa e breve do que o Privacy Service está fazendo para proteger os usuários e do que os usuários estão fazendo na Internet.

Detalhes do evento

O campo **Detalhes do evento** exibe detalhes da entrada.

Salvamento do registro atual

A página **Registro atual** exibe informações sobre as últimas ações administrativas e dos usuários. Essas informações podem ser salvas para serem exibidas posteriormente.

Para salvar o registro de eventos atual

1. Conecte-se ao Privacy Service como administrador.
2. Selecione **Registro de eventos**.
3. Na página **Registro atual**, clique em **Salvar registro**.
4. No campo **Nome do arquivo**, digite o nome do arquivo de registro.
5. Clique em **Salvar**.

Exibição de registros salvos

A página **Registro atual** exibe informações sobre as últimas ações administrativas e dos usuários. Essas informações podem ser salvas para serem exibidas posteriormente.

Para exibir um registro salvo

1. Conecte-se ao Privacy Service como administrador.
2. Selecione **Registro de eventos**.
3. Na página **Registro atual**, clique em **Abrir registro**.
4. Na caixa de diálogo **Selecione o registro salvo que será exibido**, selecione o arquivo de backup do banco de dados e clique em **Abrir**.

Para acessar os utilitários, conecte-se ao Privacy Service como administrador e clique em **Utilitários**.

Para remover arquivos, pastas ou todo o conteúdo de um disco, clique em **McAfee Shredder**. Para salvar as configurações do banco de dados do Privacy Service, clique em **Backup**. Para restaurar as suas configurações, clique em **Restaurar**.

Eliminação permanente de arquivos com o McAfee Shredder

O McAfee Shredder protege a sua privacidade eliminando, com segurança e rapidez, arquivos indesejados.

Os arquivos excluídos podem ser recuperados no seu computador até mesmo depois do esvaziamento da Lixeira. Quando um arquivo é excluído, o Windows simplesmente marca esse espaço na unidade de disco para indicar que ele não está mais sendo utilizado, mas o arquivo continua presente.

Por que o Windows deixa vestígios do arquivo?

Para excluir um arquivo permanentemente, é preciso sobrescrever várias vezes o arquivo existente com novos dados. Se o Microsoft Windows excluísse os arquivos com segurança, cada operação de arquivo seria muito lenta. A destruição de um documento nem sempre impede que ele seja recuperado, pois alguns programas fazem cópias ocultas temporárias de documentos abertos. Se você destruiu apenas os documentos exibidos no Explorer, ainda pode haver cópias temporárias desses documentos. Recomendamos que você destrua periodicamente o conteúdo do espaço livre na unidade de disco para garantir que as cópias temporárias sejam excluídas permanentemente.

NOTA
Com ferramentas de análise forense, registros de impostos, currículos ou outros documentos excluídos podem ser recuperados.

O que o McAfee Shredder apaga

O McAfee Shredder permite apagar permanentemente e com segurança:

- Um ou mais arquivos ou pastas
- Um disco inteiro
- Os rastros deixados pela navegação na Web

Eliminação permanente de arquivos no Windows Explorer

Para destruir um arquivo pelo Windows Explorer:

1. Abra o Windows Explorer e selecione os arquivos a serem destruídos.
2. Clique com o botão direito do mouse no item selecionado, aponte para **Enviar para** e selecione **McAfee Shredder**.

Esvaziamento da Lixeira do Windows

Se os arquivos se encontram na Lixeira, o McAfee Shredder oferece um método mais seguro para esvaziá-la.

Para destruir o conteúdo da Lixeira:

1. Na área de trabalho do Windows, clique com o botão direito do mouse na Lixeira.
2. Selecione **Destruir a Lixeira** e siga as instruções da tela.

Personalização das configurações do Shredder

Você pode:

- Especificar o número de destruições.
- Mostrar uma mensagem de aviso ao destruir arquivos.
- Verificar se há erros no disco rígido antes de destruir.
- Adicionar o McAfee Shredder ao menu **Enviar para**.
- Colocar um ícone do Shredder na área de trabalho do Windows.

Para personalizar as configurações do Shredder, abra o McAfee Shredder, clique em **Propriedades** e siga as instruções da tela.

Backup do banco de dados do Privacy Service

É possível restaurar o banco de dados do Privacy Service de duas maneiras. Se o banco de dados estiver corrompido ou tiver sido excluído, o Privacy Service pedirá que você restaure seu banco de dados. Também é possível restaurar as configurações do banco de dados durante a execução do Privacy Service.

1. Clique em **Utilitários** e selecione **Backup**.
2. Clique em **Procurar** para selecionar um local para o arquivo de banco de dados e, em seguida, clique em **OK**.
3. Digite uma senha no campo **Senha**.
4. Digite novamente a senha no campo **Confirme a senha** e clique em **Backup**.
5. Clique em **OK** na caixa de diálogo de confirmação.
6. Feche a janela do Privacy Service ao terminar.

> **NOTA**
> Mantenha essa senha em segredo e procure não esquecê-la. Sem a senha, não será possível restaurar as configurações do Privacy Service.

Restauração do banco de dados de backup

1 O Privacy Service oferece duas maneiras de restaurar as configurações originais:

- Carregar o arquivo de backup do banco de dados depois que o Privacy Service solicitar a restauração das configurações porque o banco de dados está corrompido ou foi excluído.
- Carregar o arquivo de backup do banco de dados durante a execução do Privacy Service.

Para restaurar as configurações do Privacy Service ao ser solicitado:

1 Clique em **Procurar** para localizar o arquivo.

2 Digite a senha no campo **Senha**.

3 Clique em **Restaurar**.
Se você não fez backup do banco de dados do Privacy Service, esqueceu a senha de backup ou a restauração do banco de dados não está funcionando, remova e reinstale o Privacy Service.

Para restaurar as configurações do Privacy Service enquanto o serviço estiver sendo executado:

1 Clique na guia **Utilitários**.

2 Clique em **Restaurar**.

3 Clique em **Procurar** e digite o caminho e o nome do arquivo de backup.

4 Clique em **Abrir**.

5 Digite a senha no campo **Senha**.

6 Clique em **Restaurar** e, em seguida, clique em **OK** na caixa de diálogo de confirmação do McAfee Privacy Service.

Estas instruções não se aplicam ao administrador.

Você pode alterar a sua senha e o seu nome de usuário. Recomendamos que você altere a senha depois que o administrador a conceder. Recomendamos também alterá-la uma vez por mês ou se suspeitar que alguém a conhece. Isso ajudará a evitar que outras pessoas utilizem a Internet com seu nome de usuário.

Alteração da sua senha

1. Clique com o botão direito do mouse no ícone da McAfee, aponte para **McAfee Privacy Service** e selecione **Opções**.
2. Clique em **Senha** e digite a senha antiga no campo **Senha antiga**.
3. Digite a nova senha no campo **Nova senha**.
4. Digite a nova senha novamente no campo **Confirme a senha** e clique em **Aplicar**.
5. Clique em **OK** na caixa de diálogo de confirmação. Agora você tem uma nova senha.

Alteração do seu nome de usuário

1. Clique com o botão direito do mouse no ícone da McAfee, aponte para **McAfee Privacy Service** e selecione **Opções**.
2. Clique em **Informações do usuário**.
3. Digite o novo nome de usuário no campo **Novo nome de usuário** e clique em **Aplicar**.
4. Clique em **OK** na caixa de diálogo de confirmação. Agora você tem um novo nome de usuário.

Limpeza do cache

Recomendamos a limpeza do cache para evitar que crianças acessem as páginas da Web visitadas recentemente. Para limpar o cache, faça o seguinte:

1. Abra o Internet Explorer.
2. No menu **Ferramentas**, clique em **Opções da Internet**. A caixa de diálogo **Opções da Internet** será exibida.
3. Na seção **Arquivos de Internet temporários**, clique em **Excluir arquivos**. A caixa de diálogo **Excluir arquivos** será exibida.
4. Selecione **Excluir todo o conteúdo off-line** e clique em **OK**.
5. Clique em **OK** para fechar a caixa de diálogo **Opções da Internet**.

Aceitação de cookies

Essa opção estará disponível somente se o administrador permitir aceitar ou rejeitar os cookies interceptados.

Se acessar sites da Web que exijam cookies, você poderá permitir que esses sites leiam cookies.

1. Clique com o botão direito do mouse no ícone da McAfee, aponte para **McAfee Privacy Service** e selecione **Opções**.
2. Clique em **Cookies aceitos**.
3. Digite o URL do site da Web no campo **http://** e clique em **Adicionar**. O site será exibido na lista **Site da Web**.

Se for necessário remover um site da Web da lista:

1. Selecione o URL do site na lista **Site da Web**.
2. Clique em **Remover** e, depois, clique em **Sim** na caixa de diálogo de confirmação.

Rejeição de cookies

Essa opção estará disponível somente se o administrador permitir aceitar ou rejeitar os cookies interceptados.

Se você acessar sites da Web que não exijam cookies, poderá rejeitar os cookies sem ser avisado.

1. Clique com o botão direito do mouse no ícone da McAfee, aponte para **McAfee Privacy Service** e selecione **Opções**.
2. Clique em **Cookies rejeitados**.
3. Digite o URL do site da Web no campo **http://** e clique em **Adicionar**. O site da Web será exibido na lista **Site da Web**.

Se for necessário remover um site da Web da lista:

1. Selecione o URL do site na lista **Site da Web**.
2. Clique em **Remover** e, depois, clique em **Sim** na caixa de diálogo de confirmação.

McAfee SpamKiller 6

Bem-vindo ao McAfee SpamKiller.

O software McAfee SpamKiller ajuda a impedir que mensagens de spam entrem na sua caixa de entrada de e-mail. Ele oferece os seguintes recursos:

Opções do usuário

- Bloquear spam utilizando filtros e colocar spam em quarentena fora da caixa de entrada
- Exibir mensagens bloqueadas e aceitas
- Monitorar e filtrar várias contas de e-mail
- Importar endereços de amigos para a lista de amigos
- Revidar contra remetentes de spam (relatar spam, reclamar de spam, criar filtros personalizados)
- Impedir que crianças vejam mensagens de spam
- Bloqueio com um só clique e recuperação com um só clique
- Suporte a conjuntos de caracteres de dois bytes
- Suporte multiusuário (para Windows 2000 e Windows XP)

Filtragem

- Atualizar filtros automaticamente
- Criar filtros personalizados para bloquear e-mails que contenham, basicamente, imagens, texto invisível ou formatação inválida
- Mecanismo de filtragem central em várias camadas
- Filtro contra ataques de dicionário
- Filtragem adaptável em vários níveis
- Filtros de segurança

Recursos

Esta versão do SpamKiller oferece os seguintes recursos:

- Filtragem - as opções avançadas de filtragem oferecem novas técnicas, incluindo suporte à filtragem de metacaracteres e à identificação de texto de lixo eletrônico.
- Phishing – o plug-in AntiPhishing do navegador, na barra de ferramentas do Internet Explorer, identifica e bloqueia facilmente sites da Web de phishing em potencial.
- Integração com o Microsoft Outlook e com o Outlook Express – a barra de ferramentas fornece uma pasta, no cliente de e-mail, para bloquear o spam diretamente.
- Instalação - instalação e configuração simplificadas. A detecção automática da conta garante facilidade na instalação e na configuração, e integração com as contas de e-mail existentes.
- Atualizações - as atualizações automáticas são executadas silenciosamente em segundo plano, sempre vigilantes para minimizar a exposição a novas ameaças de spam.
- Interface - interface de usuário intuitiva para manter o computador livre de spam.
- Suporte - suporte técnico gratuito com troca de mensagens instantâneas e e-mail ao vivo, para um atendimento ao cliente fácil, imediato e em tempo real.
- Processamento de mensagens de spam - por padrão, as mensagens de spam são marcadas como [SPAM] e colocadas na pasta do SpamKiller no Outlook e no Outlook Express ou na caixa de entrada. As mensagens marcadas também são exibidas na página **E-mail aceito**.

Compreensão do painel superior

Os ícones a seguir são exibidos no painel superior de cada página do SpamKiller:

- Clique em **Alternar usuário**  para efetuar logon como outro usuário.

  NOTA
  Alternar usuário só estará disponível se o computador estiver executando Windows 2000 ou Windows XP, se vários usuários tiverem sido adicionados ao SpamKiller e se você tiver efetuado logon no SpamKiller como administrador.

- Clique em **Suporte**  para abrir a página de suporte on-line da McAfee, que fornece tópicos relevantes sobre o SpamKiller e outros produtos da McAfee, respostas para perguntas freqüentes e muito mais. É necessário estar conectado à Internet para acessar a página de suporte.

- Clique em **Ajuda** para abrir a Ajuda on-line, que fornece instruções detalhadas sobre como configurar e usar o SpamKiller.

Compreensão da página Resumo

Clique na guia **Resumo** para abrir a página **Resumo** (Figura 6-1).

- **Visão geral do status do SpamKiller** - indica se a filtragem está ativada, quando uma lista de amigos foi atualizada pela última vez e o número de mensagens de spam recebidas hoje. Aqui é possível desativar ou ativar a filtragem do SpamKiller, atualizar listas de amigos e abrir a página **E-mail bloqueado**.
- **E-mails mais recentes que foram identificados como spam e bloqueados** - as últimas mensagens de spam que o SpamKiller bloqueou (removidas da caixa de entrada).
- **Visão geral do e-mail** - exibe o número total de e-mails, spam (mensagens bloqueadas) e a porcentagem do total de spam recebido.
- **Spam recente** - uma análise do tipo de spam recebido nos últimos 30 dias.

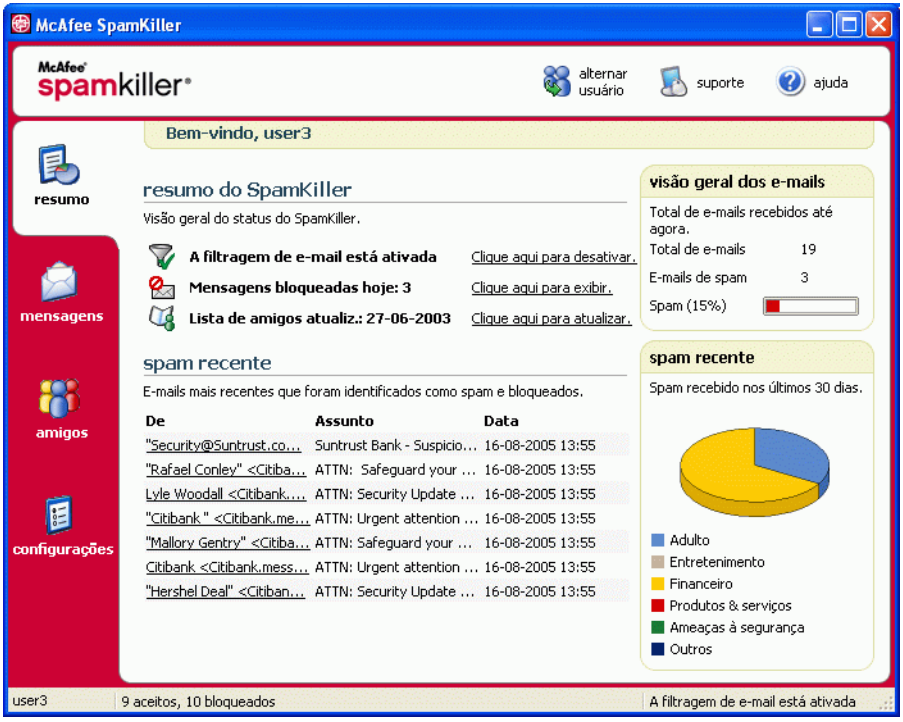


Figura 6-1. Página Resumo

Integração com o Microsoft Outlook e com o Outlook Express

Você pode usar os principais recursos do SpamKiller diretamente no Outlook Express 6.0, no Outlook 98, no Outlook 2000 e no Outlook XP, selecionando o menu ou a barra de ferramentas do SpamKiller.

A barra de ferramentas do SpamKiller é exibida à direita das barras de ferramentas padrão do Outlook e do Outlook Express. Se ela não estiver visível, expanda a janela do aplicativo de e-mail ou clique nas setas para exibir mais barras de ferramentas.

Quando a barra de ferramentas do SpamKiller for exibida pela primeira vez no aplicativo de e-mail, você poderá usar os comandos da barra de ferramentas somente em mensagens novas. Os e-mails de spam existentes devem ser excluídos manualmente.

Desativação do SpamKiller

Você pode desativar o SpamKiller e impedir a filtragem de e-mails.

Para desativar a filtragem:

Clique com o botão direito do mouse no ícone da McAfee , aponte para **SpamKiller** e, em seguida, clique em **Desativar**. Ou clique na guia **Resumo** e, em seguida, clique em **Clique aqui para desativar**.

Para ativar a filtragem:

Clique com o botão direito do mouse no ícone da McAfee, aponte para **SpamKiller** e, em seguida, clique em **Ativar**. Ou clique na guia **Resumo** e, em seguida, clique em **Clique aqui para ativar**.

Acréscimo de contas de e-mail

Você pode adicionar as seguintes contas de e-mail:

- Conta de e-mail padrão (POP3) - a maioria dos usuários domiciliares utiliza esse tipo de conta
- Conta MSN/Hotmail - contas MSN/Hotmail baseadas na Web

> **NOTA**
> Se o computador executa Windows 2000 ou Windows XP e você pretende adicionar vários usuários ao SpamKiller, adicione os usuários primeiro para poder adicionar as contas de e-mail aos respectivos perfis. Para obter mais informações, consulte *Acréscimo de usuários* na página 146. Se você adicionar vários usuários ao SpamKiller, a conta será adicionada ao perfil do usuário que estiver conectado ao SpamKiller no momento.

Acréscimo de uma conta de e-mail

1. Clique na guia **Configurações** para abrir a página **Configurações** (Figura 6-2) e, em seguida, clique em **Contas de e-mail**. A caixa de diálogo **Contas de e-mail** é exibida com todas as contas de e-mail adicionadas ao SpamKiller.

   > **NOTA**
   > Se vários usuários tiverem sido adicionados ao SpamKiller, a lista exibirá as contas de e-mail do usuário que estiver conectado ao SpamKiller no momento.

2. Clique em **Adicionar**. O assistente de contas de e-mail será exibido.

3 Siga as instruções das caixas de diálogo exibidas.

Se você adicionar uma conta MSN/Hotmail, o SpamKiller procurará uma lista de endereços MSN/Hotmail para importar para a sua **Lista de amigos pessoais**.

Figura 6-2. Página Configurações

Direcionamento do seu cliente de e-mail para o SpamKiller

Se você adicionar uma conta que o SpamKiller não detecte (a conta não aparece na caixa de diálogo **Selecionar conta**) ou se você quiser ler o seu e-mail MSN/Hotmail como uma conta POP3 no SpamKiller, direcione o seu cliente de e-mail para o SpamKiller alterando o servidor de recebimento de e-mail.

Por exemplo, se o seu servidor de recebimento de e-mail é “mail.mcafee.com”, mude-o para “localhost”.

Exclusão de contas de e-mail

Exclua uma conta de e-mail do SpamKiller caso não queira mais que ele a filtre.

Exclusão de uma conta de e-mail do SpamKiller

1 Clique na guia **Configurações** e selecione **Contas de e-mail**. A caixa de diálogo **Contas de e-mail** é exibida com todas as contas de e-mail adicionadas ao SpamKiller.

> **NOTA**
> Se vários usuários tiverem sido adicionados ao SpamKiller, a lista exibirá as contas de e-mail do usuário que estiver conectado ao SpamKiller no momento.

2 Selecione uma conta e, em seguida, clique em **Excluir**.

Edição de propriedades da conta de e-mail

É possível editar informações sobre uma conta de e-mail adicionada ao SpamKiller. Por exemplo, altere o endereço de e-mail, a descrição da conta, as informações do servidor, a freqüência com que o SpamKiller verifica se há spam na conta e como o computador se conecta à Internet.

Contas POP3

Edição de contas POP3

1 Clique na guia **Configurações** e, em seguida, clique em **Contas de e-mail**. A caixa de diálogo **Contas de e-mail** é exibida com todas as contas de e-mail adicionadas ao SpamKiller.

> **NOTA**
> Se vários usuários tiverem sido adicionados ao SpamKiller, a lista exibirá as contas de e-mail do usuário que estiver conectado ao SpamKiller no momento.

2 Selecione uma conta POP3 e, em seguida, clique em **Editar**.

3 Clique na guia **Geral** para editar a descrição da conta e o endereço de e-mail.

- **Descrição** - descrição da conta. Digite qualquer informação nessa caixa.
- **Endereço de e-mail** - endereço de e-mail da conta.

4 Clique na guia **Servidores** para editar as informações do servidor.

- **E-mails recebidos** - nome do servidor que recebe e-mails.
- **Nome do usuário** - nome de usuário usado para acessar a conta. Conhecido também como nome da conta.
- **Senha** - senha usada para acessar a conta.
- **E-mails enviados** - nome do servidor que envia e-mails. Clique em **Mais** para editar os requisitos de autenticação do servidor de saída.

5 Clique na guia **Verificando** para editar a freqüência com que o SpamKiller deve verificar se há spam na conta:

a Selecione **Verificar a cada** ou **Verificar diariamente às** e, em seguida, digite uma hora na caixa correspondente. Se você digitar o número zero, o SpamKiller verificará a conta apenas ao se conectar.

b Selecione períodos adicionais para o SpamKiller filtrar a conta:

Verificar ao iniciar - se você tem uma conexão direta e deseja que o SpamKiller verifique a conta sempre que o computador for iniciado.

Verificar quando uma conexão for discada - se você tem uma conexão discada e deseja que o SpamKiller verifique a conta sempre que você se conectar à Internet.

6 Clique na guia **Conexão** para especificar como o SpamKiller discará uma conexão de Internet para verificar se há novas mensagens a serem filtradas na caixa de entrada.

- **Nunca discar uma conexão** - o SpamKiller não disca automaticamente uma conexão para você. Primeiro, é necessário iniciar manualmente a conexão discada.
- **Discar quando necessário** - uma conexão de Internet não está disponível e o SpamKiller tenta se conectar automaticamente usando a conexão de Internet discada padrão.
- **Discar sempre** - o SpamKiller tenta se conectar automaticamente usando a conexão discada que você especificou.
- **Permanecer conectado após a filtragem** - o computador permanece conectado à Internet após o término da filtragem.

7 Clique na guia **Avançado** para editar opções avançadas.

- **Deixar as mensagens de spam no servidor** - se desejar que cópias das mensagens bloqueadas permaneçam no servidor de e-mail. Você pode ver o e-mail no cliente de e-mail e na página **E-mail bloqueado** do SpamKiller. Se a caixa de seleção não estiver marcada, as mensagens bloqueadas serão exibidas somente na página **E-mail bloqueado**.
- **Porta POP3** - (número da porta POP3) o servidor POP3 cuida das mensagens recebidas.
- **Porta SMTP** - (número da porta SMTP) o servidor SMTP cuida das mensagens enviadas.
- **Tempo limite do servidor** - período máximo que o SpamKiller espera para receber e-mails antes de parar.

  Aumente o valor do tempo limite do servidor se houver problemas ao receber e-mail. Se a sua conexão de e-mail estiver lenta, o aumento do valor do tempo limite do servidor permitirá que o SpamKiller aguarde um pouco mais antes de atingir o tempo limite.

8 Clique em **OK**.

Contas MSN/Hotmail

Edição de contas MSN/Hotmail

1 Clique na guia **Configurações** e, em seguida, clique em **Contas de e-mail**.

A caixa de diálogo **Contas de e-mail** é exibida com todas as contas de e-mail adicionadas ao SpamKiller.

> **NOTA**
> Se vários usuários tiverem sido adicionados ao SpamKiller, a lista exibirá as contas de e-mail do usuário que estiver conectado ao SpamKiller no momento.

2 Selecione uma conta MSN/Hotmail e clique em **Editar**.

3 Clique na guia **Geral** para editar a descrição da conta e o endereço de e-mail.

- **Descrição** - descrição da conta. Digite qualquer informação nessa caixa.
- **Endereço de e-mail** - endereço de e-mail da conta.

4 Clique na guia **Servidores** para editar as informações do servidor.

- **E-mails recebidos** - nome do servidor que recebe e-mails.
- **Senha** - senha usada para acessar a conta.
- **E-mails enviados** - nome do servidor que envia e-mails.
- **Usar um servidor SMTP para o envio de e-mails** - para enviar mensagens de erro sem incluir a linha de assinatura MSN na mensagem de erro. A linha de assinatura MSN permite que os remetentes de spam reconheçam facilmente se a mensagem de erro é falsa.

  Clique em **Mais** para alterar os requisitos de autenticação do servidor de saída.

5 Clique na guia **Verificando** para especificar a freqüência com que o SpamKiller deve verificar se há spam na conta:

a Selecione **Verificar a cada** ou **Verificar diariamente às** e, em seguida, digite uma hora na caixa correspondente. Se você digitar o número zero, o SpamKiller verificará a conta apenas ao se conectar.

b Selecione períodos adicionais para o SpamKiller filtrar a conta:

Verificar ao iniciar — Selecione essa opção se você tem uma conexão direta e deseja que o SpamKiller verifique a conta sempre que o computador for iniciado.

Verificar quando uma conexão for discada — Selecione essa opção se você tem uma conexão discada e deseja que o SpamKiller verifique a conta sempre que você se conectar à Internet.

6 Clique na guia **Conexão** para especificar como o SpamKiller discará uma conexão de Internet para verificar se há novas mensagens a serem filtradas na caixa de entrada.

- **Nunca discar uma conexão** - o SpamKiller não disca automaticamente uma conexão para você. Primeiro, é necessário iniciar manualmente a conexão discada.
- **Discar quando necessário** - quando uma conexão de Internet não está disponível, o SpamKiller tenta se conectar automaticamente usando a conexão de Internet discada padrão.
- **Discar sempre** - o SpamKiller tenta se conectar automaticamente usando a conexão discada que você especificou.
- **Permanecer conectado após a filtragem** - o computador permanece conectado à Internet após o término da filtragem.

7 Clique em **OK**.

Configuração de uma conta Hotmail para bloquear spam no Outlook ou no Outlook Express

O SpamKiller pode filtrar contas Hotmail diretamente. Consulte detalhes na ajuda on-line. Porém, só é possível bloquear mensagens ou adicionar amigos usando a barra de ferramentas do SpamKiller no Outlook ou no Outlook Express após a configuração da conta Hotmail.

1. Configure a sua conta Hotmail no MSK.
2. Se você já tem uma conta Hotmail no Outlook ou no Outlook Express, remova-a primeiro.
3. Adicione a conta Hotmail ao Outlook ou ao Outlook Express. Verifique se você selecionou **POP3** como tipo de conta e tipo de servidor de e-mails recebidos.
4. Nomeie o servidor de entrada como **`localhost`**.
5. Digite o nome do servidor SMTP de saída disponível (necessário).
6. Conclua o processo de configuração da conta. Agora você pode bloquear os novos e-mails de spam do Hotmail ou adicionar um amigo.

Contas MAPI

As condições a seguir são necessárias para a integração com êxito do SpamKiller ao MAPI no Outlook:

- Somente para Outlook 98: O Outlook ser inicialmente instalado com o suporte corporativo/de grupo de trabalho.
- Somente para Outlook 98: A primeira conta de e-mail ser uma conta MAPI.
- O computador estar conectado ao domínio.

Edição de contas MAPI

1. Clique na guia **Configurações** e, em seguida, clique em **Contas de e-mail**. A caixa de diálogo **Contas de e-mail** é exibida com todas as contas de e-mail adicionadas ao SpamKiller.

   NOTA
   Se vários usuários tiverem sido adicionados ao SpamKiller, a lista exibirá as contas de e-mail do usuário que estiver conectado ao SpamKiller no momento.

2. Selecione uma conta MAPI e, em seguida, clique em **Editar**.
3. Clique na guia **Geral** para editar a descrição da conta e o endereço de e-mail.
   - **Descrição** - descrição da conta. Digite qualquer informação nessa caixa.
   - **Endereço de e-mail** - endereço de e-mail da conta.

4 Clique na guia **Perfil** para editar as informações do perfil.

- **Perfil** - perfil MAPI da conta.
- **Senha** - senha correspondente ao perfil MAPI, se configurado (não é necessariamente a senha da conta de e-mail).

5 Clique na guia **Conexão** para especificar como o SpamKiller discará uma conexão de Internet para verificar se há novas mensagens a serem filtradas na caixa de entrada:

- **Nunca discar uma conexão** - o SpamKiller não disca automaticamente uma conexão para você. Primeiro, é necessário iniciar manualmente a conexão discada.
- **Discar quando necessário** - quando uma conexão de Internet não está disponível, o SpamKiller tenta se conectar automaticamente usando a conexão de Internet discada padrão.
- **Discar sempre** - o SpamKiller tenta se conectar automaticamente usando a conexão discada que você especificou.
- **Permanecer conectado após a filtragem** - o computador permanece conectado à Internet após o término da filtragem.

6 Clique em **OK**.

Acréscimo de usuários

O SpamKiller pode configurar vários usuários, correspondentes aos usuários configurados no sistema operacional Windows 2000 ou Windows XP.

Quando o SpamKiller é instalado no seu computador, um perfil de usuário de administrador é automaticamente criado para o usuário do Windows que efetuou logon. Se você adicionar contas de e-mail ao SpamKiller durante a instalação, essas contas serão adicionadas ao perfil de usuário do administrador.

Antes de adicionar mais contas de e-mail ao SpamKiller, determine se precisa adicionar mais usuários. O acréscimo de usuários é vantajoso quando várias pessoas usam o computador e têm suas próprias contas de e-mail. A conta de e-mail de cada usuário é adicionada ao perfil correspondente, permitindo que os usuários gerenciem suas próprias contas de e-mail, configurações pessoais, filtros pessoais e a **Lista de amigos pessoais**.

Os tipos de usuário definem as tarefas que o usuário pode executar no SpamKiller. A tabela a seguir é um resumo das permissões para cada tipo de usuário. Os administradores podem executar todas as tarefas, enquanto os usuários limitados só podem executar tarefas de acordo com os seus perfis pessoais. Por exemplo, os administradores podem ver todo o conteúdo das mensagens bloqueadas, enquanto os usuários limitados podem ver apenas a linha de assunto.

Tarefas	Administrador	Usuário limitado
Gerenciar contas de e-mail pessoais, **Filtros pessoais**, **Lista de amigos pessoais** e configurações de som pessoais	X	X
Gerenciar as páginas pessoais **E-mail bloqueado** e **E-mail aceito**	X	X
Exibir o texto das mensagens bloqueadas	X	
Exibir o texto das mensagens aceitas	X	X
Gerenciar os filtros globais e a **Lista de amigos globais**	X	
Relatar spam à McAfee	X	X
Enviar reclamações e mensagens de erro	X	X
Gerenciar reclamações e mensagens de erro (criar, editar e excluir modelos de mensagem)	X	
Gerenciar usuários (criar, editar e remover usuários)	X	
Fazer backup e restaurar o SpamKiller	X	
Exibir a página **Resumo** de spam recebido	X	X

Quando um usuário efetua logon no computador após ser adicionado, ele é solicitado a adicionar uma conta de e-mail ao respectivo perfil de usuário.

Para adicionar e gerenciar usuários, é exigido o seguinte:

- É necessário ter efetuado logon no SpamKiller como administrador.
- Você deve ter o Windows 2000 ou o Windows XP no seu computador.
- Os usuários adicionados ou gerenciados devem ter contas de usuário do Windows.

Senhas de usuário e proteção de crianças contra spam

A criação de uma senha de usuário fortalece o nível de privacidade. As configurações pessoais, a lista de amigos e a lista de **E-mail aceito** de um usuário não podem ser acessadas por outro usuário sem a senha de logon. A criação de senhas também é benéfica para impedir que crianças acessem o SpamKiller e vejam o conteúdo das mensagens de spam.

Criação de uma senha para um usuário do SpamKiller

1. Clique na guia **Configurações** e, em seguida, clique em **Usuários**.
2. Selecione um usuário e clique em **Editar**.
3. Digite uma senha na caixa **Senha**. Quando o usuário acessar o SpamKiller, ele precisará usar a senha para efetuar logon.

> **IMPORTANTE**
> Se você esquecer a senha, não poderá recuperá-la. Somente um administrador do SpamKiller poderá criar uma nova senha para você.

Acréscimo de um usuário ao SpamKiller

1. Clique na guia **Configurações** e, em seguida, clique em **Usuários**.
2. Clique em **Adicionar**.

   Uma lista de usuários do Windows é exibida. Para adicionar um usuário que não aparece na lista, crie uma conta de usuário do Windows para essa pessoa. Em seguida, o novo usuário deverá efetuar logon no computador pelo menos uma vez. Depois disso, adicione o usuário ao SpamKiller.

   > **NOTA**
   > Os usuários do Windows com direitos de administrador também possuem esses direitos no SpamKiller.

3. Selecione um usuário para adicionar e, em seguida, clique em **OK**. O usuário será adicionado ao SpamKiller e o nome de usuário será exibido na lista de usuários do SpamKiller.
4. Clique em **Fechar** quando terminar de adicionar usuários.

Para criar uma senha para um usuário, consulte *Criação de uma senha para um usuário do SpamKiller* na página 148.

Na próxima vez que o usuário efetuar logon no seu computador, ele será solicitado a adicionar uma conta de e-mail ao respectivo perfil de usuário do SpamKiller. Você pode adicionar contas de e-mail ao perfil do usuário se estiver conectado ao SpamKiller como o próprio usuário e possuir as informações necessárias sobre a conta de e-mail. Para obter detalhes, consulte *Acréscimo de contas de e-mail* na página 139.

Edição de um perfil de usuário do SpamKiller

1. Clique na guia **Configurações** e, em seguida, clique em **Usuários**. Uma lista de usuários do SpamKiller será exibida.
2. Selecione um usuário e clique em **Editar**.
3. Digite um novo nome e uma nova senha.

Exclusão de um perfil de usuário do SpamKiller

AVISO
Quando um perfil de usuário é removido, também são removidas as contas de e-mail desse usuário no SpamKiller.

1. Clique na guia **Configurações** e, em seguida, clique em **Usuários**. Uma lista de usuários do SpamKiller será exibida.
2. Selecione um usuário da lista e clique em **Excluir**.

Logon no SpamKiller em um ambiente multiusuário

Quando os usuários efetuam logon no computador e abrem o SpamKiller, eles são conectados automaticamente ao SpamKiller nos respectivos perfis de usuário. Se os usuários tiverem senhas do SpamKiller atribuídas, eles precisarão digitá-las na caixa de diálogo **Efetuar logon**.

Troca de usuário

É necessário ter efetuado logon no SpamKiller como administrador.

1. Clique em **Alternar usuário** na parte superior da página. A caixa de diálogo **Alternar usuário** é exibida.
2. Selecione um usuário e clique em **OK**. Se o usuário tiver uma senha, a caixa de diálogo **Efetuar logon** será exibida. Digite a senha de usuário na caixa **Senha** e clique em **OK**.

Recomendamos que você adicione os nomes e endereços de e-mail dos seus amigos à lista de amigos. O SpamKiller não bloqueia as mensagens das pessoas dessa lista; portanto, a inclusão de amigos na lista ajuda a garantir o recebimento de mensagens legítimas.

O SpamKiller permite adicionar nomes, endereços de e-mail, domínios e listas de mala direta às listas de amigos. É possível adicionar um endereço de cada vez ou todos de uma vez, importando uma lista de endereços do programa de e-mail.

O SpamKiller mantém dois tipos de lista:

- **Lista de amigos globais** - afeta todas as contas de e-mail de todos os usuários do SpamKiller. Se diversos usuários foram adicionados, é necessário estar conectado ao SpamKiller como administrador para gerenciar a lista.
- **Lista de amigos pessoais** - afeta todas as contas de e-mail associadas a um usuário específico. Se diversos usuários foram adicionados, é necessário estar conectado ao SpamKiller como esse usuário para gerenciar a lista.

Você pode adicionar amigos a uma lista de amigos para garantir que os respectivos e-mails não sejam bloqueados. A página **Amigos** mostra os nomes e endereços que foram adicionados à lista de amigos. A página **Amigos** também mostra a data em que o amigo foi adicionado e o número total de mensagens recebidas desse amigo.

Clique na guia **Endereços de e-mail** para ver endereços de e-mail da lista de amigos. Clique na guia **Domínios** para exibir os endereços de domínio da lista. Clique na guia **Listas de mala direta** para ver listas de mala direta da lista de amigos.

Para alternar entre a **Lista de amigos globais** e a **Lista de amigos pessoais**, clique na seta para baixo  localizada na guia **Endereço de e-mail**, **Domínios** ou **Listas de mala direta** e, em seguida, selecione **Lista de amigos pessoais**.

Abertura de uma lista de amigos

1 Para abrir uma lista de amigos, clique na guia **Amigos**. A página **Amigos** é exibida (Figura 6-3).

2 Clique na guia **Endereço de e-mail**, **Domínios** ou **Lista de mala direta**. A **Lista de amigos globais** é exibida. Para ver sua **Lista de amigos pessoais**, clique na seta para baixo em uma das guias e, em seguida, selecione **Lista de amigos pessoais**.

NOTA
Se o computador estiver executando o Windows 2000 ou Windows XP e vários usuários tiverem sido adicionados ao SpamKiller, os usuários limitados poderão ver somente a **Lista de amigos pessoais**.

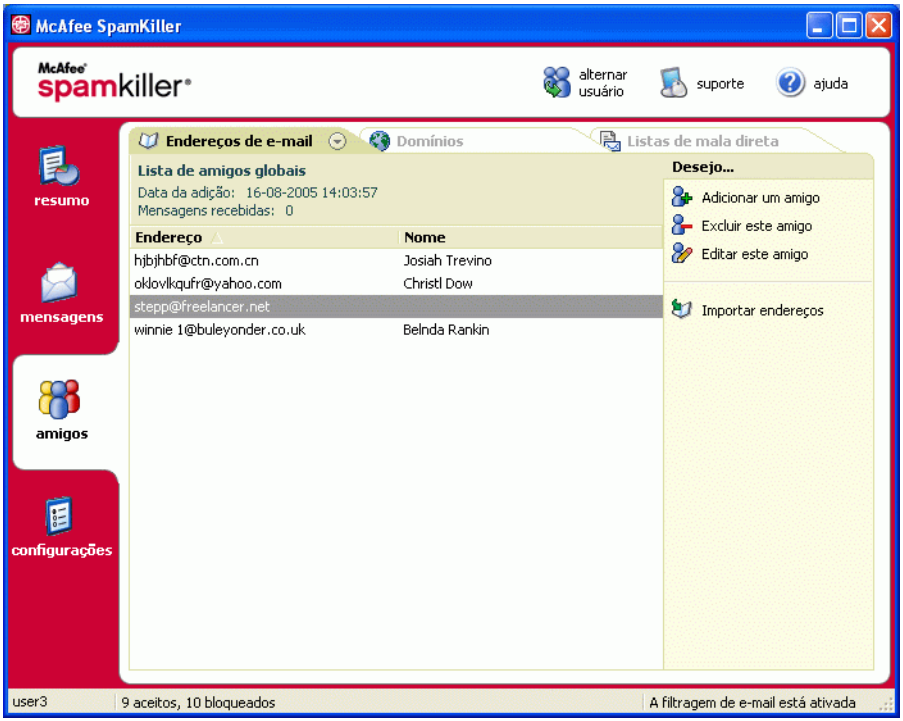


Figura 6-3. Página Amigos

Importação de listas de endereços

Importe listas de endereços para uma lista de amigos de modo manual ou automático. A importação automática permite que o SpamKiller verifique regularmente se há novos endereços nas listas de endereços e importe-os automaticamente para uma lista de amigos.

Você pode importar listas de endereços dos seguintes programas de e-mail:

- Microsoft Outlook (98 e posterior)
- Microsoft Outlook Express (todas as versões)
- Netscape Communicator (versão 6 e versões anteriores, se exportadas como arquivo LDIF)
- Qualcomm Eudora (versão 5 e posterior)
- IncrediMail Xe
- MSN/Hotmail
- Qualquer programa capaz de exportar a lista de endereços como arquivo de texto simples

Importação automática de uma lista de endereços

Você pode atualizar a sua Lista de amigos pessoais regularmente criando uma programação para importar os endereços de listas de endereços.

1. Clique na guia **Configurações** e, em seguida, clique em **Listas de endereços**. A caixa de diálogo **Importar listas de endereços** será exibida, mostrando uma relação das listas de endereços que o SpamKiller verifica regularmente e das quais importa endereços novos.
2. Clique em **Adicionar**. A caixa de diálogo **Importar programação** é exibida.
3. Selecione o **Tipo** de lista de endereços a ser importada e a **Origem** da lista.
4. Na caixa **Programação**, selecione a freqüência com que o SpamKiller deve verificar se há novos endereços na lista de endereços.
5. Clique em **OK**. Após uma atualização, os novos endereços serão exibidos na sua **Lista de amigos pessoais**.

Importação manual de uma lista de endereços

Você pode importar listas de endereços manualmente para a sua **Lista de amigos pessoais** ou para a **Lista de amigos globais**.

> **NOTA**
> Se o computador estiver executando o Windows 2000 ou o Windows XP e vários usuários tiverem sido adicionados ao SpamKiller, você deverá estar conectado como administrador para adicionar amigos à **Lista de amigos globais**.

1. Clique na guia **Amigos** e, em seguida, clique em **Importar lista de endereços**.

   A caixa de diálogo **Importar lista de endereços** é exibida, mostrando uma relação dos tipos de lista de endereços que podem ser importados.

2. Selecione um tipo de lista de endereços a ser importado ou clique em **Procurar** para importar endereços armazenados em um arquivo.

   Para importar a lista de endereços somente para a **Lista de amigos pessoais**, verifique se a caixa de seleção **Adicionar à lista de amigos pessoais** está marcada. Para importar a lista de endereços somente para a **Lista de amigos globais**, certifique-se de que a caixa de seleção não esteja marcada.

3. Clique em **Avançar**. Uma página de confirmação lista o número de endereços que o SpamKiller adicionou.

4. Clique em **Concluir**. Os endereços serão exibidos na **Lista de amigos globais** ou na **Lista de amigos pessoais**.

Edição de informações de lista de endereços

Edite informações de uma lista de endereços importada automaticamente.

1. Clique na guia **Configurações** e, em seguida, clique em **Listas de endereços**.
2. Selecione uma lista de endereços e clique em **Editar**.
3. Edite as informações sobre a lista de endereços e clique em **OK**.

Exclusão de uma lista de endereços da lista de importação automática

Remova uma entrada da lista de endereços quando não quiser mais que o SpamKiller importe automaticamente endereços dessa lista.

1. Clique na guia **Configurações** e, em seguida, clique em **Listas de endereços**.
2. Selecione uma lista de endereços e clique em **Excluir**. Uma caixa de diálogo de confirmação será exibida.
3. Clique em **Sim** para remover a lista de endereços da lista.

Acréscimo de amigos

Para assegurar que todos os e-mails recebidos são de amigos, adicione os respectivos nomes e endereços a uma lista de amigos. Você pode adicionar amigos das páginas **Amigos**, **E-mail bloqueado** e **E-mail aceito** e amigos contidos no Microsoft Outlook ou no Outlook Express.

NOTA
Se o computador estiver executando o Windows 2000 ou o Windows XP e vários usuários tiverem sido adicionados ao SpamKiller, você deverá estar conectado como administrador para adicionar amigos à **Lista de amigos globais**.

Acréscimo de amigos da página E-mail bloqueado ou E-mail aceito

1. Clique na guia **Mensagens** e, em seguida, clique na guia **E-mail bloqueado** ou **E-mail aceito**.

   Ou

   No menu do SpamKiller no Microsoft Outlook ou no Outlook Express, selecione **Exibir mensagens bloqueadas** para abrir a página **E-mail bloqueado** referente a essa conta.

   A página **E-mail bloqueado** ou **E-mail aceito** é exibida.

2. Selecione uma mensagem de um remetente que você deseja adicionar a uma lista de amigos e clique em **Adicionar um amigo**.

3. Na caixa **Endereço**, digite o endereço a ser adicionado à lista de amigos. A caixa **Endereço** talvez já contenha o endereço da mensagem selecionada.

4. Digite o nome do seu amigo na caixa **Nome**.

5. Na caixa **Tipo de amigo**, selecione o tipo de endereço a ser adicionado:

   - **Endereço de e-mail único** - o endereço de e-mail do remetente é adicionado à seção Domínios da lista de amigos.
   - **Todos no domínio** - o nome de domínio é adicionado à seção **Domínios** da lista de amigos. O SpamKiller aceita todos os e-mails provenientes do domínio.
   - **Lista de mala direta** - o endereço é adicionado à seção **Lista de mala direta** da lista de amigos.

   Para adicionar o endereço somente à **Lista de amigos pessoais**, verifique se a caixa de seleção **Adicionar à lista de amigos pessoais** está marcada. Para adicionar o endereço somente à **Lista de amigos globais**, certifique-se de que a caixa de seleção não esteja marcada.

6 Clique em **OK**. Todas as mensagens desse amigo são marcadas de modo a indicar que foram enviadas por um amigo, sendo exibidas na página **E-Mail aceito**.

Acréscimo de amigos da página Amigos

1 Clique na guia **Amigos** e, em seguida, clique em **Adicionar um amigo**. A caixa de diálogo **Propriedades do amigo** é exibida.

2 Na caixa **Endereço**, digite o endereço a ser adicionado à lista de amigos.

3 Digite o nome do seu amigo na caixa **Nome**.

4 Na caixa **Tipo de amigo**, selecione o tipo de endereço a ser adicionado:

- **Endereço de e-mail único** - o endereço de e-mail do remetente é adicionado à seção Domínios da lista de amigos.
- **Todos no domínio** - o nome de domínio é adicionado à seção **Domínios** da lista de amigos. O SpamKiller aceita todos os e-mails provenientes do domínio.
- **Lista de mala direta** - o endereço é adicionado à seção **Lista de mala direta** da lista de amigos.

Para adicionar o endereço somente à **Lista de amigos pessoais**, verifique se a caixa de seleção **Adicionar à lista de amigos pessoais** está marcada. Para adicionar o endereço somente à **Lista de amigos globais**, certifique-se de que a caixa de seleção não esteja marcada.

5 Clique em **OK**. Todas as mensagens desse amigo são marcadas de modo a indicar que foram enviadas por um amigo, sendo exibidas na página **E-Mail aceito**.

Acréscimo de amigos do Microsoft Outlook

1 Abra sua conta de e-mail no Microsoft Outlook ou no Outlook Express.

2 Selecione uma mensagem de um remetente que você deseja adicionar a uma lista de amigos.

3 Clique em  na barra de ferramentas do Microsoft Outlook. Todas as mensagens desse amigo são marcadas de modo a indicar que foram enviadas por um amigo, sendo exibidas na página **E-Mail aceito**.

Edição de amigos

1 Clique na guia **Amigos** e, em seguida, clique na guia **Endereços de e-mail**, **Domínios** ou **Listas de mala direta**.

A **Lista de amigos globais** é exibida. Para ver sua **Lista de amigos pessoais**, clique na seta para baixo em uma das guias e, em seguida, selecione **Lista de amigos pessoais**.

NOTA
Se o computador estiver executando o Windows 2000 ou o Windows XP e vários usuários tiverem sido adicionados ao SpamKiller, somente os administradores poderão acessar a **Lista de amigos globais**.

2 Selecione um endereço na lista e clique em **Editar**.

3 Edite as informações apropriadas e clique em **OK**.

Exclusão de amigos

Remova os endereços que não deseja mais em uma lista de amigos.

1 Clique na guia **Amigos** e, em seguida, clique na guia **Endereços de e-mail**, **Domínios** ou **Listas de mala direta**.

A **Lista de amigos globais** é exibida. Para ver sua **Lista de amigos pessoais**, clique na seta para baixo em uma das guias e, em seguida, selecione **Lista de amigos pessoais**.

NOTA
Se o computador estiver executando o Windows 2000 ou o Windows XP e vários usuários tiverem sido adicionados ao SpamKiller, somente os administradores poderão acessar a **Lista de amigos globais**.

2 Selecione um endereço na lista e clique em **Excluir este amigo**. Uma caixa de diálogo de confirmação será exibida.

3 Clique em **Sim** para excluir o amigo.

Clique na guia **Mensagens** para abrir a página **Mensagens** (Figura 6-4) e acessar as suas mensagens bloqueadas e aceitas. As páginas **E-mail bloqueado** e **E-mail aceito** possuem recursos semelhantes.

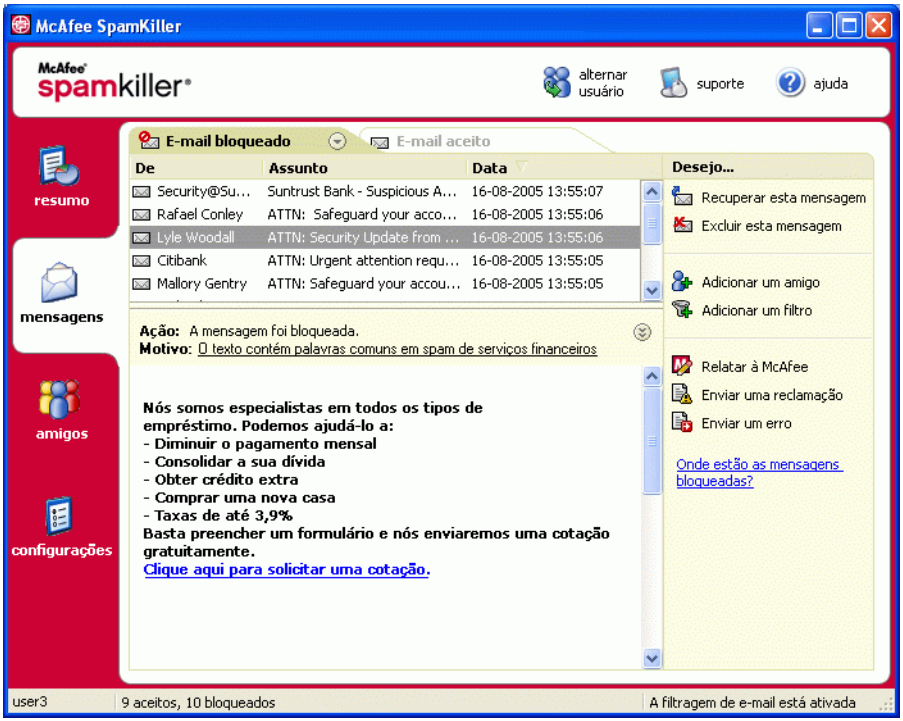


Figura 6-4. Página Mensagens

Página E-mail bloqueado

Clique na guia **E-mail bloqueado** da página **Mensagens** para exibir as mensagens bloqueadas.

> **NOTA**
> Também é possível acessar as mensagens bloqueadas no Microsoft Outlook, selecionando o menu do SpamKiller e, em seguida, clicando em **Exibir mensagens bloqueadas**.

As mensagens bloqueadas são mensagens que o SpamKiller identificou como spam, removeu da caixa de entrada e colocou na página **E-mail bloqueado**.

A página **E-mail bloqueado** exibe todas as mensagens de spam removidas das suas contas de e-mail. Para exibir os e-mails bloqueados de uma conta específica, clique na seta para baixo ⌄ localizada na guia **E-mail bloqueado** e selecione a conta a ser exibida.

O painel de mensagens superior lista as mensagens de spam classificadas por data. A mensagem mais recente é exibida primeiro. O painel de visualização inferior contém o texto da mensagem selecionada.

> **NOTA**
> Se o computador estiver executando o Windows 2000 ou o Windows XP, vários usuários foram adicionados ao SpamKiller e você estiver conectado ao SpamKiller como usuário limitado, o conteúdo da mensagem não será exibido no painel de visualização inferior.

O painel do meio exibe os detalhes da mensagem. Clique nas setas para baixo para expandir o painel de detalhes e exibir o texto e os cabeçalhos da mensagem no formato nativo, inclusive as marcas de formatação HTML. O painel de detalhes da mensagem exibe o seguinte:

- **Ação** - como o SpamKiller processou a mensagem de spam. A ação está associada à ação do filtro que bloqueou a mensagem.
- **Razão** - motivo pelo qual o SpamKiller bloqueou a mensagem. Você pode clicar na razão para abrir o editor de filtros e exibir o filtro. O editor de filtros exibe o que o filtro procura em uma mensagem e a ação executada pelo SpamKiller com as mensagens encontradas pelo filtro.
- **De** - o remetente da mensagem.
- **Data** - a data em que a mensagem foi enviada para você.
- **Para** - para quem a mensagem foi enviada.
- **Assunto** - o tópico que aparece na linha de assunto da mensagem.

A coluna da esquerda contém ícones ao lado das mensagens, caso tenham sido enviadas reclamações manuais ou mensagens de erro.

- Reclamação enviada  - foi enviada uma reclamação sobre a mensagem.
- Mensagem de erro enviada  - uma mensagem de erro foi enviada para o endereço de resposta da mensagem de spam.
- Reclamação e mensagens de erro enviadas  - uma reclamação e uma mensagem de erro foram enviadas.

Para obter mais informações sobre onde se encontram as mensagens bloqueadas, consulte *Onde estão as mensagens bloqueadas* na página 162.

Página E-mail aceito

Clique na guia **E-mail aceito** na página **Mensagens** para exibir as mensagens aceitas.

A página **E-mail aceito** exibe todas as mensagens da caixa de entrada, de todas as contas de e-mail. Entretanto, para contas MAPI, a página **E-mail aceito** não contém e-mail interno. Para exibir os e-mails aceitos de uma conta específica, clique na seta para baixo da guia **E-mail aceito** e selecione uma conta a ser exibida.

> **NOTA**
> O SpamKiller foi projetado para aceitar e-mails legítimos. Entretanto, se forem exibidos e-mails legítimos na lista **E-mail bloqueado**, você poderá colocá-los de volta na caixa de entrada (e na lista **E-mail aceito**) selecionando-os e clicando em **Recuperar esta mensagem**.

Da mesma forma que a página **E-mail bloqueado**, o painel de mensagens superior lista mensagens classificadas por data. O painel de visualização inferior contém o texto da mensagem selecionada.

O painel do meio explica se a mensagem foi enviada por alguém de uma lista de amigos ou se a mensagem está de acordo com os critérios de um filtro, embora a ação do filtro tenha sido definida como **Aceitar** ou **Marcar como possível spam**. Clique nas setas para baixo para expandir o painel de detalhes e exibir o texto e os cabeçalhos da mensagem no formato nativo, inclusive as marcas de formatação HTML.

O painel de detalhes da mensagem exibe o seguinte:

- **Ação** - como o SpamKiller processou a mensagem.
- **Razão** - se alguma mensagem foi marcada, essa opção explica por que o SpamKiller marcou a mensagem.
- **De** - o remetente da mensagem.
- **Data** - a data em que a mensagem foi enviada para você.
- **Para** - para quem a mensagem foi enviada.
- **Assunto** - o tópico que aparece na linha de assunto da mensagem.

Um dos ícones a seguir aparece ao lado de uma mensagem.

- E-mail de um amigo - o SpamKiller detectou que o remetente da mensagem consta em uma lista de amigos. É uma das mensagens que você deseja guardar.
- Possível spam - a mensagem corresponde a um filtro com uma ação definida como Marcar como possível spam.
- Reclamação enviada - uma reclamação sobre a mensagem foi enviada.

- Mensagem de erro enviada  - uma mensagem de erro foi enviada para o endereço de resposta na mensagem de spam.
- Reclamação e mensagens de erro enviadas  - uma reclamação e uma mensagem de erro foram enviadas.

Tarefas para e-mail bloqueado e e-mail aceito

O painel à direita nas páginas **E-mail bloqueado** e **E-mail aceito** lista as tarefas que você pode executar.

- **Bloquear esta mensagem** - remove uma mensagem da caixa de entrada e a coloca na página **E-mail bloqueado** do SpamKiller. (Essa opção é exibida somente na página **E-mail aceito**).
- **Recuperar esta mensagem** - coloca uma mensagem de volta na caixa de entrada (opção exibida somente na página **E-mail bloqueado**) e abre a caixa de diálogo **Opções de resgate**. Você pode adicionar automaticamente o remetente à sua lista de Amigos e resgatar todas as mensagens do remetente.
- **Excluir esta mensagem** - remove uma mensagem selecionada.
- **Adicionar um amigo** - adiciona o nome, o endereço de e-mail, o domínio ou uma lista de mala direta do remetente a uma lista de amigos.
- **Adicionar um filtro** - cria um filtro.
- **Relatar à McAfee** - informa a McAfee sobre mensagens específicas de spam que você recebeu.
- **Enviar uma reclamação** - envia uma reclamação sobre spam ao administrador do domínio do remetente ou a outro endereço de e-mail que você digitar.
- **Enviar um erro** - envia uma mensagem de erro ao endereço de resposta de uma mensagem de spam.

Recuperação de mensagens

Se a página **E-mail bloqueado** ou a pasta do SpamKiller no Microsoft Outlook e Outlook Express contiverem e-mails legítimos, você poderá colocar essas mensagens de volta na sua caixa de entrada.

Na página E-mail bloqueado

1. Clique na guia **Mensagens** e, em seguida, clique na guia **E-mail bloqueado**.

   Ou

   No menu do SpamKiller no Microsoft Outlook ou no Outlook Express, selecione **Exibir mensagens bloqueadas** para abrir a página **E-mail bloqueado** referente a essa conta.

2. Selecione uma mensagem e clique em **Recuperar esta mensagem**  . A caixa de diálogo **Opções de resgate** é exibida.

   - **Adicionar amigo** - adiciona o remetente à lista de amigos.
   - **Recuperar todas do mesmo remetente** - recupera todas as mensagens bloqueadas do remetente da mensagem selecionada.

3. Clique em **OK**. A mensagem é colocada de volta na caixa de entrada e na página **E-mail aceito**.

Na pasta do SpamKiller no Microsoft Outlook ou no Outlook Express

Selecione as mensagens e clique em **Recuperar seleção** no menu do SpamKiller ou na barra de tarefas. A sua seleção é colocada de volta na caixa de entrada e a marca da mensagem ([SPAM] por padrão) é removida.

Bloqueio de mensagens

Bloqueie as mensagens de spam que estão na caixa de entrada. Quando você bloqueia uma mensagem, o SpamKiller cria automaticamente um filtro para removê-la da caixa de entrada. Você pode bloquear mensagens da caixa de entrada na página **E-mail aceito** ou no Microsoft Outlook ou no Outlook Express.

Na página E-mail aceito

1. Clique na guia **Mensagens** e, em seguida, clique na guia **E-mail aceito**. A página **E-mail aceito** é exibida com as mensagens existentes na sua caixa de entrada.

2. Selecione uma mensagem e clique em **Bloquear esta mensagem**. A mensagem é removida da caixa de entrada e da página **E-mail aceito** e uma cópia da mensagem é exibida na página **E-mail bloqueado**.

No Microsoft Outlook

No Microsoft Outlook, as mensagens dos membros de um servidor do Exchange são consideradas seguras e não são filtradas pelo SpamKiller. Apenas mensagens de fontes externas são filtradas.

1. Abra a caixa de entrada do Microsoft Outlook ou Outlook Express.
2. Selecione uma mensagem e clique em  . Uma cópia da mensagem é colocada na página **E-mail bloqueado**.

Onde estão as mensagens bloqueadas

Por padrão, as mensagens de spam são marcadas como [SPAM] e colocadas na pasta do SpamKiller no Outlook e no Outlook Express ou na caixa de entrada. As mensagens marcadas também são exibidas na página **E-mail aceito**.

Exclusão manual de uma mensagem

1. Clique na guia **Mensagens** e, em seguida, clique na guia **E-mail bloqueado**.

   Ou

   No menu do SpamKiller no Microsoft Outlook ou no Outlook Express, selecione **Exibir mensagens bloqueadas** para abrir a página **E-mail bloqueado** referente a essa conta.
2. Selecione uma mensagem a ser excluída.
3. Clique em **Excluir esta mensagem**. Uma caixa de diálogo de confirmação será exibida.
4. Clique em **Sim** para excluir a mensagem.

Modificação do modo como as mensagens de spam são processadas

Quando o spam é encontrado, a mensagem é marcada ou bloqueada. As mensagens de spam são removidas do servidor cada vez que o SpamKiller se conecta a ele.

Marcação

A linha de assunto do e-mail é marcada com [SPAM] e a mensagem vai para a caixa de entrada ou para a pasta do SpamKiller, caso seja utilizado o Microsoft Outlook ou o Outlook Express.

Bloqueio

A mensagem é removida e colocada na página **E-mail bloqueado** do SpamKiller. Quando e-mails legítimos são bloqueados, é possível recuperar a mensagem (consulte Recuperando mensagens).

O SpamKiller remove automaticamente as mensagens bloqueadas da página **E-mail bloqueado** após 15 dias. Você pode alterar a freqüência com que as mensagens bloqueadas são removidas.

O SpamKiller não remove automaticamente as mensagens da página **E-mail aceito**, pois esta reflete as mensagens que estão na caixa de entrada.

Modificação do modo como o SpamKiller processa mensagens de spam

1. Clique na guia **Configurações** e, em seguida, no ícone **Opções de filtragem**.
2. Clique na guia **Processamento**.
   - **Colocar o spam na caixa de e-mail bloqueado** - as mensagens de spam são removidas da caixa de entrada e colocadas na página **E-mail bloqueado** do SpamKiller.
   - **Marcar o spam e manter na caixa de entrada** - trata-se da configuração padrão. As mensagens de spam permanecem na caixa de entrada, mas a linha de assunto da mensagem inclui [SPAM].

     Manter o e-mail bloqueado por ____ dias - as mensagens bloqueadas permanecem na página **E-mail bloqueado** durante o período que você especificar.

     Manter o e-mail aceito por ____ dias - as mensagens aceitas permanecem na página **E-mail aceito** durante o período que você especificar.
3. Clique em **OK**.

Utilização do filtro AntiPhishing

O e-mail não solicitado é classificado como spam (e-mails que solicitam que você adquira algo) ou phishing (e-mails que solicitam que você forneça informações pessoais para um site da Web enganoso, seja conhecido ou potencial).

O filtro AntiPhishing da McAfee o ajuda a proteger-se contra sites da Web que estão na lista negra (de phishing confirmado ou sites enganosos associados) e na lista cinza (podem apresentar conteúdo perigoso ou links para sites da lista negra).

Ao navegar em um site enganoso (conhecido ou potencial), você será redirecionado à página do **Filtro AntiPhishing da McAfee**.

Para alterar as configurações do AntiPhishing, siga estas etapas:

1. Abra o Internet Explorer.
2. No menu **Ferramentas**, selecione **Filtro AntiPhishing da McAfee**.

- **Ativar a filtragem do site da Web** - ativado por padrão. Para desativar a filtragem AntiPhishing, desmarque essa caixa de seleção.
- **Permitir o acesso a sites da Web na lista negra** - coloca um link para os sites da lista negra na página de redirecionamento. Ao clicar neste link, você é levado ao site da Web.
- **Permitir o acesso a sites da Web na lista cinza** - coloca um link para os sites da lista cinza na página de redirecionamento. Ao clicar neste link, você é levado ao site da Web.

3. Ao terminar, clique em **OK**.

Acréscimo de amigos a uma lista de amigos

Consulte *Acréscimo de amigos da página E-mail bloqueado ou E-mail aceito* na página 154.

Acréscimo de filtros

Para obter mais informações sobre filtros, consulte *Trabalho com filtros* na Ajuda on-line.

1. Para criar um filtro global, clique na guia **Configurações**, selecione **Filtros globais** e, em seguida, clique em **Adicionar**.

   Ou

   Para criar um filtro pessoal, clique na guia **Configurações**, selecione **Filtros pessoais** e, em seguida, clique em **Adicionar**.

   Ou

   Clique na guia **Mensagens**, na guia **E-mail bloqueado** ou **E-mail aceito** e em **Adicionar um filtro**.

2. Clique em **Adicionar** para iniciar a criação de uma condição de filtro. A caixa de diálogo **Condição do filtro** é exibida.

3 Crie uma condição de filtro seguindo estas etapas.

Uma condição de filtro é uma instrução que informa ao SpamKiller o que ele deve procurar em uma mensagem. No exemplo "O texto da mensagem contém hipoteca," o filtro procura mensagens que contenham a palavra "hipoteca". Para obter mais informações, consulte *Condições do filtro* na Ajuda on-line.

a Selecione um tipo de condição na primeira caixa.

b Selecione ou digite valores nas caixas subseqüentes.

c Se as opções a seguir forem exibidas, selecione-as para definir ainda mais a condição do filtro.

Procurar também nos códigos de formatação - essa opção é exibida somente se a condição do filtro for definida para pesquisar o texto da mensagem. Quando essa caixa de seleção está marcada, o SpamKiller procura no texto e nos códigos de formatação da mensagem a expressão indicada.

Comparar variações - permite que o SpamKiller detecte erros ortográficos comuns cometidos intencionalmente pelos remetentes de spam. Por exemplo, a palavra "comum" pode estar grafada como "c0mvn" para despistar os filtros.

Expressões regulares (RegEx) - permite especificar padrões de caracteres usados nas condições de filtro. Para testar um padrão de caracteres, clique em **Testar RegEx**.

Sensível a maiúsculas e minúsculas - essa opção é exibida somente em condições nas quais você tenha digitado um valor de condição. Com essa caixa de seleção marcada, o SpamKiller diferencia maiúsculas e minúsculas no valor digitado.

d Clique em **OK**.

4 Crie outra condição de filtro da maneira especificada a seguir ou vá para a etapa 5 e selecione uma ação de filtro.

a Clique em **Adicionar** e crie a condição de filtro. Clique em **OK** quando terminar de criar a condição de filtro.

As duas condições de filtro são exibidas na lista **Condições do filtro** e associadas pela conjunção **e**. O **e** indica que o SpamKiller procurará mensagens que correspondam às *duas* condições de filtro. Se desejar que o SpamKiller procure mensagens que correspondam a uma das duas condições, substitua o **e** por **ou** clicando em **e** e selecionando **ou** na caixa apresentada.

b Clique em **Adicionar** para criar outra condição ou vá para a etapa 5 e selecione uma ação de filtro.

Se você criou um total de três ou mais condições do filtro, poderá agrupá-las para criar cláusulas. Para obter exemplos de agrupamento, consulte *Trabalhando com filtros* na Ajuda on-line.

Para agrupar condições de filtro, selecione uma condição e, em seguida, clique em **Agrupar**. Para desagrupar condições de filtro, selecione uma condição agrupada e clique em **Desagrupar**.

5 Selecione uma ação do filtro na caixa **Ação**. A ação do filtro informa ao SpamKiller como processar mensagens encontradas por esse filtro. Para obter mais informações, consulte *Ações de filtro* na Ajuda on-line.

6 Clique em **Avançado** para selecionar as opções avançadas de filtro (a seleção das opções avançadas não é obrigatória). Para obter mais informações, consulte *Opções avançadas de filtro* na Ajuda on-line.

7 Clique em **OK** quando terminar de criar o filtro.

NOTA
Para editar uma condição, selecione-a e clique em **Editar**. Para excluir uma condição, selecione-a e clique em **Excluir**.

Expressões regulares

As expressões regulares estão disponíveis apenas para as seguintes condições de filtro: **O assunto**, **O texto da mensagem**, **Pelo menos uma das seguintes frases**.

Esses caracteres e seqüências especiais podem ser usados como expressões regulares para definir as condições de filtro. Por exemplo:

- A expressão regular **[0-9]*\.[0-9]+** corresponde a números de ponto flutuante expressos em notação que não seja de engenharia. A expressão regular corresponde a: “12.12”, “.1212” e “12.0”, mas não a “12” e “12.”
- A expressão regular**\D*[0-9]+\D*** corresponde a todas as palavras com números: “SpamKi11er” e V1AGRA”, mas não a “SpamKiller” e “VIAGRA”.

****

Marca o próximo caractere como especial ou literal. Por exemplo, “n“ corresponde ao caractere “n“. “\n“ corresponde a um caractere de nova linha. A seqüência “\\“ corresponde a “\“ e “\(“ corresponde a “(“.

^

Corresponde ao início da entrada.

$

Corresponde ao final da entrada.

*****

Corresponde ao caractere precedente, zero ou mais vezes. Por exemplo, “zo*“ corresponde a “z“ ou “zoo“.

+

Corresponde ao caractere precedente, uma ou mais vezes. Por exemplo, “zo+“ corresponde a “zoo“, mas não a “z“.

?

Corresponde ao caractere precedente, zero ou uma vez. Por exemplo, “a?va?“ corresponde ao “va“ de “nevar“.

.

Corresponde a qualquer caractere único, exceto o de nova linha.

(padrão)

Corresponde ao padrão e lembra a correspondência. A subseqüência de caracteres correspondente pode ser recuperada da coleção resultante de correspondências, usando o item [0]...[n]. Para corresponder com os caracteres de parêntese ( ), use “\(“ ou “\)“.

x|y

Corresponde a x ou y. Por exemplo, “m|carro“ corresponde a “m“ ou “carro“. “(m|c)ar“ corresponde a “mar“ ou “carro“.

{n}

n é um número inteiro não-negativo. Corresponde exatamente a n vezes. Por exemplo, “o{2}“ não corresponde ao “o“ de “come“, mas corresponde aos dois primeiros “o“ de “cooooomida“.

{n,}

n é um número inteiro não-negativo. Corresponde a pelo menos n vezes. Por exemplo, “o{2,}“ não corresponde ao “o“ de “come“ e corresponde a todos os “o“ de “cooooomida“. “o{1,}“ equivale a “o+“. “o{0,}“ equivale a “o*“.

{n,m}

m e n são números inteiros não-negativos. Correspondem a no mínimo n e no máximo m vezes. Por exemplo, “o{1,3}“ corresponde aos três primeiros “o“ de “cooooomida“. “o{0,1}“ equivale a “o?“.

[xyz]

Um conjunto de caracteres. Corresponde a qualquer um dos caracteres entre colchetes. Por exemplo, “[abc]“ corresponde ao “a“ de “plano“.

[^xyz]

Um conjunto negativo de caracteres. Corresponde a qualquer caractere não especificado entre colchetes. Por exemplo, "[^abc]" corresponde ao "p" de "plano".

[a-z]

Um intervalo de caracteres. Corresponde a qualquer caractere do intervalo especificado. Por exemplo, "[a-z]" corresponde a qualquer caractere alfabético minúsculo de "a" a "z".

[^m-z]

Os caracteres de um intervalo negativo. Corresponde a qualquer caractere que não esteja no intervalo especificado. Por exemplo, "[^m-z]" corresponde a qualquer caractere que não seja de "m" a "z".

\b

Corresponde a um limite de palavra, ou seja, a posição entre uma palavra e um espaço. Por exemplo, "er\b" corresponde ao "er" de "comer", mas não ao "er" de "verbo".

\B

Corresponde à ausência de um limite de palavra. "an*t\B" corresponde ao "ant" de "nunca antes".

\d

Corresponde a um caractere numérico. Equivale a [0-9].

\D

Corresponde a um caractere não-numérico. Equivale a [^0-9].

\f

Corresponde ao caractere de avanço de página.

\n

Corresponde ao caractere de nova linha.

\r

Corresponde ao caractere de retorno de carro.

\s

Corresponde a qualquer espaço em branco, incluindo espaço, tabulação, avanço de página, etc. Equivale a "[\f\n\r\t\v]".

\S

Corresponde a qualquer caractere de espaço que não esteja em branco. Equivale a "[^ \f\n\r\t\v]".

\t

Corresponde a um caractere de tabulação.

\v

Corresponde a um caractere de barra vertical.

\w

Corresponde a qualquer caractere alfanumérico ou "_". Equivale a "[A-Za-z0-9_]".

\W

Corresponde a qualquer caractere que não seja alfanumérico ou "_". Equivale a "[^A-Za-z0-9_]".

\num

Corresponde a num, onde num é um número inteiro positivo. Uma referência às correspondências lembradas. Por exemplo, "(.)\1" corresponde a dois caracteres idênticos consecutivos.

\n

Corresponde a n, onde n é um valor de escape octal. Os valores de escape octais devem conter 1, 2 ou 3 dígitos. Por exemplo, "\11" e "\011" coincidem ambos com um caractere de tabulação. "\0011" equivale a "\001" & "1". Os valores de escape octais não devem exceder 256. Caso excedam, somente os dois primeiros dígitos formarão a expressão. Permite o uso de códigos ASCII em expressões regulares.

\xn

Corresponde a n, onde n é um valor de escape hexadecimal. Os valores de escape hexadecimais devem conter exatamente dois dígitos. Por exemplo, "\x41" corresponde a "A". "\x041" equivale a "\x04" & "1". Permite o uso de códigos ASCII em expressões regulares.

Relato de spam à McAfee

Você pode relatar spam à McAfee para que ele seja analisado, permitindo criar atualizações de filtros.

1. Clique na guia **Mensagens** e, em seguida, clique na guia **E-mail bloqueado** ou **E-mail aceito**. A página **E-mail bloqueado** ou **E-mail aceito** é exibida.
2. Selecione uma mensagem e clique em **Relatar à McAfee**. Uma caixa de diálogo de confirmação será exibida.
3. Clique em **Sim**. A mensagem será enviada automaticamente à McAfee.

Envio manual de reclamações

Envie uma reclamação para impedir que determinado remetente envie mais spam para você. Para obter mais informações sobre como enviar reclamações, consulte *Enviando reclamações e mensagens de erro* na Ajuda on-line.

1. Clique na guia **Mensagens** e, em seguida, clique na guia **E-mail bloqueado** ou **E-mail aceito**. Uma lista de mensagens é exibida.
2. Selecione uma mensagem sobre a qual fará uma reclamação e clique em **Enviar uma reclamação**. A caixa de diálogo **Enviar reclamação** será exibida.
3. Selecione para quem você deseja enviar a reclamação.

   AVISO
   Na maioria dos casos, você não deve selecionar **Remetente**. O envio de uma reclamação ao remetente do spam valida seu endereço de e-mail, o que pode aumentar a quantidade de spam que esse remetente enviará a você.

4. Clique em **Avançar** e siga as instruções das caixas de diálogo exibidas.

Envio de mensagens de erro

Para obter mais informações sobre como enviar mensagens de erro, consulte *Enviando reclamações e mensagens de erro* na Ajuda on-line.

Envie uma mensagem de erro para evitar que um remetente envie mais spam a você.

Envio manual de uma mensagem de erro

1. Clique na guia **Mensagens** e, em seguida, clique na guia **E-mail bloqueado** ou **E-mail aceito**. Uma lista de mensagens é exibida.
2. Para enviar uma mensagem de erro sobre uma mensagem de spam específica, selecione a mensagem e clique em **Enviar um erro**. Uma mensagem de erro será enviada para o endereço de resposta da mensagem de spam.

O SpamKiller não consegue se comunicar com o servidor

Se o servidor do SpamKiller não iniciar ou estiver bloqueado por outro aplicativo, ele não poderá se comunicar com seu servidor.

Como iniciar manualmente o servidor do SpamKiller

Esta seção se aplica apenas a usuários do Microsoft Windows 2000 e XP.

1. Clique em **Iniciar** e selecione **Executar**.
2. Digite SERVICES.MSC e clique em **OK**.
3. Clique com o botão direito do mouse no servidor do McAfee SpamKiller e selecione **Iniciar**. O serviço do servidor será iniciado.

O servidor do SpamKiller é bloqueado por firewalls ou programas de filtragem da Internet

Se o servidor do SpamKiller já estiver iniciado e em execução, siga estas etapas.

1. Verifique se o servidor do SpamKiller e/ou o MSKSrvr.exe têm acesso total em qualquer programa de firewall instalado, incluindo o McAfee Personal Firewall.
2. Verifique se LocalHost e/ou 127.0.0.1 não foram bloqueados ou banidos por algum programa de firewall instalado, incluindo o McAfee Personal Firewall.
3. Desative quaisquer programas de privacidade ou filtragem de Internet.

Não é possível conectar-se ao servidor de e-mail

Se o servidor do SpamKiller tentar se conectar ao servidor POP3 e a conexão falhar, siga estas etapas.

Verificação da sua conexão à Internet.

Usuários de conexão discada

1. Clique em **Continuar o que eu estava fazendo** na mensagem de erro (se necessário).
2. Estabeleça uma conexão à Internet.
3. Mantenha a conexão por, no mínimo, 15 minutos, para ver se a mensagem é exibida novamente.

Banda larga (cabo, DSL)

1. Clique em **Continuar o que eu estava fazendo** na mensagem de erro (se necessário).
2. Verifique se você está conectado à Internet, entrando em um site.

Verificação dos endereços de servidor POP3 do SpamKiller

1. Clique com o botão direito no ícone da McAfee na área de notificação do sistema (canto inferior direito), aponte para **SpamKiller**, e selecione **Configurações**.
2. Clique em **Contas de e-mail**.
3. Selecione a conta de e-mail na mensagem de erro.
4. Clique em **Editar**.
5. Selecione a guia **Servidores**.
6. Anote o endereço do servidor na caixa **E-mails recebidos** e compare-o com o endereço do servidor de recebimento de e-mail que o seu provedor de serviços de Internet (ISP) listou para a sua conta de e-mail. Os dois endereços devem ser iguais.
7. Confirme a senha, digitando novamente a senha fornecida pelo provedor de serviços de Internet para a conta de e-mail.
8. Clique em **OK**.
9. Clique em **Fechar**.

Glossário 7

802.11

Um conjunto de padrões IEEE para tecnologia de LAN sem fio. O 802.11 especifica uma comunicação pelo ar entre um cliente sem fio e uma estação base ou entre dois clientes sem fio. As várias especificações do 802.11 incluem 802.11a, um padrão para comunicação em rede até 54 Mbps na banda de 5 Ghz, 802.11b, um padrão para rede até 11 Mbps na banda de 2,4 Ghz, 802.11g, um padrão para rede até 54 Mbps na banda de 2,4 Ghz, e 802.11i, um conjunto de padrões de segurança para todas as redes Ethernet sem fio.

802.11a

Uma extensão do 802.11 que se aplica a LANs sem fio e que envia dados a até 54 Mbps na banda de 5 GHz. Embora a velocidade de transmissão seja maior que com o 802.11b, o alcance é muito menor.

802.11b

Uma extensão do 802.11 que se aplica a LANs sem fio e que permite transmissão a 11 Mbps na banda de 2,4 GHz. O 802.11b é considerado atualmente o padrão em comunicação sem fio.

802.11g

Uma extensão do 802.11 que se aplica a LANs sem fio e que permite até 54 Mbps na banda de 2,4 GHz.

802.1x

Não suportado pelo Wireless Home Network Security. Um padrão IEEE para autenticação em redes com ou sem fio, porém mais freqüentemente usado em conjunto com a rede sem fio 802.11. Esse padrão proporciona uma autenticação forte e mútua entre um cliente e um servidor de autenticação. Além disso, o 802.1x pode fornecer chaves WEP dinâmicas por usuário e por sessão, eliminando o trabalho administrativo e os riscos de segurança inerentes às chaves WEP estáticas.

A

Adaptador sem fio

Contém os circuitos necessários para que um computador ou outro dispositivo se comunique com um roteador sem fio (conectado a uma rede sem fio). Os adaptadores sem fio podem ser incorporados nos circuitos principais de um dispositivo de hardware ou podem ser um acessório avulso a ser inserido em um dispositivo através da porta apropriada.

Ataque brute-force (força bruta)

Também conhecido como cracking por força bruta, trata-se de um método de tentativa e erro utilizado por programas aplicativos para decodificar dados criptografados, como senhas, através de procedimentos exaustivos (ou seja, força bruta) em vez de empregar estratégias intelectuais. Assim como um criminoso pode abrir ou arrombar um cofre tentando várias combinações possíveis, um aplicativo de crack força bruta experimenta seqüencialmente todas as combinações possíveis de caracteres válidos. A força bruta é considerada uma abordagem infalível, embora demorada.

Ataque de dicionário

Esses ataques envolvem a tentativa de uma variedade de palavras de uma lista para determinar a senha de alguém. Os atacantes não experimentam manualmente todas as combinações, mas possuem ferramentas que tentam automaticamente identificar a senha de alguém.

Ataque Man-in-the-Middle

O atacante intercepta mensagens em uma troca de chaves públicas e, em seguida, as retransmite, substituindo a chave requisitada pela sua própria chave pública, de maneira que as duas partes originais ainda pareçam estar se comunicando diretamente uma com a outra. O atacante usa um programa que aparenta ser o servidor para o cliente e que aparenta ser o cliente para o servidor. Esse ataque pode ser usado simplesmente para obter acesso às mensagens ou para permitir ao atacante modificá-las antes de retransmiti-las. O termo é derivado do jogo de bola no qual algumas pessoas tentam jogar uma bola diretamente de uma para outra enquanto uma pessoa no meio tenta alcançá-la.

Autenticação

O processo de identificação de um indivíduo, normalmente com base em um nome de usuário e uma senha. A autenticação garante que o indivíduo é quem afirma ser, mas nada diz quanto aos direitos de acesso desse indivíduo.

B

C

Chave

Uma série de letras e/ou números usados por dois dispositivos para autenticar sua comunicação. Ambos os dispositivos precisam ter a chave. Consulte também WEP e WPA-PSK.

Cliente

Um aplicativo, executado em um computador pessoal ou estação de trabalho, que depende de um servidor para executar algumas operações. Por exemplo, um cliente de e-mail é um aplicativo que permite enviar e receber e-mail.

Criptografia

A conversão de dados em um código secreto. A criptografia é a maneira mais eficaz de se conseguir segurança dos dados. Para ler um arquivo criptografado, uma pessoa precisa ter acesso a uma senha ou chave secreta que permita descriptografá-lo. Os dados não criptografados são chamados de texto simples, enquanto os dados criptografados são chamados de texto codificado.

D

E

Endereço IP

Um identificador para um computador ou dispositivo em uma rede TCP/IP. As redes que usam o protocolo TCP/IP roteiam as mensagens com base no endereço IP de destino. O formato de um endereço IP consiste em uma seqüência numérica de 32 bits escritos como quatro números separados por pontos. Cada número pode ser de zero a 255. Por exemplo, 192.168.1.100 pode ser um endereço IP.

Endereço MAC (Media Access Control)

Um endereço de baixo nível atribuído ao dispositivo físico que acessa a rede.

ESS (Extended Service Set)

Um conjunto de duas ou mais redes que formam uma única sub-rede.

F

Firewall

Um sistema desenvolvido para impedir o acesso não autorizado a uma rede privada ou a partir de uma rede privada. Os firewalls podem ser implementados tanto em hardware quanto em software, ou como uma combinação de ambos. Firewalls são freqüentemente utilizados para impedir usuários da Internet não autorizados de acessarem redes privadas conectadas à Internet, especialmente intranets. Todas as mensagens que entram e que saem da intranet passam pelo firewall. O firewall examina cada mensagem e bloqueia as que não satisfazem os critérios de segurança especificados. O firewall é considerado a primeira linha de defesa na proteção de informações privadas. Para maior segurança, os dados podem ser criptografados.

G

Gateway integrado

Um dispositivo que combina as funções de um ponto de acesso (PA), roteador e firewall. Alguns dispositivos também podem incluir aperfeiçoamentos de segurança e recursos de ponte.

H

Hotspot

Um local físico específico no qual um ponto de acesso (PA) oferece serviços públicos de rede sem fio em banda larga para visitantes móveis através de uma rede sem fio. Os hotspots costumam estar situados em locais com alta concentração de pessoas, como aeroportos, estações de trens, bibliotecas, marinas, centros de convenções e hotéis. Eles normalmente têm um alcance curto.

I

J

K

L

LAN (Local Area Network)

Uma rede de computador que se estende por uma área relativamente pequena. A maioria das LANs se restringe a um mesmo edifício ou grupo de edifícios. No entanto, uma LAN pode ser conectada a outras LANs a qualquer distância, via telefone ou ondas de rádio. Um sistema de LANs conectadas dessa forma é o que se chama de rede de longa distância (WAN, wide-area network).

A maioria das LANs conectam estações de trabalho e computadores pessoais, geralmente através de hubs ou switches simples. Cada nó (computador individual) de uma LAN possui sua própria CPU, com a qual executa programas, mas também é capaz de acessar dados e dispositivos (como, por exemplo, impressoras) em qualquer lugar da LAN. Isso significa que vários usuários podem compartilhar dispositivos caros, como impressoras a laser, bem como dados. Os usuários também podem usar a LAN para se comunicar uns com os outros, por exemplo, enviando e-mail ou entrando em sessões de chat.

Largura de banda

A quantidade de dados que podem ser transmitidos em um determinado período de tempo. Em dispositivos digitais, a largura de banda costuma ser expressa em bits por segundo (bps) ou em bytes por segundo. Em dispositivos analógicos, a largura de banda é expressa em ciclos por segundo ou Hertz (Hz).

M

MAC (Media Access Control ou Message Authenticator Code)

Quanto ao primeiro, consulte Endereço MAC. O segundo é um código utilizado para identificar uma determinada mensagem (por exemplo, uma mensagem RADIUS). O código é geralmente um “hash” criptograficamente forte do conteúdo da mensagem, incluindo um valor exclusivo para proporcionar uma proteção contra reprodução.

N

Negação de serviço

Na Internet, um ataque de negação de serviço (DoS, denial of service) é um incidente no qual um usuário ou organização é privado dos serviços ou de um recurso que, em condições normais, estaria disponível. Tipicamente, a perda de serviços consiste na indisponibilidade de um determinado serviço de rede, como o e-mail, ou a perda temporária de todos os serviços e da conectividade de rede. Nos piores casos, por exemplo, um site acessado por milhões de pessoas pode, ocasionalmente, ser forçado a interromper temporariamente sua operação. Um ataque de negação de serviço também pode destruir a programação e os arquivos de um sistema de computador. Embora normalmente seja proposital e mal-intencionado, um ataque de negação de serviço pode, às vezes, ocorrer acidentalmente. Um ataque de negação de serviço é um tipo de violação de segurança em sistemas de computadores que não costuma resultar em roubo de informações ou em outras perdas de segurança. No entanto, esses ataques podem custar bastante tempo e dinheiro à pessoa ou empresa atingida.

NIC (Network Interface Card)

Uma placa que se conecta a um laptop ou a algum outro dispositivo e que conecta esse dispositivo à LAN.

O

P

Placa adaptadora sem fio PCI

Conecta um computador desktop a uma rede. A placa se conecta em um slot de expansão PCI dentro do computador.

Placa adaptadora sem fio USB

Oferece uma interface serial Plug and Play expansível. Essa interface proporciona uma conexão padrão sem fio e de baixo custo para dispositivos periféricos, como teclados, mouses, joysticks, impressoras, scanners, dispositivos de armazenamento e câmeras de videoconferência.

Ponto de acesso (PA)

Um dispositivo de rede que possibilita a clientes 802.11 se conectarem a uma rede local (LAN). Os PAs estendem o alcance físico do serviço para usuários sem fio. Eles são ocasionalmente chamados de roteadores sem fio.

Pontos de acesso ilícitos

Um ponto de acesso que uma empresa não autoriza para operação. O problema é que os pontos de acesso ilícitos normalmente não estão em conformidade com as políticas de segurança de LAN sem fio (WLAN). Um ponto de acesso ilícito permite uma interface aberta e desprotegida com a rede corporativa, partindo de fora do perímetro controlado fisicamente.

Dentro de uma WLAN devidamente protegida, pontos de acesso ilícitos são mais prejudiciais que usuários ilícitos. Usuários não autorizados tentando obter acesso a uma WLAN provavelmente não conseguirão atingir recursos corporativos valiosos se mecanismos de autenticação eficazes estiverem implementados. No entanto, problemas graves podem ocorrer quando um funcionário ou hacker se conecta a um ponto de acesso ilícito. Tal ponto de acesso permite que praticamente qualquer um com um dispositivo equipado com 802.11 entre na rede corporativa. Isso os coloca muito próximos a recursos de importância crucial.

PPPoE

Point-to-Point Protocol Over Ethernet, um protocolo de comunicação. Usado por muitos provedores DSL, o PPPoE suporta a autenticação e as camadas de protocolo amplamente utilizadas no PPP, permitindo estabelecer uma conexão ponto a ponto na arquitetura habitualmente multiponto Ethernet.

Protocolo

Um formato padronizado para transmissão de dados entre dois dispositivos. Do ponto de vista do usuário, o único aspecto interessante em relação aos protocolos é que o computador ou dispositivo em questão precisa ter suporte para os protocolos apropriados caso queira se comunicar com outros computadores. O protocolo pode ser implementado em hardware ou em software.

Q

R

RADIUS (Remote Access Dial-In User Service)

Um protocolo que proporciona autenticação de usuários, normalmente numa situação de acesso remoto. Originalmente definido para uso com servidores de acesso remoto discado, o protocolo é atualmente usado em uma variedade de ambientes de autenticação, incluindo a autenticação 802.1x do segredo compartilhado do usuário de uma WLAN.

Rede

Um grupo de pontos de acesso e seus usuários associados; equivalente a um ESS. O McAfee Wireless Home Network Security mantém informações sobre essa rede. Consulte ESS.

Roaming

A capacidade de se passar da área de cobertura de um PA para a área de outro sem interrupção do serviço ou perda de conectividade.

Roteador

Um dispositivo de rede que encaminha pacotes de uma rede para outra. Com base em tabelas de roteamento internas, os roteadores lêem cada pacote recebido e determinam como encaminhá-lo. A interface do roteador para a qual os pacotes transmitidos são enviados pode ser determinada por qualquer combinação de endereços de origem e de destino, bem como condições de tráfego atuais, como carga, custos das linhas ou linhas ruins. Os roteadores são, às vezes, chamados de pontos de acesso (PA).

S

Segredo compartilhado

Consulte também RADIUS. Protege partes sigilosas de mensagens RADIUS. Esse segredo compartilhado é uma senha compartilhada entre o autenticador e o servidor de autenticação de alguma maneira segura.

Spoof (falsificação) de IP

Consiste em forjar o endereço IP de um pacote IP. Isso é usado em diversos tipos de ataque, incluindo seqüestro de sessão. Também é freqüentemente utilizado para falsificar os cabeçalhos de e-mail de SPAM para impedir que sejam rastreados corretamente.

SSID (Service Set Identifier)

Nome de rede para os dispositivos de um subsistema de LAN sem fio. Trata-se de uma seqüência de 32 caracteres de texto simples acrescentada ao cabeçalho de todo pacote WLAN. O SSID diferencia uma WLAN de outra, portanto, todos os usuários de uma rede precisam fornecer o mesmo SSID para ter acesso a um determinado PA. Um SSID impede o acesso de qualquer dispositivo cliente que não tenha o SSID. Contudo, o ponto de acesso (PA) divulga, por padrão, seu SSID ao se anunciar. Mesmo que a divulgação de SSID esteja desativada, um hacker pode detectar o SSID através de farejamento (sniffing).

SSL (Secure Sockets Layer)

Um protocolo desenvolvido pela Netscape para transmissão de documentos privados pela Internet. A SSL funciona utilizando uma chave pública para criptografar dados que é transferida através da conexão SSL. Tanto o Netscape Navigator quanto o Internet Explorer usam e suportam SSL, e muitos sites usam esse protocolo para obter informações confidenciais do usuário, como números de cartão de crédito. Por uma questão de convenção, os URLs que exigem uma conexão SSL começam com https: em vez de http:

T

Texto codificado

Dados que foram criptografados. O texto codificado é ilegível até ser convertido em texto simples (descriptografado) com uma chave.

Texto simples

Qualquer mensagem que não esteja criptografada.

TKIP (Temporal Key Integrity Protocol)

Um remédio rápido para superar as vulnerabilidades inerentes à segurança WEP, especialmente a reutilização de chaves de criptografia. O TKIP altera as chaves temporais a cada 10.000 pacotes, proporcionando um método de distribuição dinâmico que melhora significativamente a segurança da rede. O processo (de segurança) TKIP começa com uma chave temporal de 128 bits compartilhada entre clientes e pontos de acesso (PAs). O TKIP combina a chave temporal com o endereço MAC (da máquina cliente) e, em seguida, adiciona um vetor de inicialização relativamente grande de 16 octetos para produzir a chave que criptografa os dados. Esse procedimento garante que cada estação utilize fluxos de chaves diferentes para criptografar os dados. O TKIP usa RC4 para realizar a criptografia. A WEP também usa RC4.

U

V

VPN (Virtual Private Network)

Uma rede construída pela utilização de cabeamento público para reunificar nós. Existem, por exemplo, vários sistemas que permitem criar redes utilizando a Internet como meio para transporte de dados. Esses sistemas utilizam criptografia e outros mecanismos de segurança para garantir que somente usuários autorizados possam ter acesso à rede e que os dados não possam ser interceptados.

W

Wardriver

Pessoas munidas de laptops, software especial e algum hardware alternativo que circulam de carro por cidades, bairros e estacionamentos de empresas com o objetivo de interceptar tráfego de LAN sem fio.

WEP (Wired Equivalent Privacy)

Um protocolo de criptografia e autenticação definido como parte do padrão 802.11. Suas versões iniciais baseiam-se em codificadores RC4 e possuem vulnerabilidades significativas. A WEP tenta proporcionar segurança criptografando os dados através de ondas de rádio para que eles estejam protegidos ao serem transmitidos de um ponto para outro. No entanto, descobriu-se que a WEP não é tão segura quanto se acreditava.

Wi-Fi (Wireless Fidelity)

Termo utilizado genericamente em referência a qualquer tipo de rede 802.11, seja 802.11b, 802.11a, banda dupla, etc. O termo é empregado pela Wi-Fi Alliance.

Wi-Fi Alliance

Uma organização composta pelos maiores fornecedores de software e equipamentos de comunicação sem fio com o objetivo de (1) certificar todos os produtos com base no 802.11 quanto a interoperabilidade e (2) promover o termo Wi-Fi como marca global em todos os mercados para qualquer produto de LAN sem fio com base no 802.11. A organização atua como associação, laboratório de testes e agência reguladora para fornecedores que queiram promover a interoperabilidade e o crescimento da indústria.

Embora todos os produtos 802.11a/b/g sejam chamados Wi-Fi, somente produtos que tenham passado pelos testes da Wi-Fi Alliance podem ser denominados Wi-Fi Certified (uma marca registrada). Os produtos que são aprovados devem levar um selo de identificação em suas embalagens dizendo Wi-Fi Certified e que indique a banda de freqüências de rádio utilizada. Esse grupo era conhecido como Wireless Ethernet Compatibility Alliance (WECA), mas mudou de nome em outubro de 2002 para refletir melhor a marca Wi-Fi que desejava construir.

Wi-Fi Certified

Quaisquer produtos testados e aprovados como Wi-Fi Certified (uma marca registrada) pela Wi-Fi Alliance são certificados quanto a interoperabilidade mútua, mesmo que sejam de fabricantes diferentes. Um usuário com um produto Wi-Fi Certified pode usar qualquer marca de ponto de acesso (PA) com qualquer outra marca de hardware cliente que também seja certificado. Tipicamente, porém, qualquer produto Wi-Fi que utilize a mesma freqüência de rádio (por exemplo, 2,4 GHz para 802.11b ou 11g e 5 GHz para 802.11a) funciona com outro, mesmo que não seja Wi-Fi Certified.

WLAN (Wireless Local Area Network)

Consulte também LAN. Uma rede local que utiliza um meio sem fio para conexão. Uma WLAN usa ondas de rádio de alta freqüência em vez de fios para comunicação entre os nós.

WPA (Wi-Fi Protected Access)

Um padrão de especificação que aumenta em muito o nível de proteção de dados e controle de acesso para sistemas de LAN sem fio futuros e existentes. Desenvolvido para ser executado em hardware existente ou como uma atualização de software, o WPA é derivado do padrão IEEE 802.11i, sendo compatível com este. Quando instalado corretamente, proporciona aos usuários de LAN sem fio um elevado grau de garantia de que seus dados permaneçam protegidos e que apenas usuários de rede autorizados tenham acesso à rede.

WPA-PSK

Um modo especial de WPA desenvolvido para usuários domiciliares que não precisam de uma segurança tão forte quanto a de empresas e que não têm acesso a servidores de autenticação. Nesse modo, o usuário domiciliar digita manualmente a senha inicial para ativar o Wi-Fi Protected Access (WPA) em modo pré-compartilhado (Pre-Shared Key ou PSK), devendo ele próprio alterar a frase de senha de cada computador e ponto de acesso sem fio regularmente. Consulte também TKIP.

X

Y

Z

Índice

C

D

E

F

G

H

I

L

M

N

O

P

Q

R

S

T

U

V

W